


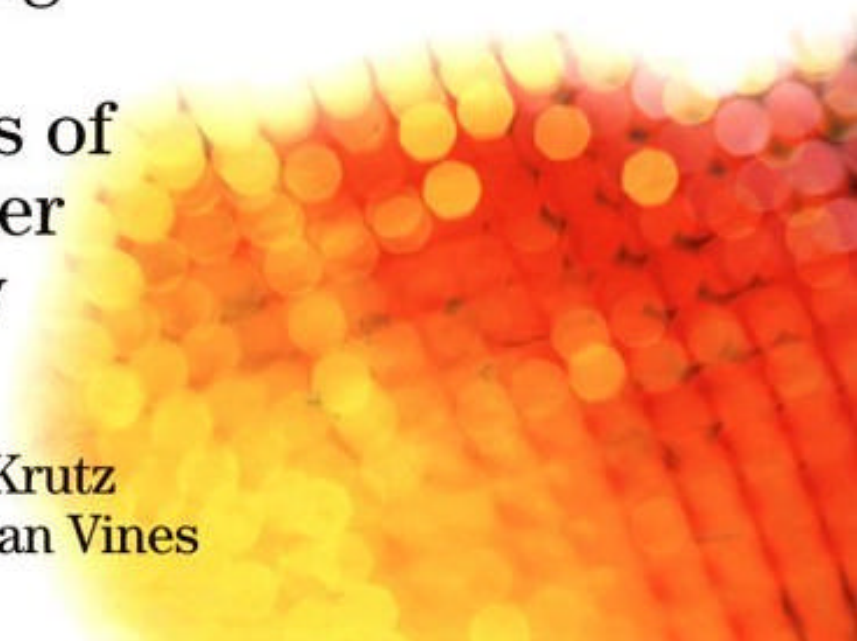
 WILEY



The **CISSP**[®] **Prep Guide**

Mastering
the Ten
Domains of
Computer
Security

Ronald L. Krutz
Russell Dean Vines



The CISSP Prep Guide—Mastering the Ten Domains of Computer Security

Ronald L. Krutz

Russell Dean Vines

Wiley Computer Publishing

John Wiley & Sons, Inc.

Publisher: Robert Ipsen

Editor: Carol Long

Managing Editor: Micheline Frederick

Text Design & Composition: D&G Limited, LLC

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons, Inc., is aware of a claim, the product names appear in initial capital or ALL CAPITAL LETTERS. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

Copyright © 2001 by Ronald L. Krutz and Russell Dean Vines. All rights reserved.

Published by John Wiley & Sons, Inc.

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4744. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 605 Third Avenue, New York, NY 10158-0012, (212) 850-6011, fax (212) 850-6008, E-Mail: PERMREQ @ WILEY.COM.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in professional services. If professional advice or other expert assistance is required, the services of a competent professional person should be sought.

Library of Congress Cataloging-in-Publication Data:

Krutz, Ronald L., 1938–

The CISSP prep guide: mastering the ten domains of computer security/Ronald L. Krutz,

Russell Dean Vines.

p. cm.

Includes bibliographical references and index.

ISBN 0-471-41356-9 (pbk. : alk. paper)

1. Electronic data processing personnel—Certification. 2. Computer networks—Examinations—Study guides. I. Vines, Russell Dean, 1952–. II. Title.

QA76.3 K78 2001

005.8—dc21 Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

The constant joys in my life—my daughters, Sheri and Lisa—who have given me the latest miracles in my life—Patrick, Ryan, and the Angel who is on the way.

—RLK

About the Authors

Ronald L. Krutz, Ph.D., P.E., CISSP. Dr. Krutz is a Senior Information Assurance Consultant with Corbett Technologies, Inc. He is the lead assessor for all Capability Maturity Model (CMM) engagements for Corbett Technologies and led the development of Corbett's HIPAA-CMM assessment methodology. Dr. Krutz is also a lead instructor for the (ISC)² CISSP Common Body of Knowledge review seminars. He has over forty years of experience in distributed computing systems, computer architectures, real-time systems, information assurance methodologies and information security training.

He has been an Information Security Consultant at Realtech Systems Corporation, an Associate Director of the Carnegie Mellon Research Institute (CMRI), and a Professor in the Carnegie Mellon University Department of Electrical and Computer Engineering. Dr. Krutz founded the CMRI Cybersecurity Center and was founder and Director of the CMRI Computer, Automation and Robotics Group. Prior to his 24 years at Carnegie Mellon University, Dr. Krutz was a Department Director in the Singer Corporate R&D Center and a Senior Engineer at Gulf Research and Development Company.

Dr. Krutz conducted and sponsored applied research and development in the areas of computer security, artificial intelligence, networking, modeling and simulation, robotics, and real-time computer applications. He is the author of three textbooks in the areas of microcomputer system design, computer interfacing, and computer architecture, and is the holder of seven patents in the area of digital systems. He also is an instructor in the University of Pittsburgh Computer Engineering Program where he teaches courses in information system security and computer organization. Dr. Krutz is a Certified Information Systems Security Professional (CISSP) and a Registered Professional Engineer (P.E.).

Russell Dean Vines, CISSP, CCNA, MCSE, MCNE. Mr. Vines is currently President and founder of the RDV Group, Inc. (www.rdvgroup.com), a New York City-based security consulting services firm, whose clients include government, finance, and new media organizations. Mr. Vines has been active in the prevention, detection, and remediation of security vulnerabilities for international corporations for many years. He is a frequent speaker on privacy, security awareness, and best practices in the information industry. He is also an instructor for the (ISC)² CISSP Common Body of Knowledge review seminars.

Mr. Vines has been active in computer engineering for nearly 20 years. He has earned high level certifications in Cisco, 3Com, Ascend, Microsoft, and Novell technologies, and has been trained in the National Security Agency's ISSO Information Assessment Methodology. He formerly directed the Security Consulting Services Group for Realtech Systems Corporation; designed, implemented, and managed large global information networks for CBS/Fox Video, Inc.; and was Director of MIS for the Children's Aid Society in New York City.

After receiving a Downbeat magazine scholarship to Boston's Berklee College of Music, Mr. Vines's early professional years were illuminated not by the flicker of a computer monitor, but by the bright lights of Nevada nightclubs. He performed as a sideman for a variety of well-known entertainers, including George Benson, John Denver, Sammy Davis Jr., and Dean Martin. Mr. Vines composed and arranged hundreds of pieces of jazz and contemporary music that were recorded and performed by his own big band and others, founded and managed a scholastic music publishing company, and worked as an artist-in-residence in communities throughout the West. He still performs and teaches music in the New York City area, and is a member of Local #802, American Federation of Musicians.

Acknowledgments

I want to express my appreciation to my wife, Hilda, for her patience and support during the writing of this guide.

—*RLK*

I would like to take this opportunity to thank those who have either directly or indirectly helped me write this book: The astute and diligent editors at Wiley. My former co-workers at Realtech Systems Corporation: Bill Glennon, Diana Ng Yang, Cuong Vu, Robert Caputo and Justin Jones. My parents Marian MacKenzie and James Vines. Good friends: Virginia French Belanger, Richard Kelsey, Dean Calabrese, George Pettway, Bill Easterby, John Sabasteanski, Ken Brandt, Edward Stroz, and the greatest tuba player in the world, Howard Johnson.

I would especially like to thank my best friend and wife, Elzy Kolb, for her continual support and guidance, without whom I would not be where I am today.

Table of Contents

The CISSP Prep Guide—Mastering the Ten Domains of
Computer Security

Foreword

Introduction

Chapter 1 - Security Management Practices

Chapter 2 - Access Control Systems

Chapter 3 - Telecommunications and Network Security

Chapter 4 - Cryptography

Chapter 5 - Security Architecture and Models

Chapter 6 - Operations Security

Chapter 7 - Applications and Systems Development

Chapter 8 - Business Continuity Planning and Disaster
Recovery Planning

Chapter 9 - Law, Investigation, and Ethics

Chapter 10 - Physical Security

Appendix A - Glossary of Terms and Acronyms

Appendix B - The RAINBOW Series—Minimum Security
Requirements for Multi-user Operating
Systems NISTIR 5153

Appendix C - Answers to Sample Questions

Appendix D - A Process Approach to HIPAA Compliance
Through a HIPAA-CMM

Appendix E - The NSA InfoSec Assessment Methodology

Appendix F - The Case for Ethical Hacking

Appendix G - The Common Criteria

Appendix H - References for Further Study

Appendix I - British Standard 7799

Index

List of Figures

List of Tables

List of Sidebars

Foreword

One day last year, the CEO of a large media company received an alarming e-mail. The sender said that he had gained access to the computer system of the CEO's company. If the CEO were willing to pay a large sum of money, the sender would reveal the weaknesses that he had found in the company's computer system. Just to ensure that he was taken seriously, several sensitive files (including photographs) that could only have come from the company's network were attached to the e-mail. This message was not a drill—this situation was reality.

As you might expect, this kind of problem goes straight to the top of the “to-do” list for the victimized company. The CEO needed many immediate answers and solutions: the true source of the e-mail, the accuracy of the claims made by the sender, the possible weaknesses that might have been used to break into the system, why the intrusion detection system was not triggered, the steps that could be taken to further tighten security, the legal actions that might be possible, and the best way to deal with an adversary who was living halfway around the world.

For several months, many people—including computer security professionals—worked to gather information and evidence, to secure the system, and to track down the source of the attack. Ultimately, undercover officers from New Scotland Yard and the FBI met the unsuspecting “cyber extortionists” at a designated location in London, where they were arrested. They are currently in jail, awaiting extradition to the United States.

For anyone who has information security experience, this case will bring many thoughts to mind about some of the tools of the trade: logging, packet sniffers, firewalls and their rule sets, and legal access rights to e-mail communications (concepts covered in this book). Also, this incident raises questions about how an adversary in a remote location can gain access to a computer network without detection.

As those of us who have been involved in this field for years know, information systems security is achieved through intelligent risk management, rather than through risk elimination. Computer information security professionals find themselves at the core of a collaborative decision-making process. They must be able to provide answers and explanations that are anchored in sound methodology.

Not all security issues that arise in the daily course of business will be as intense as the case study cited here, and many will be quite subtle. As many of the finest minds in technology focus more on the topic of security, there is a growing consensus that security is ensured through a process, rather than through a blind reliance on software or hardware products. No one in this field disputes that a computer security professional must be armed with training and experience in order to be effective.

As you read this book, keep in mind that those people who are closest to the business operations of an organization are in a great position to help notice anomalies. I often point out to clients that a violation of computer security might only be apparent to someone who is intimately familiar with the features of a given network and its file structure. It is not just what you see, but what you know.

For example, if you went home tonight and found that your family photographs on your bedroom nightstand had been switched around, yet everything else in the house was still in its place, you would immediately know that someone had been in your home. Would a security guard who does not intimately know your home be able to notice this kind of difference, even if he or she took the time to look at your nightstand? More than likely, the answer is no. Similarly, there are many computer network features that an

intruder could disturb, yet would go unnoticed by everyone except an expert who is familiar with your system.

You must sometimes point out to clients that the most serious threat to information systems security comes from people, not machines. A person who is an insider and is given a user account on a computer system has an enormous advantage in targeting an attack on that system. Computer crime statistics consistently show that insiders, as opposed to outside hackers, do greater damage to systems. As brilliant as they might be, computer criminals are a poor choice as computer security professionals.

Think of the concept this way: While the fictional criminal Dr. Hannibal Lecter, in the movie "Silence of the Lambs," was brilliant in many ways, I would not trust him with my family. I respect the knowledge that smart people possess, but when you bring one on the team you receive their knowledge and their ethics—a package deal.

As you study the depth of material provided in this book, keep in mind that the information systems security professional of today is just that: a professional. Professionals must abide by rigorous standards yet provide something that computers cannot: human judgment. As a result, the (ISC)² requires strict adherence to its Code of Ethics before granting CISSP certifications.

If you are beginning your *Certified Information System Security Professional* (CISSP) certification, this book provides the framework to help you become a CISSP. If you are a harried IT manager for whom security is becoming an increasingly daily concern, this book will give you the fundamental concepts and a solid foundation to implement effective security controls. If you are already a CISSP or an active security practitioner, the "CISSP Prep Guide" will help you succeed in a field that has become crucial to the success of business and to the security of a nation's economy.

Edward M. Stroz

April 2001

Edward Stroz is president of Stroz Associates, LLC, a consulting firm specializing in helping clients detect and respond to incidents of computer crime. He was an agent with the FBI, where he formed and supervised the computer crime squad in its New York office. He can be reached at www.strozassociates.com.

Introduction

You hold in your hand a key, a key to unlocking the secrets of the world of information systems security. This world will present you with many new challenges and rewards, because information systems security is the latest frontier in man's continuing search for effective communication. Communication has taken many forms over the centuries, the Internet and electronic communications being only our most recent attempt. But for effective communication to survive and prosper, it needs reliability, confidence, and security. It needs security professionals who can provide the secure foundation for the growth of this new communication. It needs professionals like you.

With the increasing use of the World Wide Web for e-business, transaction information must be protected from compromise. Threats to networks and information systems in general come from sources internal and external to the organization. These threats materialize in the form of stolen intellectual property, denial of service to customers, unauthorized use of critical resources, and malicious code that destroys or alters valuable data.

The need to protect information resources has produced a demand for information systems security professionals. Along with this demand came a need to ensure that these professionals possess the knowledge to perform the required job functions. To address this need, the Certified Information Systems Security Professional (CISSP) certification was developed. This certification guarantees to all parties that the certified individual meets standard criteria of knowledge and continues to upgrade that knowledge in the field of information systems security. The CISSP initiative also serves to enhance the recognition and reputation of the field of information security.

The (ISC)² Organization

The CISSP certification is the result of cooperation among a number of North American professional societies in establishing the International Information Systems Security Certification Consortium [(ISC)²] in 1989. (ISC)² is a nonprofit corporation whose sole function is to develop and administer the certification program. The organization has defined a common body of knowledge (CBK) that defines a common set of terms that information security professionals can use to communicate with each other and establish a dialogue in the field. This guide has been created based on the most recent CBK and skills as described by (ISC)² for security professionals. At this time, the domains, in alphabetical order, are:

- Access Control Systems and Methodology
- Application and Systems Development Security
- Business Continuity Planning and Disaster Recovery Planning
- Cryptography
- Law, Investigation, and Ethics
- Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications and Networking Security

(ISC)² conducts review seminars and administers examinations for information security practitioners seeking the CISSP certification. Candidates for the examination must attest that they have 3 to 5 years' experience in the information security field and subscribe to the (ISC)² Code of Ethics. The seminars cover the CBK from which the

examination questions are taken. The seminars are not intended to teach the examination.

The Examination

The examination questions are taken from the CBK and are aimed at the level of a 3-to-5-year practitioner in the field. It comprises 250 English-language questions of which 25 are not counted. The 25 are trial questions that may be used on future exams. The 25 are not identified, so there is no way to tell which questions they are. The questions are not ordered according to domain but are randomly arranged. There is no penalty for answering questions that are in doubt. Six hours are allotted for the examination.

The examination questions are multiple choice with four possible answers. No acronyms are used without being explained. It is important to read the questions carefully and thoroughly and to choose the *best* possible answer of the four. As with any conventional test-taking strategy, a good approach is to eliminate two of the four answers and then choose the best answer of the remaining two. The questions are not of exceptional difficulty for a knowledgeable person who has been practicing in the field. However, most professionals are not usually involved with all ten domains in their work. It is uncommon for an information security practitioner to work in all the diverse areas covered by the CBK. For example, specialists in physical security may not be required to work in depth in the areas of computer law or cryptography as part of their job descriptions. The examination questions, also, do not refer to any specific products or companies. Approximately 70% of the people taking the examination score a passing grade.

The Approach of This Book

Based on the experience of the authors who have both taken and passed the CISSP examination, there is a need for a single, high-quality, reference source that the candidate can use to prepare for the examination and use if the candidate is taking the (ISC)² CISSP training seminar. Prior to this text, the candidate's choices were as follows:

- Buy numerous expensive texts and use a small portion of each in order to cover the breadth of the ten domains.
- Purchase a so-called single-source book that focuses on areas in the domains not emphasized in the CBK or that leaves gaps in the coverage of the CBK.

One-stop, up-to-date preparation

This text is truly a one-stop source of information that emphasizes the areas of knowledge associated with the CBK and avoids the extraneous mathematical derivations and irrelevant material that serve to distract the candidate during the intensive period of preparation for the examination. It covers the breadth of the CBK material and is independent of the breakdown of the domains or the possible merger of domains. Thus, even though the domains of the CBK may eventually be reorganized, the fundamental content is still represented in this text. Also, of equal importance, material has been added that reflects recent advances in the information security arena that will be valuable to the practicing professional and may be future components of the CBK.

Organization of the Book

The text is organized into the following chapters:

Chapter 1—Security Management Practices

Chapter 2—Access Control Systems

Chapter 3—Telecommunications and Network Security

Chapter 4—Cryptography

Chapter 5—Security Architecture and Models

Chapter 6—Operations Security

Chapter 7—Applications and Systems Development

Chapter 8—Business Continuity Planning and Disaster Recovery Planning

Chapter 9—Law, Investigation and Ethics

Chapter 10—Physical Security

A—Glossary of Terms and Acronyms

B—The RAINBOW Series

C—Answers to Sample Questions

D—A Process Approach to HIPAA Compliance through an HIPAA-CMM

E—The NSA InfoSec Assessment Methodology

F—The Case for Ethical Hacking

G—The Common Criteria

H—References for Further Study

I—British Standard 7799

Each domain of the CBK is accompanied by a series of sample practice questions that are of the same format as those in the CISSP examination. Answers are provided to each question along with explanations of the answers.

The appendices include valuable reference material and advanced topics. For example, Appendix E summarizes the National Security Agency's InfoSec Assessment Methodology (IAM). Appendix G provides an excellent overview of the Common Criteria, which is replacing a number of U.S. and international evaluation criteria guidelines, including the Trusted Computer System Evaluation Criteria (TCSEC). The Common Criteria is the result of the merging of a number of criteria in order to establish one evaluation guideline that is accepted and used by the international community.

Emerging process approaches to information systems security as well as their application to the recent Health Insurance Portability and Accountability Act (HIPAA) are covered in Appendix D. These methodologies include the Systems Security Engineering Capability Maturity Model (SSE-CMM) and a newly proposed HIPAA-CMM. A brief history of the CMM, culminating in the HIPAA-CMM, is given in this appendix.

Who Should Read This Book

There are three main categories of readers for this comprehensive guide:

1. Candidates for the CISSP examination who are studying on their own or those taking the CISSP review seminar will find this text a valuable aid in their preparation plan. The guide provides a no-nonsense way of obtaining

the information needed without having to sort through numerous books covering portions of the CBK domains and then filtering their content to acquire the fundamental knowledge needed for the exam. The sample questions provided will acclimate the reader to the type of questions that will be encountered on the exam and the answers serve to cement and reinforce the candidate's knowledge.

2. Students attending information system security certification programs offered in many of the major universities will find this text a valuable addition to their reference library. For the same reasons cited for the candidate preparing for the CISSP exam, this book is a single source repository of fundamental and emerging information security knowledge. It presents the information at the level of the experienced information security professional and, thus, is commensurate with the standards required by universities for their certificate offerings.
3. The material contained in this book will be of practical value to information security professionals in performing their job functions. The professional, certified or not, will refer to the text as a refresher for information security basics as well as a guide to the application of emerging methodologies.

Summary

The authors sincerely believe that this text will provide a more cost-effective and timesaving means of preparing for the CISSP certification examination. By using this reference, the candidate can focus on the fundamentals of the material instead of spending time deciding upon and acquiring numerous expensive texts that may turn out to be, on the whole, inapplicable to the desired domain. It also provides the breadth and depth of coverage to avoid gaps in the CBK that are present in other "single" references.

The information security material in the text is presented in an organized, professional manner that will be a primary source of information for students in the information security field as well as practicing professionals.

Chapter 1: Security Management Practices

Overview

In our first chapter we will enter the domain of Security Management. Throughout this book you will see that many Information Systems Security (InfoSec) domains have several elements and concepts that overlap. While all other security domains are clearly focused, this domain, for example, introduces concepts that are extensively touched upon in both the Operations Security (Chapter 6) and Physical Security (Chapter 10) domains. We will try to point out those occasions where the material is repetitive, but be aware that if a concept is described in several domains, you will need to understand it.

From the published (ISC)² goals for the Certified Information Systems Security Professional candidate:

“The candidate will be expected to understand the planning, organization, and roles of individuals in identifying and securing an organization’s information assets; the development and use of policies stating management’s views and position on particular topics and the use of guidelines standards, and procedures to support the polices; security awareness training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary and private information; employment agreements; employee hiring and termination practices; and the risk management practices and tools to identify, rate, and reduce the risk to specific resources.”

A professional will be expected to know the following:

- Basic information about security management concepts
- The difference between policies, standards, guidelines, and procedures
- Security awareness concepts
- Risk management (RM) practices
- Basic information on classification levels

Our Goals

We will examine the InfoSec domain of Security Management using the following elements:

- Concepts of Information Security Management
- The Information Classification Process
- Security Policy Implementation
- The roles and responsibilities of Security Administration
- Risk Management Assessment Tools (including Valuation Rationale)
- Security Awareness Training

Domain Definition

The InfoSec domain of Security Management incorporates the identification of the information data assets with the development and implementation of policies, standards, guidelines, and procedures. It defines the management practices of data classification and risk management. It also addresses confidentiality, integrity, and availability by identifying threats, classifying *the organization’s* assets, and rating their vulnerabilities so that effective security controls can be implemented.

Management Concepts

Under the heading of Information Security Management Concepts, we will discuss the following:

- The big three: Confidentiality, Integrity, and Availability
- The concepts of identification, authentication, accountability, authorization, and privacy
- The objective of security controls — to reduce the impact of threats and the likelihood of their occurrence

The Big Three

Throughout this book you will read about the three tenets of InfoSec: Confidentiality, Integrity, and Availability (C.I.A.), as shown in Figure 1.1. These concepts represent the three fundamental principles of information security. All of the information security controls and safeguards, and all of the threats, vulnerabilities, and security processes are subject to the C.I.A yardstick.

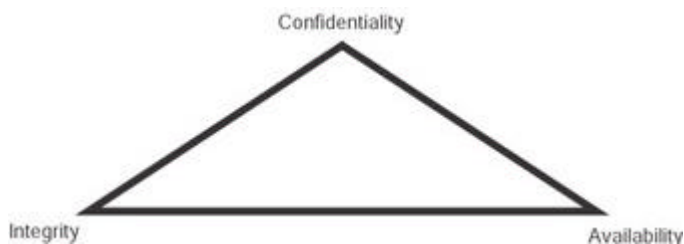


Figure 1.1: The C.I.A. triad.

Confidentiality. In InfoSec, the concept of *confidentiality* attempts to prevent the intentional or unintentional unauthorized disclosure of a message's contents. Loss of confidentiality can occur in many ways, such as through the intentional release of private company information or through a misapplication of network rights.

Integrity. In InfoSec, the concept of *integrity* ensures that:

- Modifications are not made to data by unauthorized personnel or processes
- Unauthorized modifications are not made to data by authorized personnel or processes
- The data are internally and externally consistent, i.e., that the internal information is consistent among all subentities and that the internal information is consistent with the real world, external situation.

Availability. In InfoSec, the concept of *availability* ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words, availability guarantees that the systems are up and running when they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.

Note D.A.D. is the reverse of C.I.A.

The reverse of confidentiality, integrity, and availability is disclosure, alteration, and destruction (D.A.D.).

Other Important Concepts

There are also several other important concepts and terms that a CISSP candidate must fully understand. These concepts include identification, authentication, accountability, authorization, and privacy.

Identification. The means in which users claim their identities to a system. Most commonly used for access control, identification is necessary for authentication and authorization.

Authentication. The testing or reconciliation of evidence of a user's identity. It establishes the user's identity and ensures that the users are who they say they are.

Accountability. A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual. Audit trails and logs support accountability.

Authorization. The rights and permissions granted to an individual (or process), which enable access to a computer resource. Once a user's identity and authentication are established, authorization levels determine the extent of system rights that an operator can hold.

Privacy. The level of confidentiality and privacy protection that a user is given in a system. This is often an important component of security controls. Privacy not only guarantees the fundamental tenet of confidentiality of a company's data, but also guarantees the data's level of privacy, which is being used by the operator.

Objectives of Security Controls

The prime objective of security controls is to reduce the effects of security threats and vulnerabilities to a level that is tolerable by an organization. This entails determining the impact a threat may have on an organization, and the likelihood that the threat could occur. The process that analyzes the threat scenario and produces a representative value of the estimated potential loss is called Risk Analysis (RA).

A small matrix can be created using an x-y graph where the y-axis represents the level of impact of a realized threat, and the x-axis represents the likelihood of the threat being realized, both set from low to high. When the matrix is created, it produces the graph shown in Figure 1.2. Remember the goal here is to reduce both the level of impact and the likelihood of a threat or disastrous event by implementing the security controls. A properly implemented control should move the plotted point from upper right — the threat value defined before the control was implemented — to the lower left (that is, toward 0,0), after the control was implemented. This concept is also very important when determining a control's cost/benefit ratio.

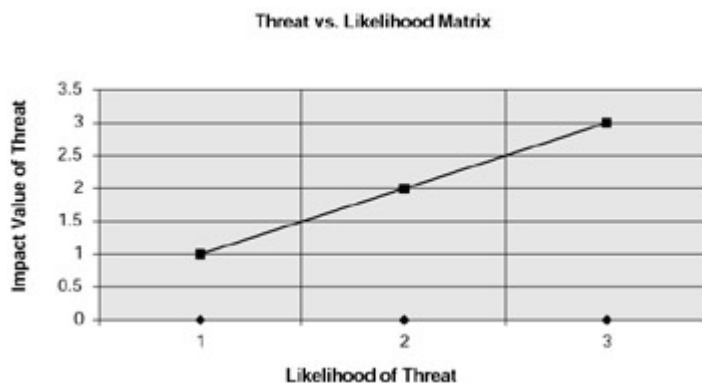


Figure 1.2: Threat versus likelihood matrix.

Therefore, an improperly designed or implemented control will show very little to no movement in the point before and after the control's implementation. The point's movement toward the 0,0 range could be so small (or in the case of very badly

designed controls, in the opposite direction) that it does not warrant the expense of implementation. In addition, the 0,0 point (no threat with no likelihood) is impossible to achieve because a very unlikely threat could still have a measurement of .000001. Thus, it would still exist and possibly have a measurable impact. For example, the possibility that a flaming pizza delivery van will crash into the operations center is extremely unlikely, however, this potentially dangerous situation could still occur and have a fairly serious impact on the availability of computing resources.

A matrix with more than four subdivisions can be used for more detailed categorization of threats and impacts, if desired.

Information Classification Process

The first major InfoSec process we examine in this chapter is the concept of Information Classification. The Information Classification Process is related to the domains of Business Continuity Planning and Disaster Recovery Planning because both focus on business risk and data valuation, yet, it is still a fundamental concept in its own right, and is one that a CISSP candidate must understand.

Information Classification Objectives

There are several good reasons to classify information. Not all data has the same value to an organization. Some data is more valuable to the people who are making strategic decisions because it aids them in making long-range or short-range business direction decisions. Some data, such as trade secrets, formulas, and new product information, is so valuable that its loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility.

For these reasons, it is obvious that information classification has a higher, enterprise-level benefit. Information can have an impact on a business globally, not just on the business unit or line operations levels. Its primary purpose is to enhance confidentiality, integrity, and availability, and to minimize the risks to the information. In addition, by focusing the protection mechanisms and controls on the information areas that need it the most, a more efficient cost-to-benefit ratio is achieved.

Information classification has the longest history in the government sector. Its value has been established, and it is a required component when securing trusted systems. In this sector, information classification is primarily used to prevent the unauthorized disclosure and the resultant failure of confidentiality.

Information classification may also be used to comply with privacy laws, or to enable regulatory compliance. A company may wish to employ classification to maintain a competitive edge in a tough marketplace. There may also be sound legal reasons for a company to employ information classification, such as to minimize liability or to protect valuable business information.

Information Classification Benefits

In addition to the reasons mentioned previously, employing information classification has several clear benefits to an organization. Some of these benefits are as follows:

- Demonstrates an organization's commitment to security protections
- Helps identify which information is the most sensitive or vital to an organization

- Supports the tenets of confidentiality, integrity, and availability as it pertains to data
- Helps identify which protections apply to which information
- May be required for regulatory, compliance, or legal reasons

Information Classification Concepts

The information produced or processed by an organization must be classified according to the organization's sensitivity to its loss or disclosure. These data owners are responsible for defining the sensitivity level of the data. This approach enables the security controls to be properly implemented according to its classification scheme.

Classification Terms

The following definitions describe several governmental data classification levels, ranging from the lowest level of sensitivity, to the highest:

1. *Unclassified*. Information that is designated as neither sensitive nor classified. The public release of this information does not violate confidentiality.
2. *Sensitive but Unclassified (SBU)*. Information that has been designated as a minor secret, but may not create serious damage if disclosed. Answers to tests are an example of this kind of information. Health care information is another example of SBU data.
3. *Confidential*. Information that is designated to be of a confidential nature. The unauthorized disclosure of this information could cause some damage to the country's national security. This level is used for documents labeled between SBU and Secret in sensitivity.
4. *Secret*. Information that is designated of a secret nature. The unauthorized disclosure of this information could cause serious damage to the country's national security.
5. *Top Secret*. The highest level of information classification (actually the President of the United States has a level only for him). The unauthorized disclosure of Top Secret information will cause exceptionally grave damage to the country's national security.

In all of these categories, in addition to having the appropriate clearance to access the information, an individual or process must have a "need-to-know" the information. Thus, an individual cleared for Secret or below is not authorized to access Secret material that is not needed for him or her to perform their assigned job functions.

In addition, the following classification terms are also used in the private sector (see Table 1.1):

1. *Public*. Information that is similar to unclassified information; all of a company's information that does not fit into any of the next categories can be considered public. This information should probably not be disclosed. However, if it is disclosed, it is not expected to seriously or adversely impact the company.
2. *Sensitive*. Information that requires a higher level of classification than normal data. This information is protected from a loss of confidentiality, as well as from a loss of integrity due to an unauthorized alteration.
3. *Private*. Information that is considered of a personal nature and is intended for company use only. Its disclosure could adversely affect the company or its employees. For example, salary levels and medical information are considered private.

4. *Confidential*. Information that is considered very sensitive and is intended for internal use only. This information is exempt from disclosure under the Freedom of Information Act. Its unauthorized disclosure could seriously and negatively impact a company. For example, information about new product development, trade secrets, and merger negotiations is considered confidential.

Table 1.1: A Simple Private/Commercial Sector Information Classification Scheme

Definition	Description
Public Use	Information that is safe to disclose publicly
Internal Use Only	Information that is safe to disclose internally, but not externally
Company Confidential	The most sensitive need-to-know information

Classification Criteria

Several criteria are used to determine the classification of an information object.

Value. Value is the number one commonly used criteria for classifying data in the private sector. If the information is valuable to an organization or its competitors, it needs to be classified.

Age. The classification of the information may be lowered if the information's value decreases over time. In the Department of Defense, some classified documents are automatically declassified after a predetermined time period has passed.

Useful Life. If the information has been made obsolete due to new information, substantial changes in the company, or other reasons, the information can often be declassified.

Personal Association. If information is personally associated with specific individuals or is addressed by a privacy law, it may need to be classified. For example, investigative information that reveals informant names may need to remain classified.

Information Classification Procedures

There are several steps in establishing a classification system. The following primary procedural steps are listed in priority order:

1. Identify the administrator/custodian.
2. Specify the criteria of how the information will be classified and labeled.
3. Classify the data by its owner, who is subject to review by a supervisor.
4. Specify and document any exceptions to the classification policy.
5. Specify the controls that will be applied to each classification level.
6. Specify the termination procedures for declassifying the information or for transferring custody of the information to another entity.
7. Create an enterprise awareness program about the classification controls.

Distribution of Classified Information

External distribution of classified information is often necessary, and the inherent security vulnerabilities will need to be addressed. Some of the instances when this distribution will be necessary are as follows:

- *Court order.* Classified information may need to be disclosed to comply with a court order.
- *Government contracts.* Government contractors may need to disclose classified information *in accordance with* (IAW) the procurement agreements that are related to a government project.
- *Senior-level approval.* A senior-level executive may authorize the release of classified information to external entities or organizations. This release may require the signing of a confidentiality agreement by the external party.

Information Classification Roles

The roles and responsibilities of all participants in the information classification program must be clearly defined. A key element of the classification scheme is the role the users, owners, or custodians of the data play in regard to the data. The roles that owner, custodian, and user play in information classification are described and are important to remember.

Owner

An *information owner* may be an executive or manager of an organization. This person is responsible for the asset of information that must be protected. An owner is different from a custodian. The owner has the final corporate responsibility of data protection, and under the concept of due care, the owner may be liable for negligence because of the failure to protect this data. However, the actual day-to-day function of protecting the data belongs to a custodian.

The responsibilities of an information owner could include the following:

- Making the original determination to decide what level of classification the information requires, which is based upon the business needs for the protection of the data.
- Reviewing the classification assignments periodically and making alterations as the business needs change.
- Delegating the responsibility of the data protection duties to the custodian.

Custodian

An *information custodian* is delegated the responsibility of protecting the information by its owner. This role is commonly executed by IT systems personnel. The duties of a custodian may include the following:

- Running regular backups and routinely testing the validity of the backup data
- Performing data restoration from the backups when necessary
- Maintaining those retained records *in accordance with* (IAW) the established information classification policy

In addition, the custodian may also have additional duties, such as being the administrator of the classification scheme.

User

In the information classification scheme, an *end user* is considered to be anyone (such as an operator, employee or external party) that routinely uses the information as part of their job. They can also be considered a consumer of the data, who needs daily access to the information to execute their tasks. The following are a few important points to note about end users:

- Users must follow the operating procedures that are defined in an organization's security policy, and they must adhere to the published guidelines for its use.
- Users must take "due care" to preserve the information's security during their work (as outlined in the corporate information use policies). They must prevent "open view" from occurring (see sidebar).
- Users must use company computing resources only for company purposes, and not for personal use.

Open View

The term "open view" refers to the act of leaving classified documents in the open where an unauthorized person can see them, thus violating the information's confidentiality. Procedures to prevent "open view" should specify that information is to be stored in locked areas, or transported in properly sealed containers, for example.

Security Policy Implementation

Security Policies are the basis for a sound security implementation. Often organizations will implement technical security solutions without first creating a foundation of policies, standards, guidelines, and procedures, which results in unfocused and ineffective security controls.

The following questions are discussed in this section:

- What are policies, standards, guidelines, and procedures?
- Why do we use policies, standards, guidelines, and procedures?
- What are the common policy types?

Policies, Standards, Guidelines, and Procedures

Policies

A policy is one of those terms that can mean several things in InfoSec. For example, there are security policies on firewalls, which refer to the access control and routing list information. Standards, procedures, and guidelines are also referred to as policies in the larger sense of a global Information Security Policy.

A good, well-written policy is more than an exercise that is created on white paper, it is an essential and fundamental element of sound security practice. A policy, for example, can literally be a life saver during a disaster, or it may be a requirement of a governmental or regulatory function. A policy can also provide protection from liability due to an employee's actions, or can form a basis for the control of trade secrets.

Policy Types

When we refer to specific policies, rather than a group “policy,” we are generally referring to those policies that are distinct from the standards, procedures, and guidelines. As you can see from the Policy Hierarchy chart shown in Figure 1.3, policies are considered the first and highest level of documentation, from which the lower level elements of standards, procedures, and guidelines flow. This order, however, does not mean that policies are more important than the lower elements. These higher level policies, which are the more general policies and statements, should be created first in the process for strategic reasons, and then the more tactical elements can follow.



Figure 1.3: Policy hierarchy.

Senior Management Statement of Policy. The first policy of any policy creation process is the Senior Management Statement of Policy. This is a general, high-level statement of a policy that contains the following elements:

- An acknowledgment of the importance of the computing resources to the business model
- A statement of support for information security throughout the enterprise
- A commitment to authorize and manage the definition of the lower level standards, procedures, and guidelines

Senior Management Commitment

Fundamentally important to any security program’s success is the senior management’s high-level statement of commitment to the information security policy process, and a senior management’s understanding of how important security controls and protections are to the enterprise’s continuity. Senior management must be aware

of the importance of security implementation to preserve the organization's viability (and for their own "Due Care" protection), and must publicly support that process throughout the enterprise.

Regulatory. *Regulatory policies* are security policies that an organization is required to implement, due to compliance, regulation, or other legal requirements. These companies may be financial institutions, public utilities, or some other type of organization that operates in the public interest. These policies are usually very detailed and are specific to the industry in which the organization operates.

Regulatory policies commonly have two main purposes:

1. To ensure that an organization is following the standard procedures or base practices of operation in its specific industry.
2. To give an organization the confidence that they are following the standard and accepted industry policy.

Advisory. *Advisory policies* are security policies that are not mandated to be followed, but are strongly suggested, perhaps with serious consequences defined for failure to follow them (such as termination, a job action warning, and so forth). A company with such policies wants most employees to consider these policies mandatory. Most policies fall under this broad category.

These policies can have many exclusions or application levels. Thus, some employees can be more controlled by these policies than others, according to their roles and responsibilities within that organization. For example, a policy that requires a certain procedure for transaction processing may allow for an alternative procedure under certain, specified conditions.

Informative. *Informative policies* are policies that exist simply to inform the reader. There are no implied or specified requirements, and the audience for this information could be certain internal (within the organization) or external parties. This does not mean that the policies are authorized for public consumption, but that they are general enough to be distributed to external parties (vendors accessing an extranet, for example) without a loss of confidentiality.

However, penalties may be defined for the failure to follow a policy, such as the failure to follow a defined authorization procedure without stating what that policy is, and then referring the reader to another more detailed and confidential policy.

Standards, Guidelines, and Procedures

The next level down from policies is the three elements of policy implementation — *standards*, *guidelines*, and *procedures*. These three elements contain the actual details of the policy, such as how they should be implemented, and what standards and procedures should be used. They are published throughout the organization via manuals, the intranet, handbooks, or awareness classes.

It is important to know that standards, guidelines, and procedures are separate, yet linked, documents from the general policies (especially the senior-level statement). Unfortunately, companies will often create one document that satisfies the needs of all of these elements; this is not good. There are a few good reasons why they should be kept separate:

- Each one of these elements serves a different function, and focuses on a different audience. Also, physical distribution of the policies is easier.
- Security controls for confidentiality are different for each policy type. For example, a high-level security statement may need to be available to

investors, but the procedures for changing passwords should not be available to anyone that is not authorized to perform the task.

- Updating and maintaining the policy is much more difficult when all the policies are combined into one voluminous document. Mergers, routine maintenance, and infrastructure changes all require that the policies be routinely updated. A modular approach to a policy document will keep the revision time and costs down.

Standards. *Standards* specify the use of specific technologies in a uniform way. This standardization of operating procedures can be a benefit to an organization by specifying the uniform methodologies to be used for the security controls. Standards are usually compulsory and are implemented throughout an organization for uniformity.

Guidelines. *Guidelines* are similar to standards — they refer to the methodologies of securing systems, but they are recommended actions only, and are not compulsory. Guidelines are more flexible than standards, and take into consideration the varying nature of the information systems. Guidelines may be used to specify the way standards should be developed, for example, or to guarantee the adherence to general security principles. The Rainbow series, described in Appendix B, and the Common Criteria, discussed in Appendix G, are considered guidelines.

Procedures. *Procedures* embody the detailed steps that are followed to perform a specific task. Procedures are the detailed actions that personnel are required to follow. They are considered the lowest level in the policy chain. Their purpose is to provide the detailed steps for implementing the policies, standards, and guidelines, which were previously created. *Practices* is also a term that is frequently used in reference to procedures.

Baselines. We mention *baselines* here because they are similar to standards, yet are a little different. Once a consistent set of baselines has been created, the security architecture of an organization can be designed, and standards can then be developed. Baselines take into consideration the difference between various operating systems, for example, to assure that the security is being uniformly implemented throughout the enterprise. If adopted by the organization, baselines are compulsory.

Roles and Responsibilities

The phrase “roles and responsibilities” pops up quite frequently in InfoSec. InfoSec controls are often defined by the job or role an employee plays in an organization. Each of these roles has data security rights and responsibilities. Roles and responsibilities are central to the “separation of duties” concept — the concept that security is enhanced through the division of responsibilities in the production cycle. It is important that individual roles and responsibilities are clearly communicated and understood (see Table 1.2).

Role	Description
Senior Manager	Has the ultimate responsibility for security.
InfoSec Officer	Has the functional responsibility for security.
Owner	Determines the data classification.
Custodian	Preserves the information’s C.I.A.

Table 1.2: Roles and Responsibilities

Role	Description
User/Operator	Performs IAW the stated policies.
Auditor	Examines security.

All of the following concepts are fully defined in Chapter 6, “Operations Security,” but we discuss them briefly here:

Senior Management. Executive or senior-level management is assigned the overall responsibility for the security of information. Senior management may delegate the function of security, but they are viewed as the end of the food chain when liability is concerned.

Information Systems Security Professionals. Information systems security professionals are delegated the responsibility for implementing and maintaining security by the senior-level management. Their duties include the design, implementation, management, and review of the organization’s security policy, standards, guidelines, and procedures.

Data Owners. Previously discussed in the section titled “Information Classification Roles,” data owners are primarily responsible for determining the data’s sensitivity or classification levels. They can also be responsible for maintaining the information’s accuracy and integrity.

Users. Previously discussed in the section titled “Information Classification Roles,” users are responsible for following the procedures, which are set out in the organization’s security policy, during the course of their normal daily tasks.

Information Systems Auditors. Information systems auditors are responsible for providing reports to the senior management on the effectiveness of the security controls by conducting regular, independent audits. They also examine whether the security policies, standards, guidelines, and procedures are effectively complying with the company’s stated security objectives.

Risk Management

A major component of InfoSec is Risk Management (RM). Risk Management’s main function is to *mitigate* risk. Mitigating risk means to reduce the risk until it reaches a level that is acceptable to an organization. Risk Management can be defined as the identification, analysis, control, and minimization of loss that is associated with events.

The identification of risk to an organization entails defining the four following basic elements:

- The actual threat
- The possible consequences of the realized threat
- The probable frequency of the occurrence of a threat
- The extent of how confident we are that the threat will happen

Many formula and processes are designed to help provide some certainty when answering these questions. It should be pointed out, however, that because life and nature are constantly evolving and changing, not every possibility can be considered.

Risk Management tries as much as possible to see the future and to lower the possibility of threats impacting a company.

Note Mitigating Risk

It's important to remember that the risk to an enterprise can never be totally eliminated — that would entail ceasing operations. Risk Mitigation means finding out what level of risk the enterprise can safely tolerate and still continue to function effectively.

Principles of Risk Management

The Risk Management task process has several elements, primarily including the following:

- Performing a Risk Analysis, including the cost benefit analysis of protections
- Implementing, reviewing, and maintaining protections

To enable this process, some properties of the various elements will need to be determined, such as the value of assets, threats, and vulnerabilities, and the likelihood of events. A primary part of the RM process is assigning values to threats, and estimating how often, or likely, that threat will occur. To do this, several formulas and terms have been developed, and the CISSP candidate must fully understand them. The terms and definitions listed in the following section are ranked in the order that they are defined during the Risk Analysis (RA).

The Purpose of Risk Analysis

The main purpose of performing a Risk Analysis is to quantify the impact of potential threats — to put a price or value on the cost of a lost business functionality. The two main results of a Risk Analysis — the identification of risks and the cost/benefit justification of the countermeasures — are vitally important to the creation of a risk mitigation strategy.

There are several benefits to performing a Risk Analysis. It creates a clear cost-to-value ratio for security protections. It also influences the decision-making process dealing with hardware configuration and software systems design. In addition, it also helps a company to focus its security resources where they are needed most. Furthermore, it can influence planning and construction decisions, such as site selection and building design.

Terms and Definitions

The following are RA terms that the CISSP candidate will need to know.

Asset

An *asset* is a resource, process, product, computing infrastructure, and so forth that an organization has determined must be protected. The loss of the asset could affect C.I.A., confidentiality, integrity, availability, overall or it could have a discrete dollar value — it could be tangible or intangible. It could also affect the full ability of an organization to continue in business. The value of an asset is composed of all of the elements that are related to that asset — its creation, development, support, replacement, public credibility, considered costs, and ownership values.

Threat

Simply put, the presence of any potential event that causes an undesirable impact on the organization is called a *threat*. As we will discuss in the Operations Domain, a threat could be man-made or natural, and have a small or large effect on a company's security or viability.

Vulnerability

The absence or weakness of a safeguard constitutes a *vulnerability*. A minor threat has the potential to become a greater threat, or a more frequent threat, because of a vulnerability. Think of a vulnerability as the threat that gets through a safeguard into the system.

Combined with the terms asset and threat, vulnerability is the third part of an element that is called a *triple* in risk management.

Safeguard

A *safeguard* is the control or countermeasure employed to reduce the risk associated with a specific threat, or group of threats.

Exposure Factor (EF)

The *EF* represents the percentage of loss a realized threat event would have on a specific asset. This value is necessary to compute the Single Loss Expectancy (SLE), which in turn is necessary to compute the Annualized Loss Expectancy (ALE). The EF can be a small percentage, such as the effect of a loss of some hardware, or a very large percentage, such as the catastrophic loss of all computing resources.

Single Loss Expectancy (SLE)

An *SLE* is the dollar figure that is assigned to a single event. It represents an organization's loss from a single threat. It is derived from the following formula:

$$\text{Asset Value (\$)} \times \text{Exposure Factor (EF)} = \text{SLE}$$

For example, an asset valued at \$100,000 that is subjected to an exposure factor of 30 percent would yield an SLE of \$30,000. While this figure is primarily defined in order to create the Annualized Loss Expectancy (ALE), it is occasionally used by itself to describe a disastrous event for a Business Impact Assessment (BIA).

Annualized Rate of Occurrence (ARO)

The *ARO* is a number that represents the estimated frequency in which a threat is expected to occur. The range for this value can be from 0.0 (never) to a large number (for minor threats, such as misspellings of names in data entry). How this number is derived can be very complicated. It is usually created based upon the likelihood of the event and number of employees that could make that error occur. The loss incurred by this event is not a concern here, only how often it does occur.

For example, a meteorite damaging the data center could be estimated to occur only once every 100,000 years, and will have an ARO of .00001. Whereas 100 data entry operators attempting an unauthorized access attempt could be estimated at six times a year per operator, and will have an ARO of 600.

Annualized Loss Expectancy (ALE)

The *ALE*, a dollar value, is derived from the following formula:

$$\text{Single Loss Expectancy (SLE)} \times \text{Annualized Rate of Occurrence (ARO)} = \text{ALE}$$

In other words, an ALE is the annually expected financial loss to an organization from a threat. For example, a threat with a dollar value of \$100,000 (SLE) that is expected to happen only once in 1,000 years (ARO of .001) will result in an ALE of \$100. This helps to provide a more reliable cost versus benefit analysis. Remember that the SLE is

derived from the asset value and the Exposure Factor (EF). Table 1.3 shows these formulas.

Table 1.3: Risk Analysis Formulas	
Concept	Derivation Formula
Exposure Factor (EF)	% of asset loss caused by threat.
Single Loss Expectancy (SLE)	Asset Value x Exposure Factor (EF).
Annualized Rate of Occurrence (ARO)	Frequency of threat occurrence per year.
Annualized Loss Expectancy (ALE)	Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO).

Overview of Risk Analysis

We will now discuss the four basic elements of the Risk Analysis process:

1. Quantitative Risk Analysis
2. Qualitative Risk Analysis
3. Asset Valuation Process
4. Safeguard Selection

Quantitative Risk Analysis

The difference between quantitative and qualitative RA is fairly simple: Quantitative RA attempts to assign independently objective numeric values (hard dollars, for example) to the components of the risk assessment and to the assessment of potential losses. Qualitative RA addresses more intangible values of a data loss, and focuses on the other issues, rather than the pure hard costs.

When all elements (asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability) are measured, rated, and assigned values, the process is considered to be fully quantitative. However, fully quantitative risk analysis is not possible because qualitative measures must be applied. Thus, the reader should be aware that just because the figures look hard on paper does not mean it is possible to foretell the future with any certainty.

A quantitative risk analysis process is a major project, and as such it requires a project or program manager to manage the main elements of the analysis. A major part of the initial planning for the quantitative RA is the estimation of the time required to perform the analysis. In addition, a detailed process plan must also be created, and roles must be assigned to the RA team.

Preliminary Security Examination (PSE). A PSE is often conducted before the actual quantitative RA. The PSE helps to gather the elements that will be needed when the actual RA takes place. A PSE also helps to focus an RA. Elements that are defined during this phase include asset costs and values, a listing of various threats to an organization (in terms of threats to both the personnel and the environment), and documentation of the existing security measures. The PSE is normally then subject to a review by an organization's management before the RA begins.

Automated Risk Analysis Products

There are several good automated risk analysis products on the market. The main objectives of these products is to minimize the manual effort that must be expended to create the risk analysis and to provide a company with the ability to forecast its expected losses quickly with different input variations. The creation of a database during an initial automated process enables the operator to rerun the analysis using different parameters—to create a *what if* scenario. These products enable the users to perform calculations quickly in order to estimate future expected losses, thereby determining the benefit of their implemented safeguards.

Risk Analysis Steps

The three primary steps in performing a risk analysis are similar to the steps in performing a Business Impact Assessment (see Chapter 6, “Operations Security”). However, a risk analysis is commonly much more comprehensive and is designed to be used to quantify complicated, multiple-risk scenarios.

The three primary steps are as follows:

1. Estimate the potential losses to assets by determining their value.
2. Analyze potential threats to the assets.
3. Define the Annualized Loss Expectancy (ALE).

Estimate Potential Losses

To estimate the potential losses incurred during the realization of a threat, the assets must be valued by commonly using some sort of standard asset valuation process (this is described in more detail later). This results in an assignment of an asset’s financial value by performing the EF and the SLE calculations.

Analyze Potential Threats

Here we determine what the threats are, and how likely and often they are to occur. To define the threats, we must also understand the asset’s vulnerabilities and perform an ARO calculation for the threat and vulnerabilities.

All types of threats should be considered in this section, no matter if they seem likely or not. It may be helpful to organize the threat listing into the types of threats by source, or by their expected magnitude. In fact, some organizations can provide statistics on the frequency of various threats that occur in your area. In addition, the other domains of InfoSec discussed in this book have several varied listings of the categories of threats.

Some of the following categories of threats could be included in this section.

Data Classification. Data aggregation or concentration that results in data inference, covert channel manipulation, a malicious code/virus/Trojan horse/worm/logic bomb, or a concentration of responsibilities (lack of separation of duties)

Information Warfare. Technology-oriented terrorism, malicious code or logic, or emanation interception for military or economic espionage

Personnel. Unauthorized or uncontrolled system access, the misuse of technology by authorized users, tampering by disgruntled employees, or falsified data input

Application/Operational. Ineffective security application that results in procedural errors or incorrect data entry

Criminal. Physical destruction or vandalism, the theft of assets or information, organized insider theft, armed robbery, or physical harm to personnel

Environmental. Utility failure, service outage, natural disasters, or neighboring hazards

Computer Infrastructure. Hardware/equipment failure, program errors, operating system flaws, or a communications system failure

Delayed Processing. Reduced productivity or a delayed funds collection that results in reduced income, increased expenses, or late charges

Define the Annualized Loss Expectancy (ALE)

Once the SLE and ARO have been determined, we can estimate the ALE using the formula we previously described.

Results

After performing the Risk Analysis, the final results should contain the following:

- Valuations of the critical assets in hard costs
- A detailed listing of significant threats
- Each threat's likelihood and its possible occurrence rate
- Loss potential by a threat — the dollar impact the threat will have on an asset
- Recommended remedial measures and safeguards or countermeasures

Remedies

There are three generic remedies to risk, which may take the form of either one or a combination of the following three:

- *Risk Reduction.* Taking measures to alter or improve the risk position of an asset throughout the company
- *Risk Transference.* Assigning or transferring the potential cost of a loss to another party (like an insurance company)
- *Risk Acceptance.* Accepting the level of loss that will occur, and absorbing that loss

The remedy chosen will usually be the one that results in the greatest risk reduction, while retaining the lowest annual cost necessary to maintain a company.

Qualitative Risk Analysis

As we mentioned previously, a qualitative RA does not attempt to assign hard and fast costs to the elements of the loss. It is more scenario-oriented, and, as opposed to a quantitative RA, a purely qualitative risk analysis is possible. Threat frequency and impact data is required to do a qualitative RA, however.

In a qualitative risk assessment, the seriousness of threats and the relative sensitivity of the assets are given a ranking, or qualitative grading, by using a scenario approach, and creating an exposure rating scale for each scenario.

During a scenario description, we match various threats to identified assets. A scenario describes the type of threat and the potential loss to which assets, and selects the safeguards to mitigate the risk.

Qualitative Scenario Procedure

After the threat listing has been created, the assets for protection have been defined, and an exposure level rating is assigned, the qualitative risk assessment scenario begins. See Table 1.4 for a simple exposure rating scale.

Table 1.4: Simple Exposure Rating Level Scale
--

Rating Level	Exposure Percentage
Blank or 0	No measurable loss
1	20% loss
2	40% loss
3	60% loss
4	80% loss
5	100% loss

The procedures in performing the scenario are as follows:

- A scenario is written that addresses each major threat.
- The scenario is reviewed by business unit managers for a reality check.
- The RA team recommends and evaluates the various safeguards for each threat.
- The RA team works through each finalized scenario using a threat, asset, and safeguard.
- The team prepares their findings and submits them to management.

After the scenarios have all been played out and the findings are published, management must implement the safeguards that were selected as being acceptable, and begin to seek alternatives for the safeguards that did not work.

Asset Valuation Process

There are several elements of a process that determine the value of an asset. Both quantitative and qualitative RA (and Business Impact Assessment) procedures require a valuation made of the asset's worth to the organization. This valuation is a fundamental step in all security auditing methodologies. A common universal mistake made by organizations is not accurately identifying the information's value before implementing the security controls. This often results in a control that either is ill-suited for asset protection, not financially effective, or it protects the wrong asset. Table 1.5 discusses quantitative versus qualitative RA.

Property	Quantitative	Qualitative
Cost/benefit analysis	Yes	No
Financial hard costs	Yes	No
Can be automated	Yes	No
Guesswork involved	Low	High
Complex calculations	Yes	No
Volume of information required	High	Low
Time/work involved	High	Low
Ease of communication	High	Low

Reasons for Determining the Value of an Asset

Here are some additional reasons to define the cost or value that have been previously described:

- The asset valuation is necessary to perform the cost/benefit analysis.
- The asset's value may be necessary for insurance reasons.
- The asset's value supports safeguard selection decisions.
- The asset valuation may be necessary to satisfy "due care" and prevent negligence and legal liability.

Elements that Determine the Value of an Asset

There are three basic elements that are used to determine an information asset's value:

1. The initial and on-going cost (to an organization) of purchasing, licensing, developing, and supporting the information asset
2. The asset's value to the organization's production operations, research and development, and business model viability
3. The asset's value established in the external marketplace, and the estimated value of the intellectual property (trade secrets, patents, copyrights, and so forth)

Safeguard Selection Criteria

Once the risk analysis has been completed, safeguards and countermeasures must be researched and recommended. There are several standard principles that are used in the selection of safeguards to ensure that a safeguard is properly matched to a threat, and to ensure that a safeguard most efficiently implements the necessary controls. Important criterion must be examined before selecting an effective countermeasure.

Cost/Benefit Analysis

The number one safeguard selection criteria is the cost effectiveness of the control that is to be implemented, which is derived through the process of the cost versus benefit analysis. To determine the total cost of the safeguard, many elements need to be considered, which include the following:

- The purchase, development, and/or licensing costs of the safeguard
- The physical installation costs and the disruption to normal production during the installation and testing of the safeguard
- Normal operating costs, resource allocation, and maintenance/repair costs

The simplest calculation to compute a cost/benefit for a given safeguard is as follows:

(ALE before safeguard implementation) – (ALE after safeguard implementation) – (annual safeguard cost) = value of safeguard to the organization

For example, if an ALE of a threat has been determined to be \$10,000, the ALE after the safeguard implementation is \$1,000, and the annual cost to operate the safeguard totals \$500, then the value of a given safeguard is thought to be \$8,500 annually. This amount is then compared against the startup costs, and the benefit or lack of benefit is determined.

This value may be derived for a single safeguard, or can be derived for a collection of safeguards through a series of complex calculations. In addition to the financial cost-to-benefit ratio, other factors can influence the decision of whether to implement a specific security safeguard. For example, an organization is exposed to legal liability if the cost to implement a safeguard is less than the cost resulting from the threat realized and the organization does not implement the safeguard.

Level of Manual Operations

The amount of manual intervention required to operate the safeguard is also a factor in the choice of a safeguard. In case after case, vulnerabilities are created due to human error or an inconsistency in application. In fact, automated systems require fail-safe defaults to allow for manual shutdown capability in case a vulnerability occurs. The more automated a process is, the more sustainable and reliable that process will be.

In addition, a safeguard should not be too difficult to operate, and it should not unreasonably interfere with the normal operations of production. These characteristics are vital for the acceptance of the control by operating personnel, and for acquiring the all-important management support that is required for the safeguard to succeed.

Auditability and Accountability Features

The safeguard must allow for the inclusion of auditing and accounting functions. The safeguard must have the ability to be audited and tested by the auditors, and its accountability must be implemented to effectively track each individual who accesses the countermeasure or its features.

Recovery Ability

The safeguard's countermeasure should be evaluated in regard to its functioning state after activation or reset. During and after a reset condition, the safeguard must provide the following:

- No asset destruction during activation or reset
- No covert channel access to or through the control during reset
- No security loss or increase in exposure after activation or reset
- Defaults to a state that does not enable any operator access or rights until the controls are fully operational

Vendor Relations

The credibility, reliability, and past performance of the safeguard vendor must be examined. In addition, the openness (open source) of the application programming should also be known in order to avoid any design secrecy that prevents later modifications or allows unknown application to have back doors into the system. Vendor support and documentation should also be considered.

Back Doors

A back door, maintenance hook, or trap door is a programming element that enables application maintenance programmers access to the internals of the application, thereby bypassing the normal security controls of the application. While this is a valuable function for the support and maintenance of a program, the security practitioner must be aware of these doors and provide a means of control and accountability during their use.

Security Awareness

Although this is our last section for this chapter, it is not the least important. Security awareness is often an overlooked element of security management, because most of a security practitioner's time is spent on controls, intrusion detection, risk assessment, and proactively or reactively administering security.

However, it should not be that way. People are often the weakest link in a security chain, often because they are not trained or generally aware of what security is all about. Employees must understand how their actions, even seemingly insignificant actions, can greatly impact the overall security position of an organization.

Employees must be aware of the need to secure information and to protect the information assets of an enterprise. Operators need training in the skills that are required to fulfill their job functions securely, and security practitioners need training to implement and maintain the necessary security controls.

All employees need education in the basic concepts of security and its benefits to an organization. The benefits of the three pillars of security awareness training — awareness, training, and education — will manifest themselves through an improvement in the behavior and attitudes of personnel, and through a significant improvement in an enterprise's security.

Awareness

As opposed to training, security awareness refers to the general, collective awareness of an organization's personnel of the importance of security and security controls. In addition to the benefits and objectives we have previously mentioned, security awareness programs also have the following benefits:

- Make a measurable reduction in the unauthorized actions attempted by personnel
- Significantly increase the effectiveness of the protection controls
- Help to avoid the fraud, waste, and abuse of computing resources

Personnel are considered to be “security aware” when they clearly understand the need for security, and how security impacts viability and the bottom line, and the daily risks to computing resources.

It is important to have periodic awareness sessions to orient new employees and refresh senior employees. The material should always be direct, simple, and clear. It should be fairly motivational and should not contain a lot of techno-jargon, and should be conveyed in a style easily understood by the audience. The material should show how the security interests of the organization parallel the interest of the audience, and how they are important to the security protections.

Let's list a few ways that security awareness can be improved within an organization, and without a lot expense or resource drain.

- *Live/Interactive Presentations.* Lectures, video, and Computer Based Training (CBT)
- *Publishing/Distribution.* Posters, company newsletters, bulletins, and the intranet
- *Incentives.* Awards and recognition for security-related achievement
- *Reminders.* Login-banner messages, marketing paraphernalia such as mugs, pens, sticky notes, and mouse pads

One caveat here: It is possible to oversell security awareness and to inundate the personnel with a constant barrage of reminders. This will most likely have the effect of turning off their attention. It is important to find the right balance of selling security awareness. An awareness program should be creative and frequently altered to stay fresh.

Training and Education

Training is different from awareness in that it utilizes specific classroom or one-on-one training. The following types of training are related to InfoSec:

- Security-related job training for operators and specific users

- Awareness training for specific departments or personnel groups with security-sensitive positions
- Technical security training for IT support personnel and system administrators
- Advanced InfoSec training for security practitioners and information systems auditors
- Security training for senior managers, functional managers, and business unit managers

In-depth training and education for systems personnel, auditors, and security professionals is very important, and is considered necessary for career development. In addition, specific product training for security software and hardware is also vital to the protection of the enterprise.

A good starting point for defining a security training program could be the topics of policies, standards, guidelines, and procedures that are in use at an organization. A discussion of the possible environmental or natural hazards, or a discussion of the recent common security errors or incidents — without blaming anyone publicly — could work. Motivating the students is always the prime directive of any training, and their understanding of the value of the security's impact to the bottom line is also vital. A common training technique is to create hypothetical security vulnerability scenarios and to get the students' input on the possible solutions or outcomes.

The Need for User Security Training

All personnel using a system should have some kind of security training that is either specific to the controls employed or general security concepts. Training is especially important for those users who are handling sensitive or critical data. The advent of the microcomputer and distributed computing has created an opportunity for the serious failures of confidentiality, integrity, and availability.

Sample Questions

Answers to the Sample Questions for this and the other chapters are found in Appendix C.

1. Which formula accurately represents an Annualized Loss Expectancy (ALE) calculation? ?
 - A. MAN stands for Metropolitan Area Network
 - B. Asset Value (AV) x EF
 - C. ARO x EF – SLE
 - D. % of ARO x AV

2. What is an ARO? ?
 - A. A dollar figure that is assigned to a single event
 - B. The annual expected financial loss to an organization from a threat
 - C. A number that represents the estimated frequency of an occurrence of an expected threat
 - D. The percentage of loss a realized threat event would have on a specific asset

3. Which choice MOST accurately describes the difference between the role of a data owner versus the role of data custodian? ?
 - A. The custodian implements the information classification scheme after the initial assignment by the owner.
 - B. The data owner implements the information classification scheme after the initial assignment by the custodian.
 - C. The custodian makes the initial information classification assignments and the operations manager implements the scheme.
 - D. The custodian implements the information classification scheme after the initial assignment by the operations manager.

4. Which choice is NOT an accurate description of C.I.A.? ?
 - A. C stands for confidentiality

- B. I stands for integrity
C. A stands for availability
D. A stands for authorization
5. Which group represents the MOST likely source of an asset loss through inappropriate computer use? ?
- A. Crackers
B. Hackers
C. Employees
D. Saboteurs
6. Which choice is the BEST description of authentication as opposed to authorization? ?
- A. The means in which a user provides a claim of their identity to a system
B. The testing or reconciliation of evidence of a user's identity
C. A system's ability to determine the actions and behavior of a single individual within a system
D. The rights and permissions granted to an individual to access a computer resource
7. What is a noncompulsory recommendation on how to achieve compliance with published standards called? ?
- A. Procedures
B. Policies
C. Guidelines
D. Standards
8. Place the following four information classification levels in their proper order, from the least sensitive classification to the most sensitive. ?
- A. SBU
B. Top secret
C. Unclassified
D. Secret
9. How is an SLE derived? ?
- A. $(\text{Cost} - \text{benefit}) \times (\% \text{ of Asset Value})$
B. $\text{AV} \times \text{EF}$
C. $\text{ARO} \times \text{EF}$
D. $\% \text{ of AV} - \text{implementation cost}$

10. What are the detailed instructions on how to perform or implement a control called? ?
- A. Procedures
 - B. Policies
 - C. Guidelines
 - D. Standards
11. What the BEST description of risk reduction? ?
- A. Altering elements of the enterprise in response to a risk analysis
 - B. Removing all risk to the enterprise at any cost
 - C. Assigning any costs associated with risk to a third party
 - D. Assuming all costs associated with the risk internally
12. Which choice MOST accurately describes the differences between standards, guidelines, and procedures? ?
- A. Standards are recommended policies and guidelines are mandatory policies.
 - B. Procedures are step-by-step recommendations for complying with mandatory guidelines.
 - C. Procedures are the general recommendations for compliance with mandatory guidelines.
 - D. Procedures are step-by-step instructions for compliance with mandatory standards.
13. A purpose of a security awareness program is to improve ?
- A. The security of vendor relations
 - B. The performance of a company's intranet
 - C. The possibility for career advancement of the IT staff
 - D. The company's attitude about safeguarding data.
14. What is the MOST accurate definition of a safeguard? ?
- A. A guideline for policy

- recommendations
- B. A step-by-step instructional procedure
 - C. A control designed to counteract a threat
 - D. A control designed to counteract an asset
15. What does an Exposure Factor (EF) describe? ?
- A. A dollar figure that is assigned to a single event
 - B. A number that represents the estimated frequency of the occurrence of an expected threat
 - C. The percentage of loss a realized threat event would have on a specific asset
 - D. The annual expected financial loss to an organization from a threat
16. Which choice would be an example of a cost-effective way to enhance security awareness in an organization? ?
- A. Train every employee in advanced InfoSec
 - B. Create an award or recognition program for employees
 - C. Calculate the cost-to-benefit ratio of the asset valuations for a risk analysis
 - D. Train only managers in implementing InfoSec controls
17. What is the prime directive of Risk Management? ?
- A. Reduce the risk to a tolerable level
 - B. Reduce all risk regardless of cost
 - C. Transfer any risk to external third parties
 - D. Prosecute any employees that are violating published security policies
18. Which choice MOST closely depicts the difference between qualitative and quantitative risk analysis? ?
- A. A quantitative RA does not use

the hard costs of losses and a qualitative RA does.

- B. A quantitative RA uses less guesswork than a qualitative RA.
- C. A qualitative RA uses many complex calculations.
- D. A quantitative RA cannot be automated.

19. Which choice is NOT a good criteria for selecting a safeguard?

?

- A. The ability to recover from a reset with the permissions set to "allow all"
- B. Comparing the potential dollar loss of an asset to the cost of a safeguard
- C. The ability to recover from a reset without damaging the asset
- D. The accountability features for tracking and identifying operators

20. Which policy type is MOST likely to contain mandatory or compulsory standards?

?

- A. Guidelines
- B. Advisory
- C. Regulatory
- D. Informative

21. What are high-level policies?

?

- A. They are recommendations for procedural controls.
- B. They are the instructions on how to perform a Quantitative Risk Analysis.
- C. They are statements that indicate a senior management's intention to support InfoSec.
- D. They are step-by-step procedures to implement a safeguard.

Answers

1. *Answer:* a). b) is the formula for an SLE, and c) and d) are nonsense.

2. *Answer:* c). a) is the definition of SLE, b) is an ALE, and d) is

- an EF.
3. Answer: a).
 4. Answer: d).
 5. Answer: c). Internal personnel far and away constitute the largest amount of dollar loss due to unauthorized or inappropriate computer use.
 6. Answer: b). a) is identification, c) is accountability, and d) is authorization.
 7. Answer: c).
 8. Answer: c), a), d), and b).
 9. Answer: b). The other answers do not exist.
 10. Answer: a).
 11. Answer: a). b) is not possible or desirable, c) is risk transference, and d) is risk acceptance
 12. Answer: d). The other answers are faulty.
 13. Answer: d).
 14. Answer: c). a) is a guideline, b) is a procedure, and d) is nonsense
 15. Answer: c). a) is a SLE, b) is an ARO, and d) is a ALE
 16. Answer: b)
 17. Answer: a). Risk can never be eliminated, and Risk Management must find the level of risk the organization can tolerate and still function effectively.
 18. Answer: b). The other answers are incorrect.
 19. Answer: a). Permissions should be set to "deny all" during reset.
 20. Answer: c). Advisory policies might specify penalties for non-compliance, but regulatory policies are required to be followed by the organization. The other two are informational or recommended only.
 21. Answer: c). High-level policies are senior management statements of recognition of the importance of InfoSec controls.

Chapter 2: Access Control Systems

The information security professional should be aware of the access control requirements and their means of implementation to ensure a system's availability, confidentiality, and integrity. In the world of networked computers, this professional should understand the use of access control in distributed as well as centralized architectures.

The professional should also understand the threats, vulnerabilities, and risks which are associated with the information system's infrastructure, and the preventive and detective measures that are available to counter them.

Rationale

Controlling access to information systems and associated networks is necessary for the preservation of their *confidentiality, integrity, and availability*. Confidentiality assures that the information is not disclosed to unauthorized persons or processes. Integrity is addressed through the following three goals:

1. Prevention of the modification of information by unauthorized users.
2. Prevention of the unauthorized or unintentional modification of information by authorized users.
3. Preservation of the internal and external consistency.
 - a. Internal consistency ensures that internal data is consistent. For example, assume that an internal database holds the number of units of a particular item in each department of an organization. The sum of the number of units in each department should equal the total number of units that the database has recorded internally for the whole organization.
 - b. External consistency ensures that the data stored in the database is consistent with the real world. Using the example previously discussed in (a), external consistency means that the number of items recorded in the database for each department is equal to the number of items that physically exist in that department.

Availability assures that a system's authorized users have timely and uninterrupted access to the information in the system. The additional access control objectives are reliability and utility.

These and other related objectives flow from the organizational security policy. This policy is a high-level statement of management intent regarding the control of access to information and the personnel who are authorized to receive that information.

Three things that must be considered for the planning and implementation of access control mechanisms are the *threats* to the system, the system's *vulnerability* to these threats, and the *risk* that the threat may materialize. These concepts are further defined as follows:

- *Threat*. An event or activity that has the potential to cause harm to the information systems or networks.
- *Vulnerability*. A weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks.
- *Risk*. The potential for harm or loss to an information system or network; the probability that a threat will materialize.

Controls

Controls are implemented to mitigate risk and reduce the potential for loss. Controls can be *preventive*, *detective*, or *corrective*. Preventive controls are put in place to inhibit harmful occurrences; detective controls are established to discover harmful occurrences; corrective controls are used to restore systems that are victims of harmful attacks.

To implement these measures, controls can be *administrative*, *logical* or *technical*, and *physical*.

- Administrative controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.
- Logical or technical controls involve the restriction of access to systems and the protection of information. Examples of these types of controls are encryption, smart cards, access control lists, and transmission protocols.
- Physical controls incorporate guards and building security in general, such as the locking of doors, securing of server rooms or laptops, the protection of cables, the separation of duties, and the backing up of files.

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. *Assurance* procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

Models for Controlling Access

Controlling access by a *subject* (an active entity such as individual or process) to an *object* (a passive entity such as a file) involves setting up access rules. These rules can be classified into three categories or models:

Mandatory Access Control. The authorization of a subject's access to an object is dependent upon *labels*, which indicate the subject's *clearance*, and the *classification* or *sensitivity* of the object. For example, the military classifies documents as unclassified, confidential, secret, and top secret. Similarly, an individual can receive a clearance of confidential, secret, or top secret and can have access to documents classified at or below his/her specified clearance level. Thus, an individual with a clearance of secret can have access to secret and confidential documents with a restriction. This restriction is that the individual must have a *need to know* relative to the classified documents involved. Therefore, the documents must be necessary for that individual to complete an assigned task. Even if the individual is cleared for a classification level of information, unless there is a need to know, the individual should not access the information. *Rule-based* access control is a type of mandatory access control because this access is determined by rules (such as the correspondence of clearance labels to classification labels) and not by the identity of the subjects and objects alone.

Discretionary Access Control. The subject has authority, within certain limitations, to specify what objects can be accessible. For example, access control lists can be used. This type of access control is used in local, dynamic situations where the subjects must have the discretion to specify what resources certain users are permitted to access. When a user, within certain limitations, has the right to alter the access control to certain objects, this is termed as *user-directed* discretionary access control. An *identity-based* access control is a type of discretionary access control that is based on an

individual's identity. In some instances, a *hybrid* approach is used, which combines the features of user-based and identity-based discretionary access control.

Non-Discretionary Access Control. A central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on the individual's role in the organization (*role-based*) or the subject's responsibilities and duties (*task-based*). In an organization where there are frequent personnel changes, non-discretionary access control is useful because the access controls are based on the individual's role or title within the organization. These access controls do not need to be changed whenever a new person takes over that role. Another type of non-discretionary access control is *lattice-based* access control. In this type of control, a lattice model is applied. In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. To apply this concept to access control, the pair of elements is the subject and object, and the subject has the greatest lower bound and the least upper bound of access rights to an object.

Control Combinations

By combining preventive and detective controls, types with the administrative, technical (logical), and physical means of implementation, the following pairings are obtained:

- Preventive/administrative
- Preventive/technical
- Preventive/physical
- Detective/administrative
- Detective/technical
- Detective/physical

These six pairings and the key elements that are associated with their control mechanisms are discussed next.

Preventive/Administrative

In this pairing, emphasis is placed on "soft" mechanisms that support the access control objectives. These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks.

Preventive/Technical

The preventive/technical pairing uses technology to enforce access control policies. These technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units. Some typical preventive/technical controls are protocols, encryption, smart cards, biometrics (*for authentication*), local and remote access control software packages, call-back systems, passwords, constrained user interfaces, menus, shells, database views, limited keypads, and virus scanning software. *Protocols*, *encryption*, and *smart cards* are technical mechanisms for protecting information and passwords from disclosure. *Biometrics* apply technologies such as fingerprint, retina, and iris scans to authenticate individuals requesting access to resources, and *access control software packages* manage access to resources holding information from subjects local to the information system or from those at remote locations. *Callback* systems provide access protection by calling back the number of a previously authorized location, but this

control can be compromised by call forwarding. *Constrained user interfaces* limit the functions that can be selected by a user. For example, some functions may be “grayed-out” on the user menu and cannot be chosen. *Shells* limit the system-level commands that can be used by an individual or process. *Database views* are mechanisms that restrict the information that a user can access in a database. *Limited keypads* have a small number of keys that can be selected by the user. Thus, the functions that are intended not to be accessible by the user are not represented on any of the available keys.

Preventive/Physical

Many preventive/physical measures are intuitive. These measures are intended to restrict the physical access to areas with systems holding sensitive information. The area or zone to be protected is defined by a circular *security perimeter* that is under access control. Preventive/physical controls include fences, badges, multiple doors (a man-trap that consists of two doors physically separated so that an individual may be “trapped” in the space between the doors after entering one of the doors), magnetic card entry systems, biometrics (*for identification*), guards, dogs, environmental control systems (temperature, humidity, and so forth), and building and access area layout. Preventive/physical measures also apply to areas that are used for storage of the backup data files.

Detective/Administrative

Several detective/administrative controls overlap with preventive/administrative controls because they can be applied for prevention of future security policy violations or to detect existing violations. Examples of such controls are organizational policies and procedures, background checks, vacation scheduling, the labeling of sensitive materials, increased supervision, security awareness training, and behavior awareness. Additional detective/administrative controls are job rotation, the sharing of responsibilities, and reviews of audit records.

Detective/Technical

The detective/technical control measures are intended to reveal the violations of security policy using technical means. These measures include intrusion detection systems and automatically-generated violation reports from audit trail information. These reports can indicate variations from “normal” operation or detect known signatures of unauthorized access episodes. In order to limit the amount of audit information flagged and reported by automated violation analysis and reporting mechanisms, *clipping levels* can be set. Using clipping levels refers to setting allowable thresholds on a reported activity. For example, a clipping level of three can be set for reporting failed log-on attempts at a workstation. Thus, three or fewer log-on attempts by an individual at a workstation will not be reported as a violation, thus eliminating the need for reviewing normal log-on entry errors.

Due to the importance of the audit information, audit records should be protected at the highest level of sensitivity in the system.

Detective/Physical

Detective/physical controls usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists. Some of these control types are motion detectors, thermal detectors, and video cameras.

Identification and Authentication

Identification and authentication are the keystones of most access control systems. *Identification* is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system. Identification establishes user accountability for the actions on the system. *Authentication* is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time. Authentication is based on the following three factor types:

- *Type 1*. Something you know, such as a PIN or password
- *Type 2*. Something you have, such as an ATM card or smart card
- *Type 3*. Something you are (physically), such as a fingerprint or retina scan

Sometimes a fourth factor, something you do, is added to this list. Something you do may be typing your name or other phrases on a keyboard. Conversely, something you do can be considered as something you are.

Two-Factor Authentication refers to the act of requiring two of the three factors to be used in the authentication process. For example, withdrawing funds from an ATM machine requires a two-factor authentication in the form of the ATM card (something you have) and a PIN number (something you know).

Passwords

Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. This "*one-time password*" provides maximum security because a new password is required for each new log-on. A password that is the same for each log-on is called a *static password*. A password that changes with each log-on is termed a *dynamic password*. The changing of passwords can also fall between these two extremes. Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use. Obviously, the more times a password is used, the more chance there is of it being compromised. A *passphrase* is a sequence of characters that is usually longer than the allotted number for a password. The passphrase is converted into a virtual password by the system.

Tokens in the form of credit card-size memory cards or smart cards, or those resembling small calculators, are used to supply static and dynamic passwords.

These types of tokens are examples of something you have. An ATM card is a memory card that stores your specific information. Smart cards provide even more capability by incorporating additional processing power on the card. The following are the four types of smart cards:

- Static password tokens
 - The owner authenticates himself to the token.
 - The token authenticates the owner to an information system.
- Synchronous dynamic password tokens
 - The token generates a new unique password value at fixed time intervals (this password could be the time of day encrypted with a secret key).
 - The unique password is entered into a system or workstation along with an owner's PIN.
 - The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is valid and that it was entered during the valid time window.
- Asynchronous Dynamic password tokens
 - This scheme is similar to the synchronous dynamic password scheme, except the new password is

generated asynchronously and does not have to fit into a time window for authentication.

- Challenge-response tokens
 - A workstation or system generates a random challenge string and the owner enters the string into the token along with the proper PIN.
 - The token generates a response that is then entered into the workstation or system.
 - The authentication mechanism in the workstation or system then determines if the owner should be authenticated.

In all these schemes, a front-end authentication device and a back-end authentication server, which services multiple workstations or the host, can perform the authentication.

Biometrics

An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics are based on the Type 3 authentication mechanism — something you are. *Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.* In biometrics, *identification* is a “one-to-many” search of an individual’s characteristics from a database of stored images. *Authentication* in biometrics is a “one-to-one” search to verify a claim to an identity made by a person. *Biometrics is used for identification in physical controls and for authentication in logical controls.*

There are three main performance measures in biometrics. These measures are as follows:

- *False Rejection Rate (FRR) or Type I Error.* The percentage of valid subjects that are falsely rejected.
- *False Acceptance Rate (FAR) or Type II Error.* The percentage of invalid subjects that are falsely accepted.
- *Crossover Error Rate (CER).* The percent in which the False Rejection Rate equals the False Acceptance Rate.

Almost all types of detection permit a system’s sensitivity to be increased or decreased during an inspection process. If the system’s sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher FRR. Conversely, if the sensitivity is decreased, the FAR will increase. Thus, to have a valid measure of the system performance, the CER is used. These concepts are shown in Figure 2.1.

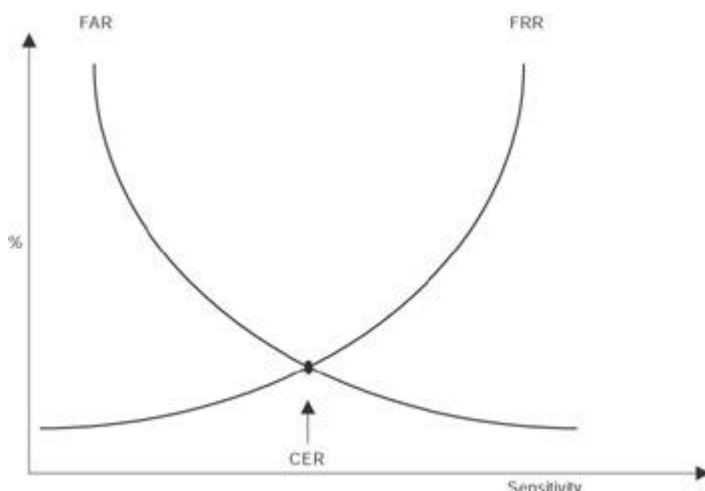


Figure 2.1: Crossover Error Rate (CER).

In addition to the accuracy of the biometric systems, there are other factors that must also be considered. These factors include the *enrollment time*, the *throughput rate*, and *acceptability*. Enrollment time is the time it takes to initially “register” with a system by providing samples of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes. For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases. In finger-scan technology, a full fingerprint is not stored — the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template. Finger-scan technology is used for one-to-one verification using smaller databases. Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.

The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a system. Acceptable throughput rates are in the range of 10 subjects per minute. Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece. Another concern would be the retinal pattern that could reveal changes in a person’s health, such as diabetes or high blood pressure.

The following are typical biometric characteristics that are used to uniquely authenticate an individual’s identity:

- Fingerprints
- Retina scans
- Iris scans
- Facial scans
- Palm scans
- Hand geometry
- Voice
- Handwritten signature dynamics

Single Sign-On (SSO)

Single Sign-On (SSO) addresses the cumbersome situation of logging on multiple times to access different resources. A user must remember numerous passwords and IDs and may take shortcuts in creating passwords that may be open to exploitation. In SSO, a user provides one ID and password per work session and is automatically logged-on to all the required applications. For SSO security, the passwords should not be stored or transmitted in the clear. SSO applications can run either on a user’s workstation or on authentication servers. The advantages of SSO include having the ability to use stronger passwords, easier administration of changing or deleting the passwords, and requiring less time to access resources. The major disadvantage of many SSO implementations is that once a user obtains access to the system through the initial log-on, the user can freely roam the network resources without any restrictions.

SSO can be implemented by using scripts that replay the users’ multiple log-ins, or by using authentication servers to verify a user’s identity and encrypted authentication tickets to permit access to system services.

Kerberos, SESAME, KryptoKnight, and NetSP are authentication server systems with operational modes that can implement SSO.

Kerberos

Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT. In Greek mythology, Kerberos is a three-headed dog that guards the entrance to the Underworld.

Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network of which a client requires services. The rationale and architecture behind Kerberos can be illustrated by using a university environment as an example. In such an environment, there are thousands of locations for workstations, local networks, and PC computer clusters. Client locations and computers are not secure, thus one cannot assume the cabling is secure. Messages, therefore, are not secure from interception. However, a few specific locations and servers can be secured and can serve as trusted authentication mechanisms for every client and service on that network. These centralized servers implement the Kerberos-trusted Key Distribution Center (KDC), Kerberos Ticket Granting Service (TGS), and Kerberos Authentication Service (AS). Windows 2000 provide Kerberos implementations.

The basic principles of Kerberos operation are as follows:

1. The KDC knows the secret keys of all clients and servers on the network.
2. The KDC initially exchanges information with the client and server by using these secret keys.
3. Kerberos authenticates a client to a requested service on a server through TGS, and by issuing temporary symmetric session keys for communications between the client and KDC, the server and the KDC, and the client and server.
4. Communication then takes place between the client and the server using those temporary session keys.

This detailed procedure will be explained using the Kerberos terminology and symbols as shown in Table 2.1.

Kerberos Item	Symbol
Client	C
Client secret key	K_C
Client network address	A
Server	S
Client/TGS session key	$K_{C, tgs}$
TGS secret key	K_{tgs}
Server secret key	K_S
Client/server session key	$K_{C, s}$
Client/TGS ticket	$T_{C, tgs}$
Client to server ticket	$T_{C, s}$
Client to server authenticator	$A_{C, s}$

Table 2.1: Kerberos Items and Symbols

Kerberos Item	Symbol
starting and ending time ticket is valid	V
Timestamp	T
M encrypted in secret key of x	[M] K _x
Ticket Granting Ticket	TGT
Optional, additional session key	Key

Kerberos Operation

The exchange of messages among the client, TGS Server, Authentication server, and the server that is providing the service is examined in more detail next.

Client-TGS Server: Initial Exchange

To initiate a request for service from a server (s), the user enters an ID and password on the client workstation. The client temporarily generates the client's secret key (K_c) from the password using a one-way hash function. (The one-way hash function performs a mathematical encryption operation on the password that cannot be reversed.) The client sends a request for authentication to the TGS server using the client's ID in the clear. Note that no password or secret key is sent. If the client is in the Authentication Server database, the TGS server returns a client/TGS session key (K_{c, tgs}) which is encrypted in the secret key of the client, and a Ticket Granting Ticket (TGT) encrypted in the secret key (K_{tgs}) of the TGS server. Thus, neither the client nor any other entity except the TGS server can read the contents of the TGT because K_{tgs} is known only to the TGS server. The TGT is comprised of the client ID, the client network address, the starting and ending time the ticket is valid (v), and the client/TGS session key. Symbolically, these initial messages from the TGS server to the client are represented as

$$[K_{c, tgs}]K_c$$

$$TGT = [c, a, v, K_{c, tgs}] K_{tgs}$$

The client decrypts the message containing the session key (K_{c, tgs}) with its secret key (K_c), and will now use this session key to communicate with the TGS server. Then the client erases its stored secret key to avoid compromising the secret key.

Client to TGS Server: Request for Service

When requesting access to a specific service on the network from the TGS server, the client sends two messages to the TGS server. In one message, the client submits the previously obtained TGT, which is encrypted in the secret key (K_{tgs}) of the TGS server, and an identification of the server (s) from which service is requested. The other message is an authenticator that is encrypted in the assigned session key (K_{c, tgs}). The authenticator contains the client ID, a timestamp, and an optional additional session key. These two messages are

$$TGT = s, [c, a, v, K_{c, tgs}] K_{tgs}$$

$$Authenticator = [c, t, key] K_{c, tgs}$$

TGS Server to Client: Issuing of Ticket for Service

After receiving a valid TGT and an authenticator from the client requesting a service, the TGS server issues a ticket ($T_{c,s}$) to the client that is encrypted in the server's secret key (K_s), and a client/server session key ($K_{c,s}$) that is encrypted in the client/TGS session key ($K_{c,tgs}$). These two messages are

Ticket $T_{c,s} = s, [c, a, v, K_{c,s}] K_s$

$[K_{c,s}] K_{c,tgs}$

Client to Server Authentication: Exchange and Providing of Service

To receive service from the server (s), the client sends the Ticket ($T_{c,s}$) and an authenticator to the server. The server decrypts the message with its secret key (K_s), and checks the contents. The contents contain the client's address, the valid time window (v), and the client/server session key ($K_{c,s}$), which will now be used for communication between the client and server. The server also checks the authenticator and, if that timestamp is valid, it provides the requested service to the client. The client messages to the server are

- Ticket $T_{c,s} = s, [c, a, v, K_{c,s}] K_s$
- Authenticator = $[c, t, key] K_{c,s}$

Kerberos Vulnerabilities

Kerberos addresses the confidentiality and integrity of information. It does not directly address availability and attacks such as frequency analysis. Furthermore, because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code. Replay can be accomplished on Kerberos if the compromised tickets are used within an allotted time window. Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.

The keys used in the Kerberos exchange are also vulnerable. A client's secret key is stored temporarily on the client workstation and can be compromised as well as the session keys that are stored at the client's computer and at the servers.

SESAME

To address some of the weaknesses in Kerberos, the Secure European System for Applications in a Multivendor Environment (SESAME) project uses public key cryptography for the distribution of secret keys and provides additional access control support. It uses the Needham-Schroeder protocol and a trusted authentication server at each host to reduce the key management requirements. SESAME employs the MD5 and crc32 one-way hash functions. In addition, SESAME incorporates two certificates or tickets. One certificate provides authentication as in Kerberos and the other certificate defines the access privileges that are assigned to a client. One weakness in SESAME is that it authenticates by using the first block of a message only and not the complete message. SESAME is also subject to password guessing like Kerberos.

KryptoKnight

The IBM KryptoKnight system provides authentication, SSO, and key distribution services. It was designed to support computers with widely varying computational capabilities. KryptoKnight uses a trusted Key Distribution Center (KDC) that knows the

secret key of each party. One of the differences between Kerberos and KryptoKnight is that there is a peer-to-peer relationship among the parties and the KDC. To implement SSO, the KDC has a party's secret key that is a one-way hash transformation of their password. The initial exchange from the party to the KDC is the user's name and a value, which is a function of a nonce (a randomly-generated one-time use authenticator) and the password. The KDC authenticates the user and sends the user a ticket encrypted with the user's secret key. This ticket is decrypted by the user and can be used for authentication to obtain services from other servers on the system. NetSP is a product that is based on KryptoKnight and uses a workstation as an authentication server. NetSP tickets are compatible with a number of access control services, including the Resource Access Control Facility (RACF).

Access Control Methodologies

Access control implementations are as diverse as their requirements. However, access control can be divided into two domains — centralized access control and decentralized/distributed access control. The mechanisms to achieve both types are summarized in the following sections.

Centralized Access Control

For dial-up users, the standard Remote Authentication and Dial-In User Service (*RADIUS*) can be used. RADIUS incorporates an authentication server and dynamic passwords. *Callback* can also be used. In *Callback*, a remote user dials in to the authentication server, provides an ID and password, and then hangs up. The authentication server looks up the caller's ID in a database of authorized users and obtains a phone number at a fixed location. Note that the remote user must be calling from that location. The authentication server then calls the phone number, the user answers, and then has access to the system. In some *Callback* implementations, the user must enter another password upon receiving a *Callback*. The disadvantage of this system is that the user must be at a fixed location whose phone number is known to the authentication server. A threat to *Callback* is that a cracker can arrange to have the call automatically forwarded to their number, enabling access to the system.

Another approach to remote access is the Challenge Handshake Authentication Protocol (*CHAP*). *CHAP* protects the password from eavesdroppers and supports the encryption of communication.

For networked applications, the Terminal Access Controller Access Control System (*TACACS*) employs a user ID and a static password for network access. *TACACS+* provides even stronger protection through the use of tokens for a two factor, dynamic password authentication.

Decentralized/Distributed Access Control

A powerful approach to controlling the access of information in a decentralized environment is through the use of databases. In particular, the relational model developed by E. F. Codd of IBM (circa 1970) has been the focus of much research in providing information security. Other database models include models that are hierarchical, network, object-oriented, and object-relational. The relational and object-relational database models support queries while the traditional file systems and the object-oriented database model do not support the use of queries. The object-relational and object-oriented models are better suited to managing complex data such as required for computer-aided design and imaging. Since the bulk of information security research and development has been focused on relational databases, this section will emphasize the relational model.

Relational Database Security

A relational database model has three parts:

- Data structures called tables or relations
- Integrity rules on allowable values and value combinations in the tables
- Operators on the data in the tables

A *database* can be defined as a persistent collection of interrelated data items. Persistency is obtained through the preservation of integrity and through the use of nonvolatile storage media. The description of the database is called a *schema*, and the schema is defined by a *Data Description Language (DDL)*. A *database management system (DBMS)* is the software that maintains and provides access to the database. For security, the DBMS can be set up so that only certain subjects are permitted to perform certain operations on the database. For example, a particular user can be restricted to certain information in the database and will not be allowed to view any other information.

A *relation* is the basis of a relational database and is represented by a two dimensional table. The rows of the table represent *records* or *tuples* and the columns of the table represent the *attributes*. The number of rows in the relation is referred to as the *cardinality* and the number of columns is the *degree*. The *domain* of a relation is the set of allowable values that an attribute can take. For example, a relation may be PARTS as shown in Table 2.2 or ELECTRICAL ITEMS as shown in Table 2.3.

Table 2.2: PARTS Relation

Part Number	Part Name	Part Type	Location
E2C491	Alternator	Electrical	B261
M4D326	Idle Gear	Mechanical	C418
E5G113	Fuel Gauge	Electrical	B561

Table 2.3: ELECTRICAL ITEMS Relation

Serial Number	Part Number	Part Name	Part Cost
S367790	E2C491	Alternator	\$200
S785439	E5D667	Control Module	\$700
S677322	E5W459	Window Motor	\$300

In each table, a *primary key* is required. A primary key is a unique identifier in the table that unambiguously points to an individual tuple or record in the table. A primary key is a subset of candidate keys within the table. A *candidate key* is an attribute that is a unique identifier within a given table. In Table 2.2, for example, the primary key would be the Part Number. If the Location of the part in Table 2.2 were unique to that part, it might be used as the primary key. Then, the Part Numbers and Locations would be

considered as candidate keys and the primary key would be taken from one of these two attributes. Now assume that the Part Number attributes in Table 2.2 are the primary keys. If an attribute in one relation has values matching the primary key in another relation, this attribute is called a *foreign key*. A foreign key does not have to be the primary key of its containing relation. For example, the Part Number attribute E2C491 in Table 2.3 is a foreign key because its value corresponds to the primary key attribute in Table 2.2.

Entity and Referential Integrity

Continuing with the example, if the Part Number was designated as the primary key in Table 2.2, then each row in the table must have a Part Number attribute. If the Part Number attribute is NULL, then *Entity Integrity* has been violated. Similarly, the *Referential Integrity* requires that for any foreign key attribute, the referenced relation must have a tuple with the same value for its primary key. Thus, if the attribute E2C491 of Table 2.3 is a foreign key of Table 2.2, then E2C491 must be a primary key in Table 2.2 to hold the referential integrity. Foreign key to primary key matches are important because they represent references from one relation to another and establish the connections among these relations.

Relational Database Operations

There are a number of operations in a relational algebra that are used to build relations and operate on the data. Five of these operations are primitives and the other operations can be defined in terms of those five. Some of the more commonly applied operations are discussed in greater detail later. The operations include

- Select (primitive)
- Project (primitive)
- Union (primitive)
- Difference (primitive)
- Product (primitive)
- Join
- Intersection
- Divide
- Views

For clarification, the Select operation defines a new relation based on a formula (for example, all the electrical parts whose cost exceed \$300 in Table 2.3). The Join operation selects tuples that have equal numbers for some attributes — for example, in Tables 2.2 and 2.3, Serial Numbers and Locations can be joined by the common Part Number. The Union operation forms a new relation from two other relations (for example, for relations that we call *X* and *Y*, the new relation consists of each tuple that is in either *X* or *Y* or both).

An important operation related to controlling the access of database information is the *View*. A *View* is defined from the operations of Join, Project, and Select. A *View* does not exist in a physical form and can be considered as a virtual table that is derived from other tables. These other tables could be tables that exist within the database or previously defined *Views*. A *View* can be thought of as a way to develop a table that is going to be frequently used even though it may not physically exist within the database. *Views* can be used to restrict access to certain information within the database, to hide attributes, and to implement content-dependent access restrictions. Thus, an individual requesting access to information within a database will be presented with a *View* containing the information that the person is allowed to see. The *View* will then hide the information that individual is not allowed to see. In this way, the *View* can be thought of as implementing *Least Privilege*.

In developing a query of the relational database, an optimization process is performed. This process includes generating query plans and selecting the best (lowest in cost) of the plans. A *query plan* is comprised of implementation procedures that correspond to each of the low-level operations in that query. The selection of the lowest cost plan involves assigning costs to the plan. Costs may be a function of disk accesses and CPU usage.

A bind is also applied in conjunction with a plan to develop a query. A *bind* is used to create the plan and fixes or resolves the plan. *Bind variables* are placeholders for literal values in a Structured Query Language (SQL) query being sent to the database on a server. The SQL statement is sent to the server for parsing and then, later, values are bound to the placeholders and sent separately to the server. This separate binding step is the origin of the term bind variable.

Data Normalization

Normalization is an important part of database design that ensures that attributes in a table depend only on the primary key. This process makes it easier to maintain data and have consistent reports.

Normalizing data in the database consists of three steps:

1. Eliminating any repeating groups by putting them into separate tables.
2. Eliminating redundant data (occurring in more than one table).
3. Eliminating attributes in a table which are not dependent on the primary key of that table.

SQL

Developed at IBM, SQL is a standard data manipulation and relational database definition language. The SQL Data Definition Language is used to create and delete views and relations (tables). SQL commands include Select, Update, Delete, Insert, Grant, and Revoke. The latter two commands are used in access control to Grant and Revoke privileges to resources. Usually, the owner of an object can withhold or transfer GRANT privileges related to an object to another subject. However, if the owner intentionally does not transfer the GRANT privileges, which are relative to an object to the individual A, A cannot pass on the GRANT privileges to another subject. In some instances, however, this security control may be circumvented. For example, if A copies the object, A essentially becomes the owner of that object and, thus, can transfer the GRANT privileges to another user, such as user B.

SQL security issues include the granularity of authorization and the number of different ways the same query may be executed.

Object-Oriented Data Bases (OODB)

Relational database models are ideal for business transactions where most of the information is in text form. Complex applications involving multimedia, computer-aided design, video, graphics, and expert systems are more suited to OODB. For example, OODB places no restrictions on the types or sizes of data elements as is the case with relational databases. OODB has the characteristics of ease of reusing code and analysis, reduced maintenance, and an easier transition from analysis of the problem to design and implementation. Its main disadvantages are a steep learning curve, even for

experienced traditional programmers, and high overhead of hardware and software required for development and operation.

Object-Relational Databases

The object-relational database is the marriage of object-oriented and relational technologies and combines the attributes of both. This model was introduced in 1992 with the release of the UniSQL/X unified relational and object-oriented database system. Hewlett Packard then released OpenODB (later called Oadapter), which extended its AllBase relational Database Management System.

Intrusion Detection

An Intrusion Detection System (IDS) is a system that is used to monitor network traffic or to monitor host audit logs in order to determine if any violations of an organization's security policy have taken place. An IDS can detect intrusions that have circumvented or passed through a firewall or are occurring within the local area network behind the firewall.

A truly effective IDS will detect common attacks as they are occurring, which includes distributed attacks. This type of IDS is called a *network-based* IDS because it monitors network traffic in real time. Conversely, a *host-based* IDS is resident on centralized hosts.

A Network-Based IDS

A network-based IDS usually provides reliable, real-time information without consuming network or host resources. A network-based IDS is passive while it acquires data. Because a network-based IDS reviews packets and headers, denial of service attacks can also be detected. Furthermore, because this IDS is monitoring an attack in real-time, it can also respond to an attack in progress to limit damage.

A problem with a network-based IDS system is that it will not detect attacks against a host made by an intruder who is logged in at the host's terminal. If a network IDS along with some additional support mechanism determines that an attack is being mounted against a host, it is usually not able to determine the type or effectiveness of the attack that is being launched.

A Host-Based IDS

A host-based IDS can review the system and event logs in order to detect an attack on the host and to determine if the attack was successful. (It is also easier to respond to an attack from the host.) Detection capabilities of host-based ID systems are limited by the incompleteness of most host audit log capabilities.

IDS Detection Methods

An IDS detects an attack through two major mechanisms — a signature-based ID or a statistical anomaly-based ID. These approaches are also termed Knowledge-based and Behavior-based ID, respectively, and are reinforced in Chapter 3, "Telecommunications and Network Security."

A Signature-Based ID

In a signature-based ID, signatures or attributes, which characterize an attack, are stored for reference. Then, when data about events are acquired from host audit logs or from network packet monitoring, this data is compared with the attack signature database. If there is a match, a response is initiated. A weakness of this approach is

the failure to characterize slow attacks that are extended over a long time period. To identify these types of attacks, large amounts of information must be held for extended time periods.

Another issue with signature-based ID is that only attack signatures that are stored in their database are detected.

A Statistical Anomaly-Based ID

With this method, an IDS acquires data and defines a “normal” usage profile for the network or host that is being monitored. This characterization is accomplished by taking statistical samples of the system over a period of normal use. Typical characterization information used to establish a normal profile includes memory usage, CPU utilization, and network packet types. With this approach, new attacks can be detected because they produce abnormal system statistics. Some disadvantages of a statistical anomaly-based ID are that it will not detect an attack that does not significantly change the system operating characteristics, or it may falsely detect a non-attack event that had caused a momentary anomaly in the system.

Some Access Control Issues

As discussed earlier in this chapter, the cost of access control must be commensurate with the value of the information that is being protected. The value of this information is determined through qualitative and quantitative methods. These methods incorporate factors such as the cost to develop or acquire the information, the importance of the information to an organization and its competitors, and the effect on the organization’s reputation if the information is compromised.

Access control must offer protection from an unauthorized, unanticipated, or unintentional modification of information. This protection should preserve the data’s internal and external consistency. The confidentiality of the information must also be similarly maintained and the information should be available on a timely basis. These factors cover the integrity, confidentiality, and availability components of information system security.

Accountability is another facet of access control. Individuals on a system are responsible for their actions. This accountability property enables system activities to be traced to the proper individuals. Accountability is supported by audit trails that record events on the system and network. Audit trails can be used for intrusion detection and for the reconstruction of past events. Monitoring individual activities, such as keystroke monitoring, should be accomplished in accordance with the company policy and appropriate laws. Banners at the log-on time should notify the user of any monitoring that is being conducted.

The following measures are used to compensate for both internal and external access violations:

- Backups
- RAID (Redundant Array of Independent Disks) technology
- Fault tolerance
- Business Continuity Planning
- Insurance

Sample Questions

1. The goals of integrity do NOT include ?
 - A. Accountability of responsible individuals
 - B. Prevention of the modification of information by unauthorized users
 - C. Prevention of the unauthorized or unintentional modification of information by authorized users
 - D. Preservation of internal and external consistency
2. Kerberos is an authentication scheme that can be used to implement ?
 - A. Public key cryptography
 - B. Digital signatures
 - C. Hash functions
 - D. Single Sign-On
3. The fundamental entity in a relational database is the ?
 - A. Domain
 - B. Relation
 - C. Pointer
 - D. Cost
4. In a relational database, security is provided to the access of data through ?
 - A. Candidate keys
 - B. Views
 - C. Joins
 - D. Attributes
5. In biometrics, a “one-to-one” search to verify an individual’s claim of an identity is called ?
 - A. Audit trail review
 - B. Authentication
 - C. Accountability
 - D. Aggregation
6. Biometrics is used for identification in the physical controls and for authentication in the ?
 - A. Detective controls
 - B. Preventive controls
 - C. Logical controls
 - D. Corrective controls
7. Referential Integrity requires that for any ?

foreign key attribute, the referenced relation must have

- A. A tuple with the same value for its primary key
 - B. A tuple with the same value for its secondary key
 - C. An attribute with the same value for its secondary key
 - D. An attribute with the same value for its other foreign key
8. A password that is the same for each log-on is called a ?
- A. Dynamic password
 - B. Static password
 - C. Passphrase
 - D. One-time pad
9. The number of times a password should be changed is NOT a function of ?
- A. The criticality of the information to be protected
 - B. The frequency of the password's use
 - C. The responsibilities and clearance of the user
 - D. The type of workstation used
10. The description of a relational database is called the ?
- A. Attribute
 - B. Record
 - C. Schema
 - D. Domain
11. A statistical anomaly-based intrusion detection system ?
- A. Acquires data to establish a normal system operating profile
 - B. Refers to a database of known attack signatures
 - C. Will detect an attack that does not significantly change the system's operating characteristics
 - D. Does not report an event that caused a momentary anomaly in the system

12. Intrusion detection systems can be all of the following types EXCEPT ?
- A. Signature-based
 - B. Statistical anomaly-based
 - C. Network-based
 - D. Defined-based
13. In a relational data base system, a primary key is chosen from a set of ?
- A. Foreign keys
 - B. Secondary keys
 - C. Candidate keys
 - D. Cryptographic keys
14. A standard data manipulation and relational database definition language is ?
- A. OOD
 - B. SQL
 - C. SLL
 - D. Script
15. An attack that can be perpetrated against a remote user's callback access control is ?
- A. Call forwarding
 - B. A Trojan horse
 - C. A maintenance hook
 - D. Redialing
16. The definition of CHAP is ?
- A. Confidential Hash Authentication Protocol
 - B. Challenge Handshake Authentication Protocol
 - C. Challenge Handshake Approval Protocol
 - D. Confidential Handshake Approval Protocol
17. Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network and facilitates communications through the assignment of ?
- A. Public keys
 - B. Session keys
 - C. Passwords
 - D. Tokens
18. Three things that must be considered for the planning and implementation of access control mechanisms are ?

- A. Threats, assets, and objectives
 B. Threats, vulnerabilities, and risks
 C. Vulnerabilities, secret keys, and exposures
 D. Exposures, threats, and countermeasures
19. In mandatory access control, the authorization of a subject to have access to an object is dependent upon ?
- A. Labels
 B. Roles
 C. Tasks
 D. Identity
20. The type of access control that is used in local, dynamic situations where subjects have the ability to specify what resources certain users may access is called ?
- A. Mandatory access control
 B. Rule-based access control
 C. Sensitivity-based access control
 D. Discretionary access control
21. Role-based access control is useful when ?
- A. Access must be determined by the labels on the data
 B. There are frequent personnel changes in an organization
 C. Rules are needed to determine clearances
 D. Security clearances must be used
22. Clipping levels are used to ?
- A. Limit the number of letters in a password
 B. Set thresholds for voltage variations
 C. Reduce the amount of data to be evaluated in audit logs
 D. Limit errors in callback systems
23. Identification is ?
- A. A user being authenticated by the system
 B. A user providing a password to

- the system
- C. A user providing a shared secret to the system
- D. A user professing an identity to the system
24. Authentication is ?
- A. The verification that the claimed identity is valid
- B. The presentation of a user's ID to the system
- C. Not accomplished through the use of a password
- D. Only applied to remote users
25. An example of two-factor authentication is ?
- A. A password and an ID
- B. An ID and a PIN
- C. A PIN and an ATM card
- D. A fingerprint
26. In biometrics, a good measure of performance of a system is the ?
- A. False detection
- B. Crossover Error Rate (CER)
- C. Positive acceptance rate
- D. Sensitivity
27. In finger scan technology, ?
- A. The full fingerprint is stored.
- B. Features extracted from the fingerprint are stored.
- C. More storage is required than in fingerprint technology.
- D. The technology is applicable to large one-to-many database searches.
28. An acceptable biometric throughput rate is ?
- A. One subject per two minutes
- B. Two subjects per minute
- C. Ten subjects per minute
- D. Five subjects per minute
29. In a relational database, the *domain* of a relation is the set of allowable values ?
- A. That an attribute can take
- B. That tuples can take
- C. That a record can take
- D. Of the primary key

30. Object-Oriented Database (OODB) systems:
- A. Are ideally suited for text-only information
 - B. Require minimal learning time for programmers
 - C. Are useful in storing and manipulating complex data such as images and graphics
 - D. Consume minimal system resources

?

Answers

1. *Answer: a).* Accountability is holding individuals responsible for their actions. Answers b, c and d are the three goals of integrity.
2. *Answer: d).* Kerberos is a third-party authentication protocol that can be used to implement single sign-on. Answer a is incorrect since public key cryptography is not used in the basic Kerberos protocol. Answer b is a public key-based capability, and answer c is a one-way transformation used to disguise passwords or to implement digital signatures.
3. *Answer: b).* The fundamental entity in a relational database is the relation in the form of a table. Answer a is the set of allowable attribute values and answers c and d are distractors.
4. *Answer: b).* Answer a, candidate keys, are the set of unique keys from which the primary key is selected. Answer c, Joins, are operations that can be performed on the database, and the attributes (d) denote the columns in the relational table.
5. *Answer: b).* Answer a is a review of audit system data, usually done after the fact. Answer c is holding individuals responsible for their actions, and answer d is obtaining higher sensitivity information from a number of pieces of information of lower sensitivity.
6. *Answer: c).* The other answers are different categories of controls where preventive controls attempt to eliminate or reduce vulnerabilities before an attack occurs; detective controls attempt to determine that an attack is taking place or has taken place; and corrective controls involve taking action to restore the system to normal operation after a successful attack.
7. *Answer: a).* Answers b and c are incorrect since a secondary key is not a valid term. Answer d is a distractor since referential integrity has a foreign key referring to a primary key in another relation.
8. *Answer: b).* In answer a, the password changes at each logon. For answer c, a passphrase is a long word or phrase that is converted by the system to a password. In answer d, a one-time pad refers to a using a random key only once when sending a cryptographic message.
9. *Answer: d).* The type of workstation used as the platform is not the determining factor. Items a, b and c are determining

- factors.
10. *Answer: c).* The other answers are portions of a relation or table.
 11. *Answer: a).* A statistical anomaly-based intrusion detection system acquires data to establish a normal system operating profile. Answer b is incorrect since it is used in signature-based intrusion detection. Answer c is incorrect since a statistical anomaly-based intrusion detection system will not detect an attack that does not significantly change the system operating characteristics. Similarly, answer d is incorrect since the statistical anomaly-based IDS is susceptible to reporting an event that caused a momentary anomaly in the system.
 12. *Answer: d).* All the other answers are types of IDS.
 13. *Answer: c).* Candidate keys by definition. Answer a is incorrect since a foreign key in one table refers to a primary key in another. Answer b is a made-up distractor and answer d refers to keys used in encipherment and decipherment.
 14. *Answer: b).* All other answers do not apply.
 15. *Answer: a).* A cracker can have a person's call forwarded to another number to foil the call back system. Answer b is incorrect since it is an example of malicious code embedded in useful code. Answer c is incorrect since it might enable bypassing controls of a system through means used for debugging or maintenance. Answer d is incorrect since it is a distractor.
 16. *Answer: b).*
 17. *Answer: b).* Session keys are temporary keys assigned by the KDC and used for an allotted period of time as the secret key between two entities. Answer a is incorrect since it refers to asymmetric encryption that is not used in the basic Kerberos protocol. Answer c is incorrect since it is not a key, and answer d is incorrect since a token generates dynamic passwords.
 18. *Answer: b).* Threats define the possible source of security policy violations, vulnerabilities describe weaknesses in the system that might be exploited by the threats, and the risk determines the probability of threats being realized. All three items must be present to meaningfully apply access control. Therefore, the other answers are incorrect.
 19. *Answer: a).* Mandatory access controls use labels to determine if subjects can have access to objects, depending on the subjects' clearances. Answer b, roles, is applied in non-discretionary access control as is answer c, tasks. Answer d, identity, is used in discretionary access control.
 20. *Answer: d).* Answers a and b require strict adherence to labels and clearances. Answer c is a made-up distractor.
 21. *Answer: b).* Role-based access control is part of non-discretionary access control. Answers a, c and d relate to mandatory access control.
 22. *Answer: c).* Reducing the amount of data to be evaluated, by definition. Answer a is incorrect since clipping levels do not relate to letters in a password. Answer b is incorrect since clipping levels in this context have nothing to do with

- controlling voltage levels. Answer d is incorrect since they are not used to limit call back errors.
- 23.** *Answer: d).* A user presents an ID to the system as identification. Answer a is incorrect since presenting an ID is not an authentication act. Answer b is incorrect since a password is an authentication mechanism. Answer c is incorrect since it refers to cryptography or authentication.
- 24.** *Answer: a).* Answer b is incorrect since it is an identification act. Answer c is incorrect since authentication can be accomplished through the use of a password. Answer d is incorrect since authentication is applied to local and remote users.
- 25.** *Answer: c).* These items are something you know and something you have. Answer a is incorrect since, essentially, only one factor is being used, something you know (password.) Answer b is incorrect for the same reason. Answer d is incorrect since only one biometric factor is being used.
- 26.** *Answer: b).* The other items are made-up distractors.
- 27.** *Answer: b).* The features extracted from the fingerprint are stored. Answer a is incorrect since the equivalent of the full fingerprint is not stored in finger scan technology. Answers c and d are incorrect since the opposite is true of finger scan technology.
- 28.** *Answer: c).*
- 29.** *Answer: a).*
- 30.** *Answer: c).* The other answers are false since for a., relational databases are ideally suited to text-only information, b. and d., OODB systems have a steep learning curve and consume a large amount of system resources .

Chapter 3: Telecommunications and Network Security

Overview

This section is the most detailed and comprehensive domain of study for the CISSP test. Although it is just one domain in the Common Book of Knowledge (CBK) of Information Systems Security, due to its size and complexity it is taught in two sections at the (ISC)² CISSP CBK Study Seminar.

From the published (ISC)² goals for the Certified Information Systems Security Professional candidate:

The professional should fully understand the following:

- *Communications and network security as it relates to voice, data, multimedia, and facsimile transmissions in terms of local area, wide area, and remote access*
- *Communications security techniques to prevent, detect, and correct errors so that integrity, availability, and the confidentiality of transactions over networks may be maintained*
- *Internet/intranet/extranet in terms of firewalls, routers, gateways, and various protocols*
- *Communications security management and techniques, which prevent, detect, and correct errors so that the integrity, availability, and confidentiality of transactions over networks may be maintained*

This is one reason why we feel the CISSP certification favors those candidates with engineering backgrounds, rather than say, auditing backgrounds. It is easier to learn the Legal, Risk Management, and Security Management domains if you have a science or engineering background than the reverse (that is, learning cryptology and telecommunications with a nonengineering or non-science background). While more advanced telecommunications or data communications specialists will find the domain to be rather basic, it is fairly comprehensive in its subject matter and in this case, can help fill in the gaps that a full-time, working engineer may have missed conceptually. And, of course, the focus here is security methodology: How does each element of Telecommunications (TC) and Data Communications affect the basic structure of Confidentiality, Integrity, and Availability (C.I.A.)? To that end, remember (as in every domain) that the purpose of the CBK seminar series and the CISSP test is not to teach or test a candidate on the latest and greatest technological advances in Telecommunications/Data Communications, but how standard Telecommunications/Data Communications practices affect InfoSec. Enclosed is an outline of recommended study areas for this domain. Even an advanced Telecommunications/Data Communications engineer must clearly understand these concepts and terminology.

Our Goals

We have divided this chapter into two sections: Management Concepts and Technology Concepts. These are the concepts a CISSP candidate needs to understand for the exam. We have laid out the areas of study so that you can quickly go to an area that you feel you need to brush up on, or you can “take it from the top” and read the chapter in this order:

The “Management Concepts” section examines the following areas:

- The C.I.A. Triad
- Remote Access Management

- Intrusion Detection and Response
 - Intrusion Detection Systems
 - Computer Incident Response Teams
- Network Availability
 - RAID
 - Backup Concepts
 - Managing Single Points of Failure
- Network Attacks and Abuses
- Trusted Network Interpretation (TNI)

In the “Technology Concepts” section, we will examine the following:

- Protocols
 - The Layered Architecture Concept
 - Open Systems Interconnect (OSI) Model
 - Transmission Control Protocol/Internet Protocol (TCP/IP) Model
 - Security-Enhanced and Security-Focused Protocols
- Firewall Types and Architectures
- Virtual Private Networks (VPN)
 - VPN Protocol Standards
 - VPN Devices
- Data Networking Basics
 - Data Network Types
 - Common Data Network Services
 - Data Networking Technologies
 - LAN Technologies
 - WAN Technologies
 - Remote Access Technologies
 - Remote Identification and Authentication Technologies

Domain Definition

The Telecommunications and Network Security domain includes the structures, transmission methods, transport formats, and security measures that are used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media. This domain is the information security domain that is concerned with protecting data, voice and video communications, and ensuring the following:

Confidentiality. Making sure that only those who are supposed to access the data can access it. Confidentiality is the opposite of “disclosure.”

Integrity. Making sure that the data has not been changed unintentionally, due to an accident or malice. Integrity is the opposite of “alteration.”

Availability. Making sure that the data is accessible when and where it is needed. Availability is the opposite of “destruction.”

The Telecommunications Security Domain of information security is also concerned with the prevention and detection of the misuse or abuse of systems, which poses a threat to the tenets of Confidentiality, Integrity, and Availability (C.I.A.).

Management Concepts

This section describes the function of the Telecommunications and Network Security management. This includes the management of networks, communications systems, remote connections, and security systems.

The C.I.A. Triad

The fundamental information systems security concept of C.I.A. relates to the Telecommunications domain in the following three ways.

Confidentiality

Confidentiality is the prevention of the intentional or unintentional unauthorized disclosure of contents. Loss of confidentiality can occur in many ways. For example, loss of confidentiality can occur through the intentional release of private company information or through a misapplication of network rights.

Some of the elements of telecommunication used to ensure confidentiality are

- Network security protocols
- Network authentication services
- Data encryption services

Integrity

Integrity is the guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered. Loss of integrity can occur either through an intentional attack to change information (for example, a web site defacement) or, by the most common type: data is altered accidentally by an operator. Integrity also contains the concept of *nonrepudiation* of a message source, which will be described later.

Some of the elements used to ensure integrity are

- Firewall services
- Communications Security Management
- Intrusion detection services

Availability

This concept refers to the elements that create reliability and stability in networks and systems, which assures that connectivity is accessible when needed, allowing authorized users to access the network or systems. Also included in that assurance is the guarantee that security services for the security practitioner are usable when they are needed. The concept of availability also tends to include areas in the Information Systems that are traditionally not thought of as pure security (such as guarantee of service, performance, and up-time), yet are obviously affected by an attack like a Denial of Service (DoS).

Some of the elements that are used to ensure availability are

- Fault tolerance for data availability, such as backups and redundant disk systems
- Acceptable log-ins and operating process performances
- Reliable and interoperable security processes and network security mechanisms

You should also know another point about availability: The use of ill-structured security mechanisms can also affect availability. Over-engineered or poorly designed security systems can impact the performance of a network or system as seriously as an

intentional attack. The C.I.A. triad is often represented by a triangle, as shown in Figure 3.1.

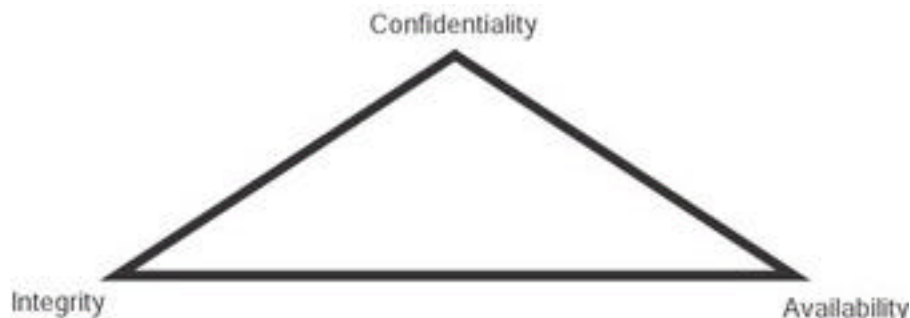


Figure 3.1: The C.I.A. triad.

Remote Access Security Management

Remote Access Security Management (RASM) is defined as the management of the elements of the technology of remote computing. Several current remote computing technologies confront a security practitioner:

- Dial-Up, Async, and Remote Internet Connectivity
 - Digital Subscriber Line (xDSL)
 - Integrated Services Digital Network (ISDN)
 - Wireless computing — mobile and cellular computing, and Personal Digital Assistants (PDAs)
 - Cable modems
- Securing Enterprise and Telecommuting Remote Connectivity
 - Securing external connections (such as Virtual Private Networks (VPNs), Secure Sockets Layer (SSL), Secure Shell (SSH-2), and so forth)
 - Remote access authentication systems (such as RADIUS and TACACS)
 - Remote node authentication protocols (such as Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP))
- Remote User Management Issues
 - Justification for and the validation of the use of remote computing systems
 - Hardware and software distribution
 - User support and remote assistance issues

Intrusion Detection (ID) and Response

Intrusion Detection (ID) and Response is the task of monitoring systems for evidence of an intrusion or an inappropriate usage. This includes notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects. This is not a preventative function. It exists after the fact of intrusion (which it detects) and entails the following two major concepts:

- Creation and maintenance of intrusion detection systems and processes for the following:
 - Host or network monitoring
 - Event notification
- Creation of a Computer Incident Response Team (CIRT) for the following:
 - Analysis of an event notification
 - Response to an incident if the analysis warrants it
 - Escalation path procedures

- Resolution, post-incident follow-up, and reporting to the appropriate parties

ID Systems

Various types of Intrusion Detection Systems exist from many vendors. A CISSP candidate should remember the two fundamental variations on the way they work: a) network- vs. host-based systems, and b) knowledge- vs. behavior-based systems. A short description of the differences has been provided, along with some of the pros and cons of each.

Network- vs. Host-Based ID Systems

The two most common implementations of Intrusion Detection are Network-based and Host-based. Their differences are as follows:

- Network-based ID systems
 - Commonly reside on a discrete network segment and monitor the traffic on that network segment
 - Usually consist of a network appliance with a Network Interface Card (NIC) that is operating in promiscuous mode and is intercepting and analyzing the network packets in real time
- Host-based ID systems
 - Use small programs (intelligent agents), which reside on a host computer, and monitor the operating system continually
 - Write to log files and trigger alarms
 - Detect inappropriate activity only on the host computer — they do not monitor the entire network segment

Knowledge- vs. Behavior-Based ID Systems

The two current conceptual approaches to Intrusion Detection methodology are knowledge-based ID systems and behavior-based ID systems, sometimes referred to as signature-based ID and statistical anomaly-based ID, respectively.

Knowledge-based ID. Systems use a database of previous attacks and known system vulnerabilities to look for current attempts to exploit their vulnerabilities, and trigger an alarm if an attempt is found. These systems are more common than behavior-based ID systems.

The following are the advantages of a knowledge-based ID system:

- This system is characterized by low false alarm rates (or positives).
- Their alarms are standardized and are clearly understandable by security personnel.

The following are the disadvantages of knowledge-based ID systems:

- This system is resource-intensive — the knowledge database continually needs maintenance and updates.
- New, unique, or original attacks often go unnoticed.

Behavior-based ID. Systems dynamically detect deviations from the learned patterns of user behavior and an alarm is triggered when an activity is considered intrusive

(outside of normal system use) occurs. Behavior-based ID systems are less common than knowledge-based ID systems.

The following are the advantages of a behavior-based ID system:

- The system can dynamically adapt to new, unique, or original vulnerabilities.
- A behavior-based ID system is not as dependent upon specific operating systems as a knowledge-based ID system.

The following are the disadvantages of a behavior-based ID system:

- The system is characterized by high false alarm rates. High positives are the most common failure of ID systems and can create data noise that makes the system unusable.
- The activity and behavior of the users while in the networked system may not be static enough to effectively implement a behavior-based ID system.

Note Remember: Intrusion detection is Detective rather than Preventative.

Computer Incident Response Team

As part of a structured program of Intrusion Detection and Response, a Computer Emergency Response Team (CERT) or Computer Incident Response Team (CIRT) is commonly created. As “CERT” is copyrighted, “CIRT” is more often used.

The prime directive of every CIRT is *Incident Response Management*, which manages a company’s response to events that pose a risk to their computing environment.

This management often consists of the following:

- Coordinating the notification and distribution of information pertaining to the incident to the appropriate parties (those with a need to know) through a predefined escalation path
- Mitigating risk to the enterprise by minimizing the disruptions to normal business activities and the costs associated with remediating the incident (including public relations)
- Assembling teams of technical personnel to investigate the potential vulnerabilities and to resolve specific intrusions

Additional examples of CIRT activities are

- Management of the network logs, including collection, retention, review, and analysis of data
- Management of the resolution of an incident, management of the remediation of a vulnerability, and post-event reporting to the appropriate parties

Network Availability

This section defines those elements that can provide for or threaten network availability. Network availability can be defined as an area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability. Later we will examine the areas of these networks that are required to provide redundancy and fault tolerance. A more techno-focused description of these topologies and devices can be found in the “Technology Concepts” section later in this chapter.

Now we will examine the following:

- RAID
- Backup concepts
- Managing single points of failure

RAID

RAID stands for the *Redundant Array of Inexpensive Disks*. It is also commonly referred to as the Redundant Array of Independent Disks. Its primary purpose is to provide fault tolerance and protection against file server hard disk crashes. Some RAID types secondarily improve system performance by caching and distributing disk reads from multiple disks that work together to save files simultaneously. Basically, RAID separates the data into multiple units and stores it on multiple disks by using a process called “striping”. It can be implemented either as a hardware or a software solution, but as we will see in the following “Hardware vs. Software” section, each type of implementation has its own issues and benefits.

The RAID Advisory Board has defined three classifications of RAID: Failure Resistant Disk Systems (FRDSs), Failure Tolerant Disk Systems, and Disaster Tolerant Disk Systems. As of this writing only the first one, FRDS, is an existing standard, and the others are still pending. We will now discuss the various implementation levels of an FRDS.

Failure Resistant Disk System

The basic function of an FRDS is to protect file servers from data loss and a loss of availability due to disk failure. It provides the ability to reconstruct the contents of a failed disk onto a replacement disk and provides the added protection against data loss due to the failure of many hardware parts of the server. One feature of an FRDS is that it enables the continuous monitoring of these parts and the alerting of their failure.

Failure Resistant Disk System Plus

An update to the FRDS standard is called FRDS+. This update adds the ability to automatically *hot swap* (swapping while the server is still running) failed disks. It also adds protection against environmental hazards (such as temperature, out-of-range conditions, and external power failure) and includes a series of alarms and warnings of these failures.

Overview of the Ten Levels of RAID

RAID Level 0 creates one large disk by using several disks. This process is called *striping*. It stripes data across all disks (but provides no redundancy) by using all of the available drive space to create the maximum usable data volume size and to increase the read/write performance. One problem with this level of RAID is that it actually lessens the fault tolerance of the disk system rather than increasing it — the entire data volume is unusable if one drive in the set fails.

RAID Level 1 is commonly called *mirroring*. It mirrors the data from one disk or set of disks by duplicating the data onto another disk or set of disks. This is often implemented by a one-for-one disk to disk ratio: Each drive is mirrored to an equal drive partner that is continually being updated with current data. If one drive fails, the system automatically gets the data from the other drive. The main issue with this level of RAID is that the one-for-one ratio is very expensive — resulting in the highest cost per megabyte of data capacity. This level effectively doubles the amount of hard drives you need, therefore it is usually best for smaller capacity systems.

RAID Level 2 consists of bit-interleaved data on multiple disks. The parity information is created using a *hamming code* that detects errors and establishes which part of which drive is in error. It defines a disk drive system with 39 disks: 32 disks of user storage

and seven disks of error recovery coding. This level is not used in practice and was quickly superseded by the more flexible levels of RAID that follow.

RAID Levels 3 and 4 are discussed together because they function in the same way. The only difference is that level 3 is implemented at the *byte level* and level 4 is usually implemented at the *block level*. In this scenario, data is striped across several drives and the parity check bit is written to a dedicated parity drive. This is similar to RAID 0. They both have a large data volume, but the addition of a dedicated parity drive provides redundancy. If a hard disk fails, the data can be reconstructed by using the bit information on the parity drive. The main issue with this level of RAID is that the constant writes to the parity drive can create a performance hit. In this implementation, spare drives can be used to replace crashed drives.

RAID Level 5 stripes the data and the parity information at the block level across all the drives in the set. It is similar to RAID 3 and 4 except that the parity information is written to the next available drive rather than to a dedicated drive by using an *interleave* parity. This enables more flexibility in the implementation and increases fault tolerance as the parity drive is not a single point of failure, as it is in RAID 3 or 4. The disk reads and writes are also performed concurrently, thereby increasing performance over levels 3 and 4. The spare drives that replace the failed drives are usually hot swappable, meaning they can be replaced on the server while the system is up and running. This is probably the most popular implementation of RAID today.

RAID Level 7 is a variation of RAID 5 wherein the array functions as a *single virtual disk* in the hardware. This is sometimes simulated by software running over a RAID level 5 hardware implementation. This enables the drive array to continue to operate if any disk or any path to any disk fails. It also provides parity protection.

Various other implementations of RAID are created by vendors to combine the features of several RAID levels, although these levels are not officially defined. Level 10 is created by combining level 0 (striping) with level 1 (mirroring). Level 6 is created by combining level 1 (mirroring) with level 5 (interleave). Table 3.1 shows the various levels of RAID with terms you will need to remember.

RAID Level	Description
0	Striping
1	Mirroring
2	Hamming Code Parity
3	Byte Level Parity
4	Block Level Parity
5	Interleave Parity
7	Single Virtual Disk

Hardware vs. Software RAID

RAID can be implemented in either hardware or software. Each type has its own issues and benefits. A hardware RAID implementation is usually platform-independent. It runs below the operating system (OS) of the server and usually does not care if the OS is Novell, NT, or Unix. The hardware implementation uses its own Central Processing Unit (CPU) for calculations on an intelligent controller card. There can be more than one of these cards installed to provide hardware redundancy in the server. RAID levels 3 and 5 run faster on hardware. A software implementation of RAID means it runs as part of the operating system on the file server. Often RAID levels 0, 1, and 10 run faster on software RAID because of the need for the server's software resources. Simple striping or mirroring can run faster in the operating system because neither use the hardware-level parity drives.

Other Types of Server Fault Tolerant Systems

Redundant Servers. A redundant server implementation takes the concept of RAID 1 (mirroring) and applies it to a pair of servers. A primary server mirrors its data to a secondary server, thus enabling the primary to “rollover” to the secondary in the case of primary server failure (the secondary server steps in and takes over for the primary server). This rollover can be hot or warm (that is, the rollover may or may not be transparent to the user), depending upon the vendor's implementation of this redundancy. This is also commonly known as *server fault tolerance*. Common vendor implementations of this are Novell's SFTIII, Octopus, and Vinca's Standby Server. Figure 3.2. shows a common redundant server implementation.

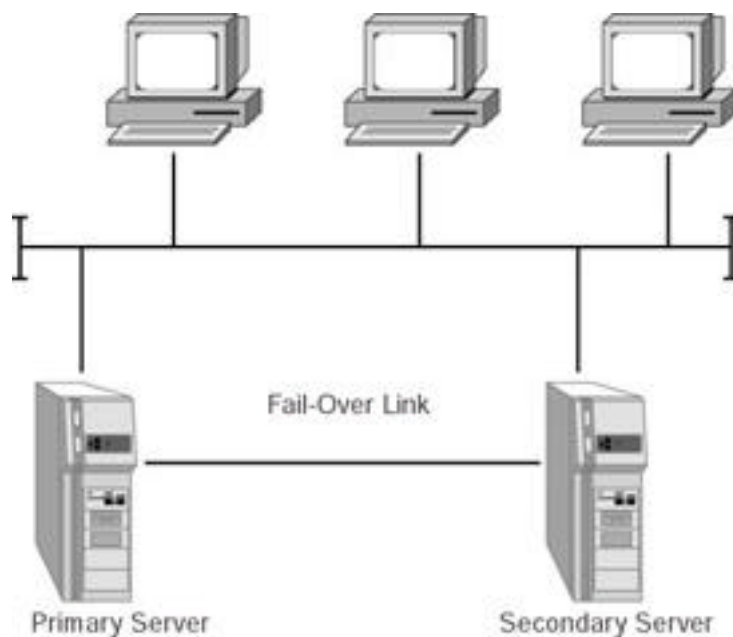


Figure 3.2: Redundant servers.

Server Clustering. A server cluster is a group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability. The concept of server clustering is similar to the redundant server implementation previously discussed except that all the servers in the cluster are on-line and take part in processing service requests. By enabling the secondary servers to provide processing time, the cluster acts as an intelligent entity and balances the traffic load to improve performance. The cluster looks like a single server from the user's point of view. If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a “server farm.” Examples of this type of vendor

implementation are Microsoft Cluster Server (“Wolfpack”), Oracle Parallel Server, and Tandem NonStop. Figure 3.3 shows a type of server clustering.

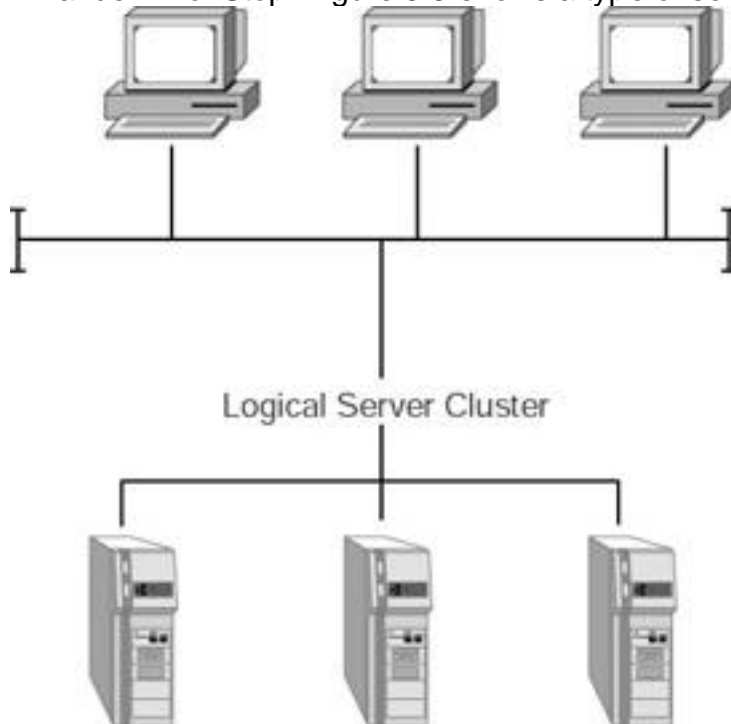


Figure 3.3: Server clustering.

Backup Concepts

A CISSP candidate will also need to know the basic concepts of data backup. The candidate may be presented with questions regarding file selection methods, tape format types, and common problems.

Tape Backup Methods

The purpose of a tape backup method is to protect and/or restore lost, corrupted, or deleted information, thereby preserving the data integrity and ensuring network availability.

There are several varying methods of selecting files for backup. Some have odd names, like Grandfather/Father/Son, Towers of Hanoi, and so forth. The three most basic common methods are as follows:

1. *Full Backup Method.* This backup method makes a complete backup of every file on the server every time it is run. The method is primarily run when time and tape space permits, and is used for system archive or baselined tape sets.
2. *Incremental Backup Method.* This backup method only copies files that have been recently added or changed (that day) and ignores any other backup set. It is usually accomplished by resetting the archive bit on the files after they have been backed up. This method is used if time and tape space is at an extreme premium. However, this method has some inherent vulnerabilities, which will be discussed later.
3. *Differential Backup Method.* This backup method only copies files that have changed since a full backup was last performed. This type of backup is additive because

the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup. In this scenario, each file's archive bit is not reset until the next full backup.

Note A Full Backup must be made regardless of whether Differential or Incremental methods are used.

Backup Method Example

A full backup was made on Friday night. This full backup is just what it says; it copied every file on the file server to the tape regardless of the last time any other backup was made. This type of backup is common for creating full copies of the data for off-site archiving or in preparation for a major system upgrade. On Monday night, another backup is made. If the site uses the Incremental Backup Method, Monday, Tuesday, Wednesday, and Thursday's backup tapes contain only those files that were altered during that day (Monday's incremental backup tape has only Monday's data on it, Tuesday's backup tape has only Tuesday's on it, and so on). All backup tapes may be required to restore a system to its full state after a system crash because some files that changed during the week may only exist on one tape. If the site is using the Differential Backup Method, Monday's tape backup has the same files that the Incremental's tape has (Monday is the only day that the files have changed so far). However, on Tuesday, rather than only backing up that day's files, it also backs up Monday's files, creating a longer back up. Although this increases the time required to do the backup and the amount of tapes needed, it does provide more protection from tape failure and speeds up recovery time.

Tape Format Types

The following are the four most common backup tape format technologies:

1. *Digital Audio Tape (DAT)*. Digital Audio Tape can be used to backup data systems in addition to its original intended audio uses.
2. *Quarter Inch Cartridge drives (QIC)*. This format is mostly used for home/small office backups, has a small capacity, and is slow, but inexpensive.
3. *8mm Tape*. This format is commonly used in Helical Scan tape drives, but was superseded by Digital Linear Tape (DLT).
4. *Digital Linear Tape (DLT)*. The tape is 4mm in size, yet the compression techniques and head scanning process make it a large capacity and fast tape.

The criteria for selecting which of these tape formats to use is usually based upon a comparison of the trade-off of performance vs. capacity vs. cost. The bottom line is: How big is the data that you need to backup and how long can you operate until it is recovered? Table 3.2 is a quick reference of the major types of backup tape formats.

Table 3.2: Tape Format Technology Comparison

Properties	DAT	QIC	8mm	DLT
Capacity	4GB/12GB	13GB	20GB	20/35GB

Table 3.2: Tape Format Technology Comparison

Properties	DAT	QIC	8mm	DLT
Max. Transfer Rate	1MBps	1.5MBps	3MBps	5MBps
Cost	Medium	Low	Medium	High

Other Backup Media

Compact Disk (CD) optical media types. Write-once, read-many (WORM) optical disk “jukeboxes” are used for archiving data that does not change. This is a very good format to use for a permanent backup. This format is used by companies to store data in an accessible format that may need to be accessed at a much later date, such as legal data. The shelf life of a CD is also longer than tape. Rewritable and erasable (CDR/W) optical disks are sometimes used for backups that require short time storage for changeable data, but require faster file access than tape. This format is used more often for very small data sets.

Zip/Jaz drives, SyQuest, and Bernoulli boxes. These types of drives are frequently used for the individual backups of small data sets of specific application data. These formats are very transportable and are often the standard for data exchange in many businesses.

Tape Arrays. A Tape Array is a large hardware/software system that uses the RAID technology we discussed earlier. It uses a large device with multiple (sometimes 32 or 64) tapes that are configured as a single array. These devices require very specific hardware and software to operate, but provide a very fast backup and a multi-tasking backup of multiple targets with considerable fault tolerance.

Hierarchical Storage Management (HSM). HSM provides a continuous on-line backup by using optical or tape “jukeboxes,” similar to WORMs. It appears as an infinite disk to the system, and can be configured to provide the closest version of an available real-time backup. This is commonly employed in very large data retrieval systems.

Common Backup Issues and Problems

All backup systems share common issues and problems, whether they use a tape or CD-ROM format. There are three primary backup concerns.

Slow Data Transfer of the Backup. All backups take time, especially tape backup. Depending upon the volume of data that needs to be copied, full backups to tape can take an incredible amount of time. In addition, the time required to restore the data must also be factored into any disaster recovery plan. Backups that pass data through the network infrastructure must be scheduled during periods of low network utilization, which are commonly overnight, over the weekend, or during holidays. This also requires off-hour monitoring of the backup process.

Server Disk Space Utilization Expands Over Time. As the amount of data that needs to be copied increases, the length of time to run the backup proportionally increases and the demand on the system grows as more tapes are required. Sometimes the data volume on the hard drives expands very quickly, thus overwhelming the backup process. Therefore, this process must be monitored regularly.

The Time the Last Backup Was Run Is Never the Time of the Server Crash. With non-continuous backup systems, data that was entered after the last backup prior to a system crash will have to be recreated. Many systems have been designed to provide on-line fault tolerance during backup (the old Vortex Retrochron was one), yet because backup is a post-processing batch process, some data re-entry will need to be performed.

Note Physically securing the tapes from unauthorized access is obviously a security concern and is considered a function of the Operations Security Domain.

Managing Single Points of Failure

A *Single Point of Failure* is an element in the network design that, if it fails or is compromised, can negatively affect the entire network. Network design methodologies expend a lot of time and resources to search for these points; here we have provided only a few. The technological aspects of cabling and networking topologies are discussed in more detail in the “Technology Concepts” section later in this chapter. Now, we will discuss how they can contribute to creating a single point of failure.

Cabling Failures

Coaxial. These are coaxial cables with many workstations or servers attached to the same segment of cable, which creates a single point of failure if it is broken. Exceeding the specified effective cable length is also a source of cabling failures.

Twisted Pair. Twisted Pair cables currently have two categories in common usage: CAT3 and CAT5. The fundamental difference between these two types is how tightly the copper wires are wound. This tightness determines the cable’s resistance to interference, the allowable distance it can be pulled between points, and the data’s transmission speed before attenuation begins to affect the signal. CAT3 is an older specification with a shorter effective distance. Cable length is the most common failure issue with twisted pair cabling.

Fiber Optic. Fiber Optic cable is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length (up to two kilometers in some cases). It can carry a heavy load of activity much easier than the copper types, and as such is commonly used for infrastructure backbones, server farms, or connections that need large amounts of bandwidth. The primary drawbacks of this cable type are its cost of installation and the high level of expertise needed to have it properly terminated.

Topology Failures

Ethernet. Ethernet is currently the most popular topology. The older coaxial cable has been widely replaced with twisted pair, which is extremely resistant to failure, especially in a star-wired configuration.

Token Ring. Token ring was designed to be a more fault-tolerant topology than Ethernet, and can be a very resilient topology when properly implemented. Because a token is passed by every station on the ring, a NIC that is set to the wrong speed or is in an error state can bring down the entire ring.

Fiber Distributed Data Interface (FDDI). FDDI is a token-passing ring scheme like a token ring, yet it also has a second ring that remains dormant until an error condition is detected on the primary ring. The primary ring is then isolated and the secondary ring begins working, thus creating an extremely fault-tolerant network. This fault tolerance is occasionally overridden in certain implementations that use both rings to create a faster performance.

Leased Lines. Leased lines, such as T1 connections and Integrated Services Digital Network (ISDN) lines, can be a single point of failure and have no built-in redundancy like the Local Area Network (LAN) topologies. A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed at both ends of the connection. Having multiple vendors can also help with redundancy — the T1 lines are not all supplied by one carrier.

Frame Relay. Frame relay uses a public switched network to provide Wide Area Network (WAN) connectivity. Frame relay is considered extremely fault-tolerant

because any segment in the frame relay cloud that is experiencing an error or failure diverts traffic to other links. Sometimes fault tolerance is achieved by a client using multiple vendors for this service, such as in leased lines.

Other Single Points of Failure

Other single points of failure can be unintentionally created by not building redundancy into the network design. For example, network devices can create a single point of failure when all network traffic in or out of the network passes through this single device. This can happen with firewalls, routers, hubs, and switches. All single devices should have redundant units installed and/or redundant power supplies and parts. Dial-up or ISDN Basic Rate Interface (BRI) connections are often created as backup routes for faster leased lines.

Power Failure

Blackouts, brownouts, surges, and spikes are all examples of power fluctuations that can seriously harm any electronic equipment. Servers, firewalls, routers, and mission-critical workstations are network devices that should have their own Uninterruptible Power Supply (UPS) attached. A UPS can provide a source of clean, filtered, steady power, unlike a battery backup. Intelligent UPS systems can shut down devices gracefully (without a hard crash), notify personnel that a power outage has occurred, and restart the system after the outage has been remedied. For example, in New York, the supplied power wattage range varies widely throughout the day and can be very damaging on electronics without a UPS. Network Operations Centers (NOC) and other providers of carrier services commonly install their own Direct Current (DC) power generators as part of the network infrastructure design. A more thorough description of electrical power failures and controls can be found in Chapter Ten, "Physical Security."

Network Attacks and Abuses

The CISSP candidate will need to know the various types of attacks on and abuses of networked systems and how they work. In current practice, these attacks are constantly evolving — this is probably the most dynamic area of InfoSec today. Large teams and huge amounts of money and resources are dedicated to reacting to the latest twists and turns of intrusions into networked systems, particularly on the Internet. This area is also a constant source of fodder for the media. Arguments can be made on whether internal versus external intrusions are more serious or common — a recent study estimated that about 60 percent of unauthorized network intrusions originated internally and this figure is on a downward trend. With the Internet economy so visible, external C.I.A. failures can create some very serious credibility and PR problems that will negatively affect the bottom line.

Saving Configuration Files and Trivial File Transfer Protocol

Sometimes when a network device fails, the configuration, which was programmed into it, will also be lost. This can especially happen to routers. The procedure that is used to prevent this from occurring consists of capturing the configuration files by logging a terminal session during a configuration session, and then storing that configuration on floppies, or installing a Trivial File Transfer Protocol (TFTP) server. The TFTP server is then accessed during the configuration session to save or retrieve configuration information to the network device. This server can be located in a secure area. If the network is very large, a TFTP server is considered mandatory. Many networking devices now support TFTP.

General Classes of Network Abuses

We will now explain several classes of network attacks a CISSP candidate should know. These classes are grouped very generally, and should not be considered a complete listing of network attacks or abuses.

Class A: Unauthorized Access of Restricted Network Services by the Circumvention of Security Access Controls

This type of usage is called *logon abuse*. It refers to legitimate users accessing networked services that would normally be restricted to them. Unlike network intrusion, this type of abuse focuses primarily on those users who may be internal to the network, legitimate users of a different system, or users who have a lower security classification. *Masquerading* is the term used when one user pretends to be another user. An attacker socially engineering passwords from an ISP would be an example of this type of masquerading.

Class B: Unauthorized Use of a Network for Non-Business Purposes

This style of network abuse refers to the non-business or personal use of a network by otherwise authorized users, such as Internet surfing to inappropriate content sites (travel, pornography, sports, and so forth). As per the (ISC)² Code of Ethics and the Internet Advisory Board (IAB) recommendations, the use of networked services for other than business purposes can be considered abuse of the system. While most employers do not enforce extremely strict web surfing rules, occasional harassment litigation resulting from employees accessing pornography sites and employees operating private web businesses using the company's infrastructure can constitute unauthorized use.

Class C: Eavesdropping

This type of network attack consists of the unauthorized interception of network traffic. Eavesdropping attacks occur through the interception of network traffic. Certain network transmission methods, such as by satellite, wireless, mobile, PDAs, and so on, are vulnerable to eavesdropping attacks. *Tapping* refers to the physical interception of a transmission medium (like the splicing of the cable or the creation of an induction loop to pick up electromagnetic emanations from copper).

Passive Eavesdropping. Covertly monitoring or listening to transmissions that are unauthorized by either the sender or receiver.

Active Eavesdropping. Tampering with a transmission to create a covert signaling channel, or actively *probing* the network for infrastructure information.

An active variation on eavesdropping is called *Covert Channel* eavesdropping, which consists of using a hidden unauthorized network connection to communicate unauthorized information. A *Covert Storage Channel* operates by writing information to storage by one process and then reading using another process from a different security level. A *Covert Timing Channel* signals information to another process by modulating its own resource use to affect the response time of another.

Eavesdropping and probing are often the preliminary steps to session hijacking and other network intrusions.

Class D: Denial of Service and Other Service Disruptions

These types of attacks create service outages due to the saturation of networked resources. This saturation can be aimed at the network devices, servers, or infrastructure bandwidth — whatever network area that unusual traffic volumes can seriously degrade. For example, the Distributed Denial of Service (DDoS) attack that

occurred in February of 2000 is not specifically considered a hack because the attack's primary goal was not to gather information (confidentiality or integrity is not intentionally compromised), but to halt service by overloading the system. This attack, however, can be used as a diversion to enable an intentional hack to gain information from a different part of the system by diverting the company's Information Technology (IT) resources elsewhere. Detailed examples of DoS attacks are provided later in the text.

Class E: Network Intrusion

This type of attack refers to the use of unauthorized access to break into a network primarily from an external source. Unlike a login abuse attack, the intruders are not considered to be known to the company. Most common conceptions of hacks reside in this category. Also known as a penetration attack, it exploits known security vulnerabilities in the security perimeter.

Spoofing. Refers to an attacker deliberately inducing a user (subject) or device (object) into taking an incorrect action by giving it incorrect information.

Piggy-backing. Refers to an attacker gaining unauthorized access to a system by using a legitimate user's connection. A user leaves a session open or incorrectly logs off, enabling an attacker to resume the session.

Back-door attacks. Commonly refers to intrusions via dial-up or async external network connections.

Class F: Probing

Probing is an active variation of eavesdropping. It is usually used to give an attacker a road map of the network in preparation for an intrusion or a DoS attack. It can give the eavesdropper a list of available services. Traffic analysis through the use of a "Sniffer" is one probing type of eavesdropping where scans of the hosts for various enabled services are employed to document what systems are active on a network and what ports are open.

Probing can be performed either manually or automatically. Manual vulnerability checks are performed by using tools such as Telnet to connect to a remote service to see what is listening. Automated vulnerability scanners are software programs that automatically perform all the probing and scanning steps and report the findings back to the user. Due to its free availability on the Internet, the number of this type of automated probing has skyrocketed recently.

Common Denial of Service (DoS) Attacks

The DoS attack may use some of the following techniques to overwhelm a target's resources:

- Filling up a target's hard drive storage space by using huge email attachments or file transfers
- Sending a message, which resets a target host's subnet mask, causing a disruption of the target's subnet routing
- Using up all of a target's resources to accept network connections, resulting in additional network connections being denied

Additional specific types of DoS attacks are listed next.

Buffer Overflow Attack. A basic *buffer overflow* attack occurs when a process receives much more data than expected. If the process has no programmed routine to deal with this excessive amount of data, it acts in an unexpected way that the intruder can exploit. Several types of buffer overflow attacks exist, with the most common being

the “*Ping of Death*” (large packet Ping attack) or the use of over 256-character user or file names in email. A large packet Ping attack involves the use of the Internet Control Message Protocol (ICMP) Packet Internet Groper (PING) utility. The intruder sends a “ping” that consists of an illegally modified and very large IP datagram, thus overflowing the system buffers and causing the system to reboot or hang.

SYN Attack. A *SYN attack* occurs when an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker floods the target system’s small “in-process” queue with connection requests, but it does not respond when a target system replies to those requests. This causes the target system to “time out” while waiting for the proper response, which makes the system crash or become unusable.

Teardrop Attack. A *Teardrop attack* consists of modifying the length and fragmentation offset fields in sequential Internet Protocol (IP) packets. The target system then becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets.

Smurf. A *Smurf attack* uses a combination of IP spoofing and ICMP to saturate a target network with traffic, thereby launching a denial of service attack. It consists of three elements — the source site, the bounce site, and the target site. The attacker (the source site) sends a spoofed PING packet to the broadcast address of a large network (the bounce site). This modified packet contains the address of the target site. This causes the bounce site to broadcast the misinformation to all of the devices on its local network. All of these devices now respond with a reply to the target system, which is then saturated with those replies.

Common Session Hijacking Attacks

IP Spoofing Attacks. Unlike a Smurf attack where spoofing is used to create a DoS attack, IP spoofing is used to convince a system that it is communicating with a known entity that gives an intruder access. *IP spoofing* involves an alteration of a packet at the TCP level, which is used to attack Internet-connected systems that provide various TCP/IP services. The attacker sends a packet with an IP source address of a known, trusted host. This target host may accept the packet and act upon it.

TCP Sequence Number Attacks. *TCP sequence number attacks* exploit the communications session, which was established between the target and the trusted host that initiated the session. The intruder tricks the target into believing it is connected to a trusted host and then hijacks the session by predicting the target’s choice of an initial TCP sequence number. This session is then often used to launch various attacks on other hosts.

Other Fragmentation Attacks

IP fragmentation attacks use varied IP datagram fragmentation to disguise its TCP packets from a target’s IP filtering devices. The following are some examples of these types of attacks:

- A *tiny fragment attack* occurs when the intruder sends a very small fragment that forces some of the TCP header field into a second fragment. If the target’s filtering device does not enforce minimum fragment size, this illegal packet can then be passed on through the target’s network.
- An *overlapping fragment attack* is another variation on a datagram’s zero-offset modification (like the teardrop attack). Subsequent packets overwrite the initial packet’s destination address information and then the second packet is passed by the target’s filtering device. This can happen if the target’s filtering device does not enforce a minimum fragment offset for fragments with non-zero offsets.

Trusted Network Interpretation

One of the most important documents of the twenty or so books in the Rainbow series is the Trusted Network Interpretation (TNI), which is also called the “Red Book.” These books and the resulting standards were developed by the National Institute of Standards and Technology (NIST). The Rainbow series is described in detail in Appendix B.

The Red Book interprets the criteria described in the Trusted Computer Security Evaluation Criteria (TCSEC, called the “Orange Book”) for networks and network components, so it is applicable for this chapter. The reader should note that time and technological changes lessen the relevancy of the TNI to contemporary networking.

To deal with technical issues that are outside the scope of the Orange Book, the Red Book examines an interpretation of the Orange Book as it relates to networks, and examines other security services that are not addressed by the Orange Book. The TNI provides Orange Book interpretations for trusted computer and communications network systems under the areas of assurance requirements. It creates rating structures for this assurance and describes and defines additional security services for networks in the areas of communications integrity, DoS, and transmission security. It also assumes that the physical, administrative, and procedural protection measures are already in place. The primary purpose of these interpretations is to provide a standard to manufacturers who are incorporating security features, which operate at defined assurance levels that provide a measurable degree of trust. Table 3.3 is a short introduction to the various TNI evaluation classes.

Table 3.3: TNI Evaluation Classes

Class	Description
D:	Minimal protection
C:	Discretionary protection
C1:	Discretionary security protection
C2:	Controlled access protection
B:	Mandatory protection
B1:	Labeled security protection
B2:	Structured protection
B3:	Security domains

TNI Issues

The TNI is restricted to a limited class of networks — namely centralized networks with a single accreditation authority. It addresses network issues, which are not addressed in the Orange Book, and in a way, it competes with the ISO architecture. Because the distributed network model is becoming the standard (this includes the rise of the Internet), the TNI can be thought of as a bridge between the Orange Book and these newer network classes.

Technology Concepts

This section describes the functions of various Telecommunications and Network technologies.

Protocols

Here's where we get into the meat of networking, and can understand the layered model and the protocols that accompany it. In this section, we will examine the OSI and the TCP/IP layered models, and the protocols that accompany each of these models.

A protocol is a standard set of rules that determines how computers communicate with each other across networks. When computers communicate with one another, they exchange a series of messages. A protocol describes the format that a message must take and the way in which computers must exchange messages. Protocols enable different types of computers such as Macintosh, PC, UNIX, and so on to communicate in spite of their differences. They communicate by describing a standard format and communication method by adhering to a layered architecture model.

The Layered Architecture Concept

Layered architecture is a conceptual blueprint of how communications should take place. It divides communication processes into logical groups called *layers*.

There are many reasons to use a layered architecture:

- To clarify the general functions of a communications process, rather than focusing on the specifics of how to do it
- To break down complex networking processes into more manageable sublayers
- Using industry-standard interfaces enables interoperability
- To change the features of one layer without changing all of the programming code in every layer
- Easier troubleshooting

Layered Models

Layered models serve to enhance the development and management of a network architecture. While they primarily address issues of data communications, they also include some data processing activities at the upper layers. These upper layers address applications software processes, the presentation format, and the establishment of user sessions. Each independent layer of a network architecture addresses different functions and responsibilities. All of these layers work together to maximize the performance of the process and interoperability. Examples of the various functions that are addressed are data transfer, flow control, sequencing, error detection, and notification.

How Data Moves through a Layered Architecture

Data is sent from a source computer to a destination computer. In a layered architecture model, the data passes downward through each layer from the highest layer (the Application Layer 7 in the OSI model) to the lowest layer (the Physical Layer 1 of the OSI model) of the source. It is then transmitted across the medium (cable) and is received by the destination computer where it is passed up the layers in the opposite direction, from the lowest (Layer 1) to the highest (Layer 7).

Each of the various protocols operates at specific layers. Each protocol in the source computer has a job to do: Each one is responsible for attaching its own unique information to the data packet when it comes through its own layer. When the data reaches the destination computer, it moves up the model. Each protocol on the destination computer also has a job to do: Each protocol detaches and examines only the data that was attached by its protocol counterpart at the source computer, then it sends the rest of the packet up the *protocol stack* to the next highest layer. Each layer at each destination sees and deals only with the data that was packaged by its counterpart on the sending side.

Open Systems Interconnect (OSI) Model

In the early 1980s, the Open Systems Interconnection (OSI) reference model was created by the International Standards Organization (ISO) to help vendors create interoperable network devices. The OSI reference model describes how data and network information is communicated from one computer through a network media to another computer. The OSI reference model breaks this approach into seven distinct layers. Layering divides a problem into functional groups that permit an easier understanding of each piece of the problem. Each layer has a unique set of properties and directly interacts with its adjacent layers.

The OSI model was expected to become the standard, yet it did not prevail over TCP/IP. Actually, in some cases, they have been joined at the Application Level to obtain the benefits of each.

The Seven Layers of the OSI Reference Model

The OSI protocol model is divided into seven layers (see Figure 3.4), which we shall examine here.

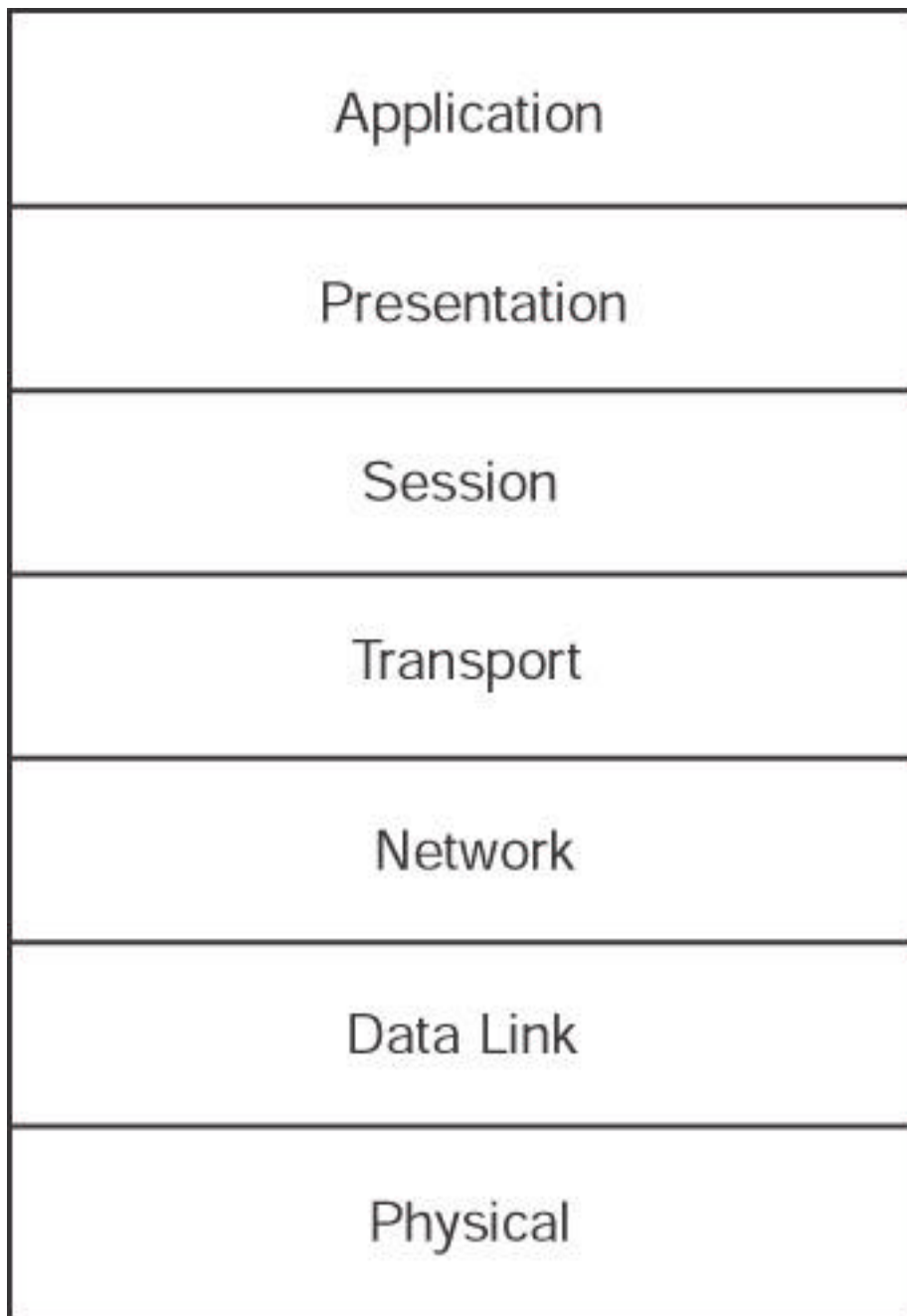


Figure 3.4: The OSI seven-layer reference model.

Data Encapsulation

Data Encapsulation is the process in which the information from one data packet is wrapped around or attached to the data of another packet. In the OSI reference model, each layer encapsulates the layer immediately above it as the data flows down the protocol stack. The logical communication, which happens at each layer of the OSI reference model, does not involve several physical connections because the information that each protocol needs to send is encapsulated within the protocol layer.

Tip

As we describe these OSI layers, you will notice that not all of the layers are equally discussed — we will focus on some layers more than others. The OSI layers that we are most concerned with are the Application, Network, Transport, Data Link, and Physical layers.

Application Layer (Layer 7). The *Application Layer* of the OSI model supports the components that deal with the communication aspects of an application. The Application Layer is responsible for identifying and establishing the availability of the intended communication partner. It is also responsible for determining if sufficient resources exist for the intended communication. This layer is the highest level and is the interface to the user.

The following are some examples of Application Layer applications:

- The World Wide Web (WWW)
- Email gateways
- Electronic Data Interchange (EDI)
- Special interest bulletin boards

Presentation Layer (Layer 6). The *Presentation Layer* presents data to the Application Layer. It is essentially a translator, such as Extended Binary-Coded Decimal Interchange Mode (EBCDIC) or American Standard Code for Information Interchange (ASCII). Tasks like data compression, decompression, encryption, and decryption are all associated with this layer. This layer defines how the applications can enter a network.

When you are surfing the web, most likely you are frequently encountering some of the following Presentation Layer standards:

- Picture (*PICT*). A picture format.
- Tagged Image File Format (*TIFF*). A standard graphics format.
- Joint Photographic Experts Group (*JPEG*). Standard defined by the Joint Photographic Experts Group for graphics.
- Musical Instrument Digital Interface (*MIDI*). A format used for digitized music.
- Motion Picture Experts Group (*MPEG*). The Motion Picture Experts Group's standard for the compression and coding of motion video.

Session Layer (Layer 5). The *Session Layer* makes the initial contact with other computers and sets up the lines of communication. It formats the data for transfer between end nodes, provides session restart and recovery, and performs the general maintenance of the session from end-to-end. The Session Layer offers three different modes — simplex, half-duplex, and full-duplex. It also splits up a communication session into three different phases. These phases are connection establishment, data transfer, and connection release.

The following are some examples of session-layer protocols:

- Network File System (*NFS*). This was developed by Sun Microsystems and is used with Unix workstations.
- Structured Query Language (*SQL*). This language provides users with a way to define their information requirements.
- Remote Procedure Call (*RPC*). This is a client/server redirection tool that is used for disparate service environments.

Transport Layer (Layer 4). The *Transport Layer* defines how to address the physical locations and/or devices on the network, make connections between nodes, and how to handle the networking of messages. It is responsible for maintaining the end-to-end integrity and control of the session. Services located in the Transport Layer both segment and reassemble the data from upper-layer applications and unite it onto the same data stream, which provides end-to-end data transport services and establishes a logical connection between the sending host and destination host on an network. The Transport Layer is also responsible for providing mechanisms for multiplexing upper-layer applications, session establishment, and the tear-down of virtual circuits. TCP and UDP operate at this layer.

Network Layer (Layer 3). The *Network Layer* defines how the small packets of data are routed and relayed between end systems on the same network or on interconnected networks. At this layer, message routing, error detection, and control of node data traffic are managed. The Network Layer's primary function is the job of sending packets from the source network to the destination network. IP operates at this layer.

Data Link Layer (Layer 2). The *Data Link Layer* defines the protocol that computers must follow in order to access the network for transmitting and receiving messages. Token Ring and Ethernet operate within this layer. This layer establishes the communications link between individual devices over a physical link or channel. It also ensures that messages are delivered to the proper device and translates the messages from layers above into bits for the Physical Layer to transmit. It also formats the message into data frames and adds a customized header that contains the hardware destination and source address. The Data Link Layer contains the *Logical Link Control Sublayer* and the *Media Access Control (MAC) Sublayer*.

Physical Layer (Layer 1). The *Physical Layer* defines the physical connection between a computer and a network and it converts the bits into voltages or light impulses for transmission. It also defines the electrical and mechanical aspects of the device's interface to a physical transmission medium, such as twisted pair, coax, or fiber. Communications hardware and software drivers are found at this layer, as well as electrical specifications such as EIA-232 (RS-232) and Synchronous Optical Network (SONET). The Physical Layer has only two responsibilities: It sends bits and receives bits.

The Physical Layer defines the following standard interfaces:

- EIA/TIA-232 and EIA/TIA-449
- V.24 and V.35
- X.21
- High-Speed Serial Interface (HSSI)

OSI Security Services and Mechanisms

OSI defines six basic security services to secure OSI communications. A *security service* is a collection of security mechanisms, files, and procedures that help protect the network.

These are the six basic security services:

1. Authentication
2. Access control
3. Data confidentiality
4. Data integrity
5. Nonrepudiation
6. Logging and monitoring

In addition, the OSI model also defines eight security mechanisms. A *security mechanism* is a control that is implemented in order to provide the six basic security services.

These are the eight security mechanisms:

1. Encipherment
2. Digital signature
3. Access control
4. Data integrity
5. Authentication
6. Traffic padding
7. Routing control

8. Notarization

Transmission Control Protocol/Internet Protocol (TCP/IP) Model

Transmission Control Protocol/Internet Protocol (TCP/IP) is the common name for the suite of protocols that was developed by the Department of Defense (DoD) in the 1970s to support the construction of the Internet. The Internet is based on TCP/IP. A CISSP candidate should be familiar with the major properties of TCP/IP, and should know which protocols operate at which layers of the TCP/IP protocol suite. TCP and IP are the two most well-known protocols in the suite.

The TCP/IP Protocol Model (see Figure 3.5) is similar to the OSI model, but it defines only the following four layers instead of seven:

- *Application Layer.* Consists of the applications and processes that use the network.
- *Host-to-Host Transport Layer.* Provides end-to-end data delivery service to the Application Layer.
- *Internet Layer.* Defines the IP datagram and handles the routing of data across networks.
- *Network Access or Link Layer.* Consists of routines for accessing physical networks and the electrical connection.

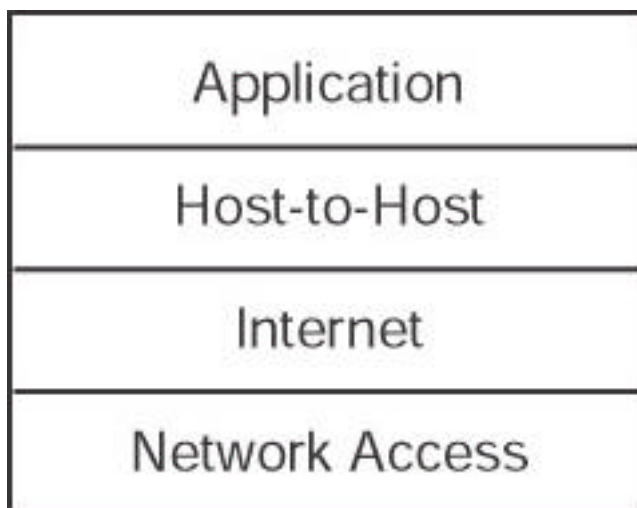


Figure 3.5: The TCP/IP layered model.

The *Application Layer* is very similar to the OSI Application Layer and performs most of the same functions. It is sometimes called the Process/Application Layer in some DoD definitions.

The *Host-to-Host* Layer is comparable to OSI's Transport Layer. It defines the protocols for setting up the level of transmission service. It also provides for reliable end-to-end communications, ensures the data's error-free delivery, handles the data's packet sequencing, and maintains the data's integrity.

The *Internet Layer* corresponds to the OSI's Network Layer. It designates the protocols that are related to the logical transmission of packets over the network. This layer gives network nodes an IP address and handles the routing of packets among multiple networks. It also controls the communication flow between hosts.

At the bottom of the TCP/IP model, the *Network Access Layer* monitors the data exchange between the host and the network. The equivalent of the Data Link and Physical layers of the OSI model, it oversees hardware addressing and defines protocols for the physical transmission of data.

TCP/IP Protocols

The functional protocols can be grouped by the TCP/IP layer that they inhabit. The main protocols that we are concerned with in the Telecommunications domain (and the corresponding layer) are listed next. We shall describe each one in the following text.

- Host-to-Host Transport Layer Protocols
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Layer Protocols

Internet Protocol (IP)

- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Internet Control Message Protocol (ICMP)

Host-to-Host Transport Layer Protocols

Transmission Control Protocol (TCP). TCP provides a full-duplex, *connection-oriented, reliable*, virtual circuit. Incoming TCP packets are sequenced to match the original transmission sequence numbers. Because any lost or damaged packets are retransmitted, TCP is very costly in terms of network overhead and is slower than UDP.

Reliable data transport is addressed by TCP to ensure that the following will be achieved:

- An acknowledgment is sent back to the sender upon the reception of delivered segments.
- Any unacknowledged segments are retransmitted.
- Segments are sequenced back in their proper order upon arrival at their destination.
- A manageable data flow is maintained in order to avoid congestion, overloading, and data loss.

TCP and UDP must use port numbers to communicate with the upper layers. Port numbers are used to keep track of the different conversations that are simultaneously crossing the network. Originating source port numbers dynamically assigned by the source host are usually some number greater than 1023.

User Datagram Protocol (UDP). UDP is a scaled down version of TCP. UDP is used like TCP, yet it only gives a “best effort” delivery. It does not offer error correction, does not sequence the packet segments, and does not care about the order in which the packet segments arrive at their destination. Thus, it is referred to as an *unreliable* protocol.

UDP does not create a virtual circuit and does not contact the destination before delivering the data. Thus, it is also considered a *connectionless* protocol. UDP imposes much less overhead, however, which makes it faster than TCP for applications that can afford to lose a packet now and then, such as streaming video or audio. Table 3.4 lists the main differences between TCP and UDP.

TCP	UDP
Acknowledged	Unacknowledged

Table 3.4: TCP vs. UDP Protocols

TCP	UDP
Sequenced	Unsequenced
Connection-oriented	Connectionless
Reliability	Unreliable
High Overhead (slower)	Low overhead (faster)

Connection-Oriented versus Connection-less Network Services

The traditional telephone versus letter example might help you to understand the difference between a TCP and a UDP. Calling someone on the phone is like TCP, you have established a virtual circuit with the party at the other end. That party may or may not be the person you want to speak to (or may be an answering machine), but you know whether or not you spoke to them. Alternatively, using UDP is like sending a letter. You write your message, address it, and mail it. This is like UDP's connectionless property. You are not really sure it will get there, but you assume the post office will provide its "best effort" to deliver it.

The Internet Layer Protocols

Internet Protocol (IP). IP is the Big Daddy of all the protocols. All hosts on a network have a logical ID that is called an IP address. This software address contains the information that aids in simplifying routing. Each data packet is assigned the IP address of the sender and the IP address of the recipient. Each device then receives the packet and makes routing decisions based upon the packet's destination IP address.

IP provides an "unreliable datagram service." It supplies a) no guarantees that the packet will be delivered, b) no guarantees that it will be delivered only once, and c) no guarantees that it will be delivered in the order in which it was sent.

Note IP addresses are currently 32 bits long. Because we ran out of available IP addresses long ago, a new initiative called IPv6 will extend that to 128 bits. It is estimated that IPv6 will supply over 1,000,000 IP addresses for every person on the planet!

Address Resolution Protocol (ARP). IP needs to know the hardware address of the packet's destination so it can send it. ARP is used to match an IP address to an Ethernet address. An Ethernet address is a 48-bit address that is hard-wired into the NIC of the network node. ARP matches up the 32-bit IP address with this hardware address, which is technically referred to as the Media Access Control (MAC) address or the physical address.

ARP interrogates the network by sending out a broadcast seeking a network node that has a specific IP address, and asks it to reply with its hardware address. ARP maintains a dynamic table of these translations between IP addresses and Ethernet addresses, so that it only has to broadcast a request to every host the first time it is needed.

Reverse Address Resolution Protocol (RARP). In some cases, the reverse is required: The MAC address is known, yet the IP address needs to be discovered. This is sometimes the case when diskless machines are booted onto the network. The

RARP protocol sends out a packet, which includes its MAC address and a request to be informed of the IP address that should be assigned to that MAC address. A RARP server then responds with the answer.

Internet Control Message Protocol (ICMP). ICMP is a management protocol and messaging service provider for IP. Its primary function is to send messages between network devices regarding the health of the network. It also informs hosts of a better route to a destination if there is trouble with an existing route. It can also help identify the problem with that route.

The utility PING uses ICMP messages to check the physical connectivity of the machines on a network.

Other TCP/IP Protocols

Telnet. Telnet's function is terminal emulation. It enables a user on a remote client machine to access the resources of another machine. Telnet's capabilities are limited to running applications — it cannot be used for downloading files.

File Transfer Protocol (FTP). FTP is the protocol that is used to facilitate file transfer between two machines. FTP is also employed to perform file tasks. It enables access for both directories and files, and can also accomplish certain types of directory operations. However, FTP cannot execute remote files as programs.

Trivial File Transfer Protocol (TFTP). TFTP is a stripped-down version of FTP. TFTP has no directory browsing abilities; it can do nothing but send and receive files. Unlike FTP, authentication does not occur, so it is insecure. Some sites choose not to implement TFTP due to the inherent security risks.

Network File System (NFS) NFS is the protocol that supports file sharing. It enables two different types of file systems to interoperate.

Simple Mail Transfer Protocol (SMTP). SMTP is the protocol we use every day to send and receive Internet email. When a message is sent, it is sent to a mail queue. The SMTP server regularly checks the mail queue for messages and delivers them when they are detected.

Line Printer Daemon (LPD). The LPD daemon, along with the Line Printer (LPR) program, enables print jobs to be spooled and sent to a network's shared printers.

X Window. X Window defines a protocol for the writing of graphical user interface-based client/server applications.

Simple Network Management Protocol (SNMP). SNMP is the protocol that provides for the collection of network information by polling the devices on the network from a management station. This protocol can also notify network managers of any network events by employing agents that send an alert called a *trap* to the management station. The databases of these traps are called Management Information Bases (MIBs).

Bootstrap Protocol (BootP). When a diskless workstation is powered on, it broadcasts a BootP request to the network. A BootP server hears the request and looks up the client's MAC address in its BootP file. If it finds an appropriate entry, it responds by telling the machine its IP address and the file from which it should boot. BootP is an Internet Layer protocol.

Security-Enhanced and Security-Focused Protocols

The following are two types of security-enhanced protocol extensions:

- Security enhancements to the Telnet protocol, such as Remote Terminal Access, and Secure Telnet.
- Security enhancements to the Remote Procedure Call protocol, such as Secure RPC Authentication (SRA).

The following protocols are two examples of security-focused protocols that were primarily created to support Internet transactions and authentication:

- *Secure Electronic Transaction (SET)*. Originated by VISA and MasterCard as an Internet credit card protocol. It supports the authentication of both the sender and receiver and it ensures content privacy in an effort to reduce merchant fraud on public networks. Although it is still widely in use, SET is being overtaken by SSL.
- *Secure HTTP (S-HTTP)*. An early standard for encrypting HTTP documents. The HTTP server caches and secures stored S-HTTP documents. This protocol is also being overtaken by SSL.

SET and S-HTTP operate at the Application Layer of the OSI model. Following are three protocols that provide security services at the Transport Layer. SSH and SSL are very heavily used for protecting Internet transactions.

These are the three security-focused protocols:

- *Secure Shell (SSH-2)*. SSH is a strong method of performing client authentication. Because it supports authentication, compression, confidentiality, and integrity, SSH is used frequently on the Internet. SSH has two important components: RSA certificate exchange for authentication and Triple DES for session encryption.
- *Secure Sockets Layer (SSL)*. An encryption technology that is used to provide secure transactions such as the exchange of credit card numbers. SSL is a socket layer security protocol and is a two-layered protocol that contains the SSL Record Protocol and the SSL Handshake Protocol. Similar to SSH, SSL uses symmetric encryption for private connections and asymmetric or public key cryptography for peer authentication. It also uses a Message Authentication Code for message integrity checking.
- *Simple Key Management for Internet Protocols (SKIP)*. A security technology that provides high availability in encrypted sessions (for example, crashed gateways). SKIP is similar to SSL, except that it requires no prior communication in order to establish or exchange keys on a session-by-session basis. Therefore, no connection setup overhead exists and new key values are not continually generated.

Firewall Types and Architectures

A CISSP candidate will need to know the basic types of firewalls and their functions, which firewall operates at which protocol layer, and the basic variations of firewall architectures.

Firewall Types

We will first begin by looking at the various types of firewalls. We have them ordered here by generation (in what order they were developed).

Packet Filtering Firewalls

The first type of firewall we examine is the *packet filtering* firewall, which can also be called a *screening router*. This type of firewall examines both the source and destination address of the incoming data packet. This firewall either blocks or passes the packet to its intended destination network, which is usually the local network segment where it resides. The firewall can then deny access to specific applications and/or services based on the *Access Control Lists (ACLs)*, which are database files that reside on the firewall, are maintained by the firewall administrator, and tell the firewall

specifically which packets can and cannot be forwarded to certain addresses. The firewall can also enable access for only authorized application port or service numbers. A packet filtering firewall looks at the data packet to get information about the source and destination addresses of an incoming packet, the session's communications protocol (TCP, UDP, or ICMP), and the source and destination application port for the desired service. This type of firewall system is considered a *first generation firewall*, and can operate at either the Network or Transport Layer of the OSI model.

Application Level Firewalls

Another type of firewall is known as an *Application Level Firewall* (see Figure 3.6). This firewall is commonly a host computer that is running proxy server software, which makes it a *Proxy Server*. This firewall works by transferring a copy of each accepted data packet from one network to another, thereby masking the data's origin. This can control which services are used by a workstation (FTP and so on), and it also aids in protecting the network from outsiders who may be trying to get information about the network's design.

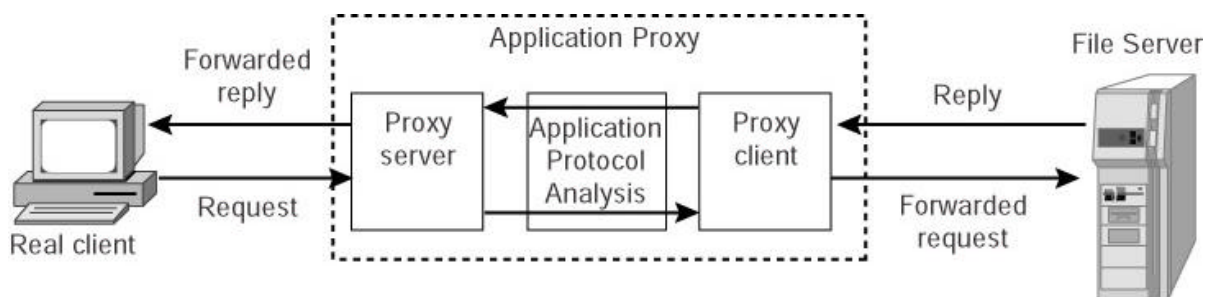


Figure 3.6: An application proxy service firewall.

This type of firewall is considered a *second generation* firewall. It is also called an *Application Layer Gateway*. It operates at the OSI protocol *Layer seven*, the Application Layer. One drawback of this type of firewall is that it reduces network performance due to the fact that it must analyze every packet and decide what to do with each packet.

A variation of the application level firewall is called a *Circuit Level Firewall*. Like an application level firewall, this firewall is used as a proxy server. However, this firewall creates a virtual circuit between the workstation client and the server. It also provides security for a wide variety of protocols and is easier to maintain.

Stateful Inspection Firewalls

Another type of firewall is known as a *Stateful Inspection Firewall*. In a stateful inspection firewall, data packets are captured by an inspection engine that is operating at the faster Network Layer. These packets are queued and then analyzed at all OSI layers. This boosts performance over the application level firewall, and also provides a more complete inspection of the data. By examining the "state" and "context" of the incoming data packets, it helps to track the protocols that are considered "connectionless," such as UDP-based applications and Remote Procedure Calls (RPC). This type of firewall system is used in *third generation* firewall systems.

Dynamic Packet Filtering Firewalls

A dynamic packet filtering firewall is a *fourth generation firewall* technology that enables the modification of the firewall security rule. This type of technology is mostly used for providing limited support for UDP. For a short period of time, this firewall remembers all

of the UDP packets that have crossed the network's perimeter, and it decides whether to enable packets to pass through the firewall.

Kernel Proxy

A *Kernel Proxy* is a *fifth generation firewall* architecture that provides a modular, kernel-based, multi-layer session evaluation and runs in the Windows NT Executive, which is the kernel mode of Windows NT. It is a very specialized firewall architecture that uses dynamic and custom TCP/IP-based stacks to inspect the network packets and to enforce security policies. Unlike normal TCP/IP stacks, these stacks are constructed out of kernel-level proxies.

Firewall Architectures

Now we will discuss the four types of firewall architectures — packet-filtering, screened hosts, dual-homed hosts, and screened-subnet firewalls. Keep in mind that some of these architectures are specifically associated with one of the previously discussed firewall generation types, while other architectures can be a combination of generation types.

Packet-Filtering Routers

The most common and oldest firewall device in use is the *Packet Filtering Router* (see Figure 3.7). A packet-filtering router sits between the private “trusted” network and the “untrusted” network or network segment, and is sometimes used as a *boundary router*. A packet-filtering router uses Access Control Lists (ACLs). This firewall protects against standard generic external attacks. One problem with this type of firewall is that ACLs can be manually difficult to maintain.



Figure 3.7: A packet-filtering boundary router.

This type of firewall has several drawbacks: It lacks strong user authentication, employs minimal auditing, and its complex ACLs negatively impact network performance. This packet filtering router is sometimes used to directly manage the access to a demilitarized zone (*DMZ*) network segment.

Screened-Host Firewall Systems

This firewall architecture employs both a packet-filtering router and a bastion host and is called a *Screened-Host Firewall* (see Figure 3.8). It is a little more complicated than the other architectures because it offers a higher level of security by providing both network-layer (packet-filtering) and application-layer (proxy) services. This type of firewall system is considered to be safer because it requires an intruder to penetrate two separate systems before the trusted network can be compromised. The bastion host is configured on the local “trusted” network with a packet-filtering router between the “untrusted” network and the bastion host. Because the bastion host is commonly the focus of external attacks, it is sometimes called the *sacrificial host*.

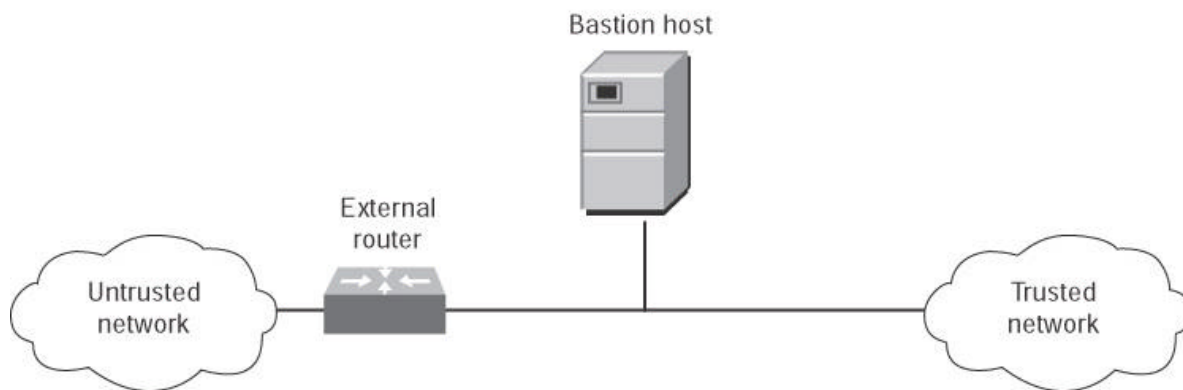


Figure 3.8: A screened-host firewall.

Dual-Homed Host Firewalls

Another very common firewall architecture configuration is the *Dual-Homed Host* (see Figure 3.9). It is also called a dual-homed or multi-homed bastion host. This architecture is a simple configuration that consists of a single computer (the host) with two NICs: One is connected to the local “trusted” network and the other is connected to the Internet or an “untrusted” external network. A dual-homed host firewall usually acts to block or filter some or all of the traffic trying to pass between the networks. IP traffic forwarding is usually disabled or restricted — all traffic between the networks and the traffic’s destination must pass through some kind of security inspection mechanism. A multi-homed bastion host can translate between two network access layer protocols, such as Ethernet to Token Ring, for example.

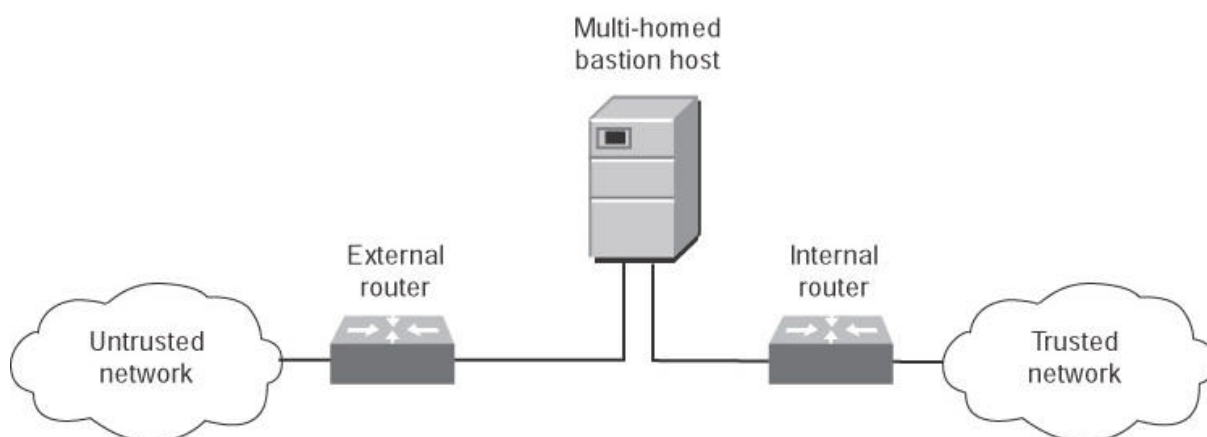


Figure 3.9: A dual-homed firewall.

A design issue with this firewall is that the host’s routing capabilities must be disabled so that it does not unintentionally enable internal routing, which will connect the two networks together transparently and negate the firewall’s function.

Screened-Subnet Firewalls (with a Demilitarized Zone)

One of the most secure implementations of firewall architectures is the *Screened-Subnet firewall* (see Figure 3.10). It employs two packet-filtering routers and a bastion host. Like a screened host firewall, this firewall supports both packet-filtering and proxy services, yet it also defines a *demilitarized zone* (DMZ). This creates a small network between the untrusted network and the trusted network where the bastion host and other public web services exist. The outside router provides protection against external attacks, while the inside router manages the private network access to a DMZ by routing it through the bastion host. An issue with this configuration is its complex configuration and maintenance.

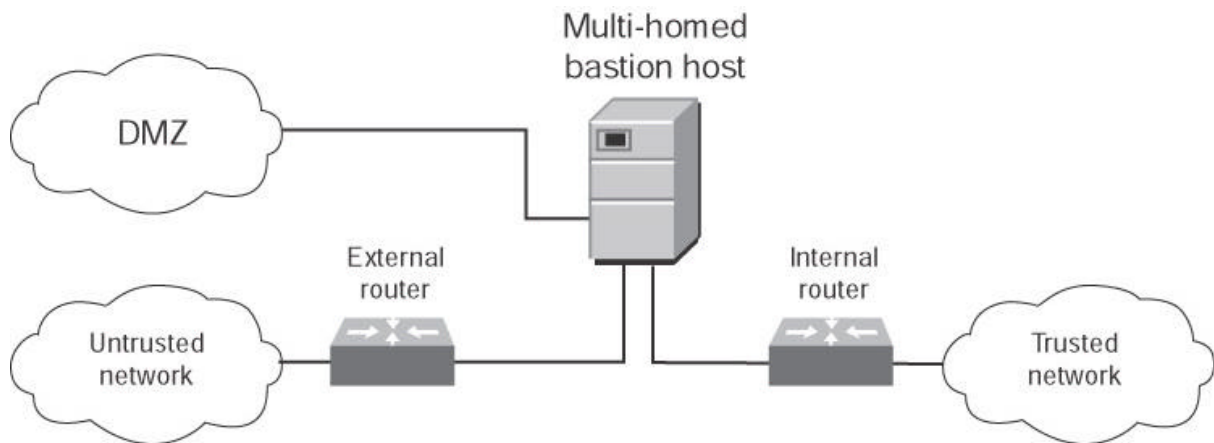


Figure 3.10: A screened-subnet with a DMZ.

Another Firewall Variation

Another variation of firewall protection is provided by a proprietary firewall called a “SOCKS” server. This is a circuit-level proxy server that does not require the server resource overhead of conventional proxy servers. It does, however, require proprietary SOCKS client software to be loaded on every workstation. This firewall is mostly used for outbound Internet access by a workstation. The problem with this type of firewall configuration is that it is IT support intensive (due to the individual workstation configurations) and uses proprietary software.

Virtual Private Networks

A *Virtual Private Network* (VPN) is created by dynamically building a secure communications link between two nodes using a *secret encapsulation method* (see Figure 3.12). This link is commonly called a *secure encrypted tunnel*, although it is more accurately defined as an *encapsulated tunnel*, because encryption may or may not be used.

Network Address Translation

Network Address Translation (NAT) is a very important concept in data networking, especially when it pertains to firewalls (see Figure 3.11). As a firewall administrator, you do not really want to let remote systems know the true IP addresses of your internal systems. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets — 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255 — that are known as “global non-routable addresses.” NAT is a tool that is used for masking true IP addresses by employing these internal addresses. NAT converts a private IP address to a registered “real” IP address. Most firewall systems now include NAT capability. NAT is also used when corporations use private addressing ranges for internal networks — these ranges are not allowed to be routed on the Internet.

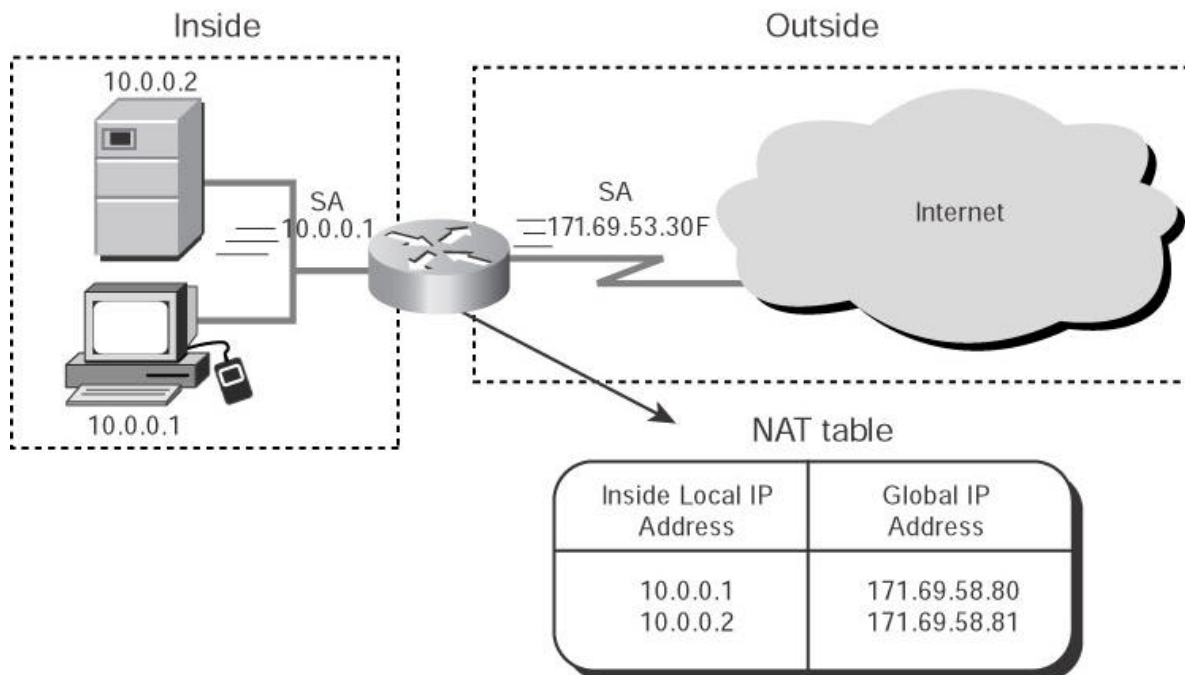


Figure 3.11: Network Address Translation (NAT).

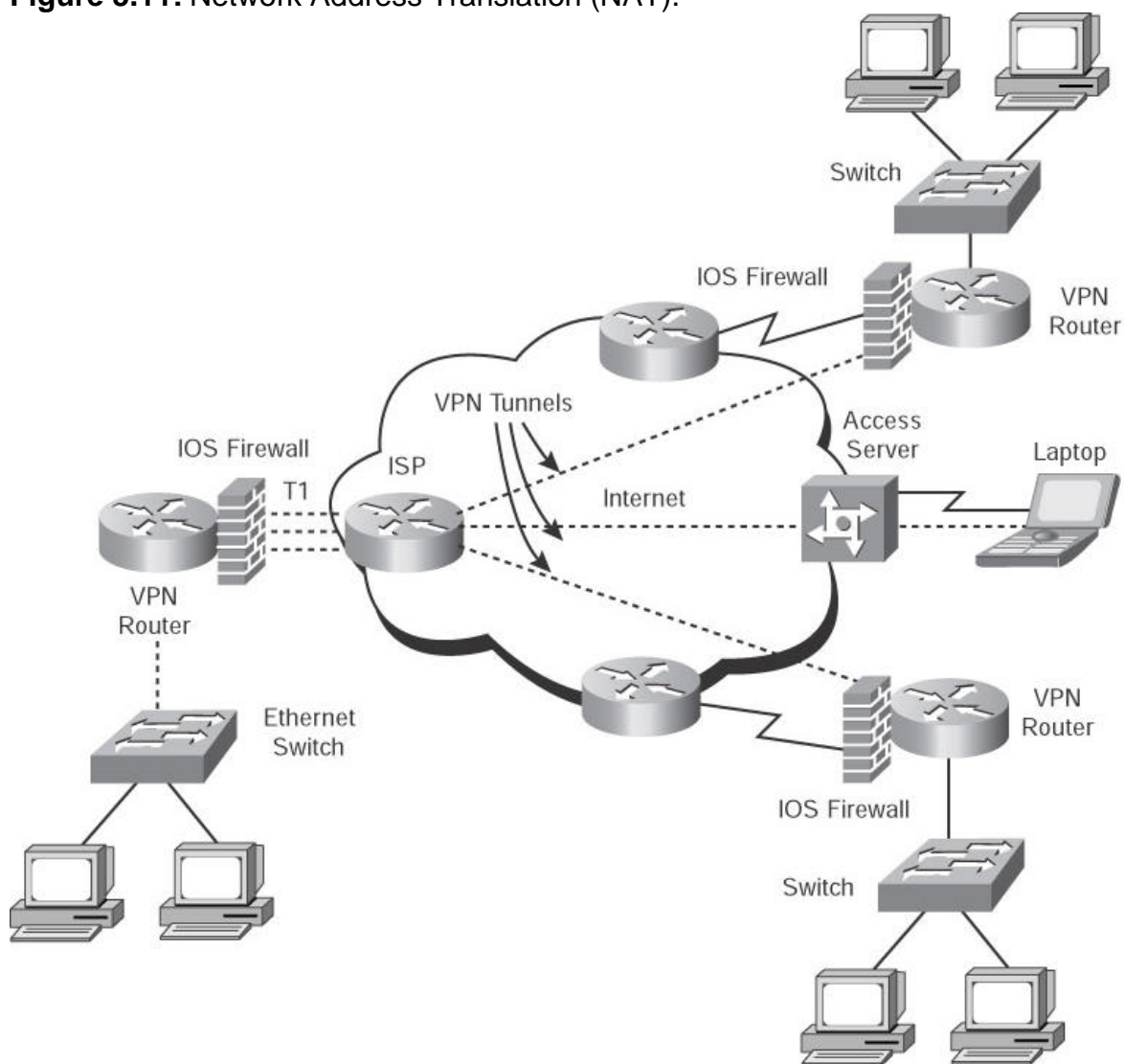


Figure 3.12: Example of a Cisco VPN.

This tunnel can be created by using methods such as the following:

- Installing software or hardware agents on the client or a network gateway

- Implementing various user or node authentication systems
- Implementing key and certificate exchange systems

VPN Protocol Standards

The following are the three most common VPN communications protocol standards:

Point-to-Point Tunneling Protocol (PPTP). *PPTP* works at the *Data Link Layer* of the OSI model. Designed for individual client to server connections, it enables only a single point-to-point connection per session. This standard is very common with asynchronous connections that use Win9x or NT clients. PPTP uses native Point-to-Point Protocol (PPP) authentication and encryption services.

Layer 2 Tunneling Protocol (L2TP). *L2TP* is a combination of PPTP and the earlier Layer 2 Forwarding Protocol (*L2F*) that works at the *Data Link Layer* like PPTP. It has become an accepted tunneling standard for VPNs. In fact, dial-up VPNs use this standard quite frequently. Like PPTP, this standard was designed for single point-to-point client to server connections. Note that multiple protocols can be encapsulated within the L2TP tunnel.

IPSec. *IPSec* operates at the *Network Layer* and it enables multiple and simultaneous tunnels, unlike the single connection of the previous standards. IPSec has the functionality to encrypt and authenticate IP data. It is built into the new IPv6 standard, and is used as an add-on to the current IPv4. While PPTP and L2TP are aimed more at dial-up VPNs, IPSec focuses more on network-to-network connectivity. The elements of IPSec are described in more detail in Chapter 4, “Cryptography.”

VPN Devices

VPN devices are hardware or software devices that utilize the previously discussed VPN standards to create a secure tunnel. The VPN devices should be grouped into two types: *IPSec-compatible* and *non-IPSec-compatible*.

IPSec-Compatible VPN Devices

IPSec-compatible VPN devices are installed on a network’s perimeter and encrypt the traffic between networks or nodes by creating a secure tunnel through the unsecured network. Because they employ IPSec encryption, they only work with IP, thus they are not multiprotocol. These devices operate at the Network Layer (Layer Three). These devices have two operational modes:

1. *Tunnel mode.* The entire data packet is encrypted and encased in an IPSec packet.
2. *Transport mode.* Only the datagram is encrypted, leaving the IP address visible.

Non-IPSec-compatible VPN Devices

Common VPN devices that are not compatible with IPSec include Socks-based proxy servers, PPTP-compatible devices, and SSH-using devices.

Socks-based proxy servers can be used in a VPN configuration as well as in a firewall configuration. In this implementation, they enable access to the internal network from the outside, instead of enabling internal workstations access to the external Internet through a proxy firewall (described earlier in the “Firewall Architectures” section). While not a traditional VPN protocol, Socks-based systems contain authentication and encryption features, which are similar to VPN protocols that are very strong. Socks operates at the OSI Layer 7.

Previously described, PPTP is most frequently implemented in Win9x clients and/or WinNT Servers and clients. It is multiprotocol, uses PAP or CHAP user authentication, compresses data for efficient transmissions, and employs end-to-end encryption. *Dial-*

up VPNs are LAN Remote Access Servers that have multiprotocol VPN services implemented and using PPTP. They are commonly used by Internet Service Providers (ISPs).

Secure Shell (SSH-2) is not strictly a VPN product, but it can be used like one. SSH opens a secure, encrypted shell (command line) session from the Internet through a firewall to the SSH server. After the connection is established, it can be used as a terminal session or for tunneling other protocols.

Firewall-Based VPNs

Firewall-based VPNs are frequently available on third-generation firewalls. These devices employ a VPN system, which is integrated into a firewall and often uses proprietary or non-standard VPN protocols. These VPNs operate at the application layer in the tunnel mode. Because they commonly use user-based authentication and end-to-end encryption, performance degradation is often a problem with these devices.

Data Networking Basics

A CISSP candidate will also need to know the basics of the data network structures — the types of cabling, the various network access methods and topologies, and the differences between various LANs and WANs.

A Data Network consists of two or more computers that are connected for the purpose of sharing files, printers, exchanging data, and so forth. To communicate on the network, every workstation must have an NIC inserted into the computer, a transmission medium (such as copper, fiber, or wireless), a Network Operating System (NOS), and a LAN device of some sort (such as a hub, bridge, router, or switch) to physically connect the computers together. Figure 3.13 shows common data networking components.

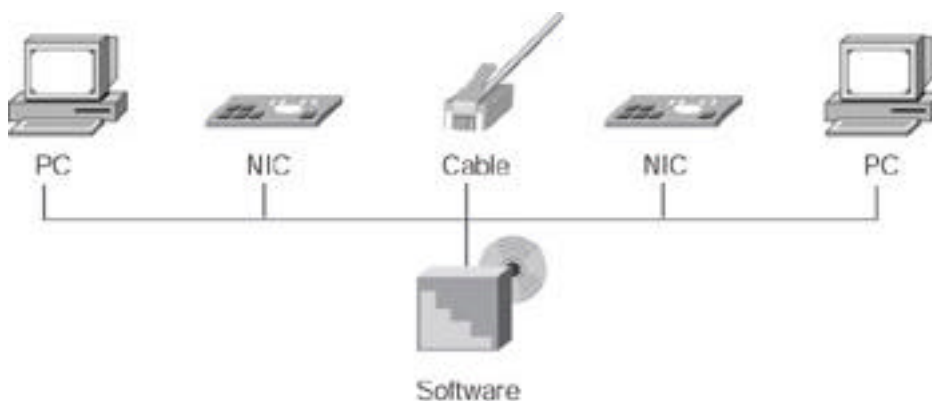


Figure 3.13: Data networking components.

Data Network Types

We will examine the following Data Network types:

- Local Area Networks (LAN)
- Wide Area Networks (WAN)
- Internet, intranet, and extranet

Local Area Networks

A *Local Area Network (LAN)* (see Figure 3.14) is a discrete network that is designed to operate in a specific limited geographic area like a single building or floor. LANs connect workstations and file servers together so that they can share network resources like printers, email, and files. LAN devices are connected using a type of connection medium (such as copper wire or fiber optics), and they use various LAN

protocols and access methods to communicate through LAN devices (such as bridges or routers). LANs can also be connected to a public switched network.

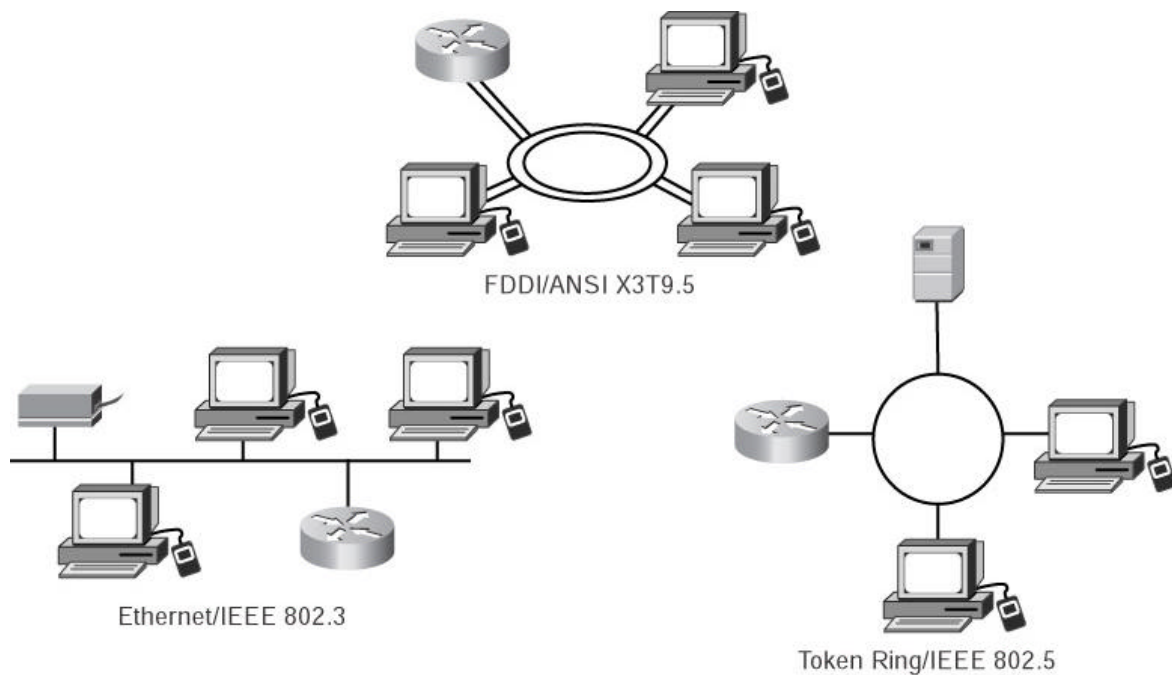


Figure 3.14: Local Area Networks (LANs).

Two common types of LANs are as follows:

- **Campus Area Network (CAN).** A typically large campus network that connects multiple buildings with each other across a high-performance, switched backbone on the main campus.
- **Metropolitan Area Network (MAN).** Although not often used as a description, essentially a LAN that extends over a city-wide metropolitan area.

Both a CAN or MAN can have connections to a WAN.

Wide Area Networks

A *Wide Area Network (WAN)* can be thought of as a network of subnetworks that physically or logically interconnect LANs over a large geographic area. A WAN is basically everything outside of a LAN. A WAN may be privately operated for a specific user community, may support multiple communication protocols, or may provide network connectivity and services via interconnected network segments (extranets, intranets, and VPNs). WAN technologies will be described later in more detail.

Internet

The *Internet* is a WAN that was originally funded by the Department of Defense, which uses TCP/IP for data interchange. The term Internet is used to refer to any and all kinds of Advanced Research Projects Agency Network (ARPANET), Department of Defense Research Projects Agency Network (DARPANET), Defense Data Network (DDN), or DoD Internets. It specifically refers to the global network of public networks and Internet Service Providers (ISPs) throughout the world. The Internet can be utilized by either public or private networks (with a VPN).

Intranet

An intranet is an Internet-like logical network that uses a firm's internal, physical network infrastructure. Because it uses TCP/IP and HTTP standards, it can use low-cost Internet products like web browsers. A common example of an intranet would be a company's human resource department publishing employee guidelines that are accessible by all company employees on the intranet. An intranet provides more security and control than a public posting on the Internet.

Extranet

Like an intranet, an extranet is a private network that uses Internet protocols. Unlike an intranet, an extranet can be accessed by users outside of the company (partners, vendors, and so forth), yet it cannot be accessed by the general public. An example of this type of network is a company's supplier, who can access a company's private network (via a VPN or Internet connection with some kind of authentication), but only has access to the information that he needs.

In addition, a CISSP candidate should also know the difference between asynchronous versus synchronous communications and analog versus digital technologies. Figure 3.15 shows the difference between an analog and digital signal, while Table 3.5 shows the difference between analog and digital technologies.

Analog Signal



Digital Signal



Figure 3.15: Examples of analog and digital signals.

Table 3.5: Analog versus Digital Technologies	
Analog	Digital
Infinite wave form	Saw-tooth wave form
Continuous signal	Pulses
Varied by amplification	On-off only

Asynchronous versus Synchronous Communications

Asynchronous Communication transfers data by sending bits of data sequentially. Start and stop bits mark the beginning and the end of each transfer. Communications

devices must operate at the same speed to communicate. Asynchronous Communication is the basic language of modems and dial-up remote access systems. Synchronous Communication is characterized by very high speed transmission rates that are governed by electronic clock timing signals.

Common Data Network Services

The following are some of the common services that a data network provides:

- *File services.* They share data files and subdirectories on file servers.
- *Mail services.* They send and receive email internally or externally through an email gateway device.
- *Print services.* They print documents to a shared printer or a print queue/spooler.
- *Client/Server services.* They allocate computing power resources among workstations with some shared resources centralized in a file server.
- *Domain Name Service.* It matches Internet Uniform Resource Locator (URL) requests with the actual address or location of the server that is providing that URL. It is a distributed database system that is used to map host names to IP addresses. The Domain Name System (DNS) is a global network of servers that provide these Domain Name Services.

A Word about Network Architectures

Network Architecture refers to the communications products and services, which ensure that the various components of a network (such as devices, protocols, and access methods) work together. Originally a manufacturer's network system often did not interoperate within its own product line, much less enable connectivity with the products of other manufacturers. While IBM's Systems Network Architecture (SNA) and Digital Equipment Corporation's DECnet were seen as an advance in solving these problems within the vendor's product line, they still did not interoperate outside of that product line. The Open Systems Interconnection (OSI) model by the International Standardization Organizations (ISO) was a big step in solving this problem. Other network architecture examples include the Xerox Networking System (XNS) and the Advanced Research Projects Agency Network (ARPANET), the originator of the Internet. These and other standard computer network architectures divide and sub-divide the various functions of data communications into isolated layers, which makes it easier to create products and standards that can interoperate.

Data Networking Technologies

In this section, we examine the basic components of LAN and WAN technologies, including cabling, transmission protocols, and topologies.

LAN Technologies

To become more familiar with the various types of LAN technologies, we need to examine LAN cabling, protocols, transmission and access methods, topologies, and devices.

LAN Cabling Types

Network cabling comes in three flavors — twisted pair, coaxial, and fiber optic — as shown in Figure 3.16.



Figure 3.16: Cabling types.

Twisted Pair Cabling. Twisted pair cabling is a relatively low-speed transmission medium, which consists of two insulated wires that are arranged in a regular spiral pattern. The wires can be shielded (STP) or unshielded (UTP). *Unshielded Twisted Pair* cabling is a four-pair wire medium that is used in a variety of networks. UTP does not require the fixed spacing between connections that is necessary with coaxial-type connections.

UTP comes in several categories. The category rating is based on how tightly the copper cable is wound within the shielding: The tighter the wind, the higher the rating and its resistance against interference and attenuation. In fact, UTP Category 3 wire was often used for phone lines, but now the Category 5 wire is the standard, and even higher categories are available. This UTP cabling can be more easily tapped by eavesdroppers than the other cable types.

The categories of UTP are

- *Category 1 UTP.* Was used for telephone communications and is not suitable for transmitting data.
- *Category 2 UTP.* Specified in the EIA/TIA -586 standard to be able to handle data rates of up to 4 million bits per second (Mbps).
- *Category 3 UTP.* Used in 10BaseT networks and is specified to be able to handle data rates of up to 10 Mbps.
- *Category 4 UTP.* Used in Token Ring networks and can transmit data at speeds of up to 16 Mbps.
- *Category 5 UTP.* Specified to be able to handle data rates of up to 100 Mbps, and is currently the UTP standard for new installations.
- *Category 6 UTP.* Specified to be able to handle data rates of up to 155 Mbps.
- *Category 7 UTP.* Specified to be able to handle data rates of up to 1 billion bits per second (GBps).

Coaxial Cable (Coax). Coax consists of a hollow outer cylindrical conductor that surrounds a single, inner wire conductor. Two types of coaxial cable are currently used in LANs: 50-ohm cable, which is used for digital signaling, and 75-ohm cable, which is used for analog signaling and high-speed digital signaling.

Coax is more expensive, yet it is more resistant to Electromagnetic Interference (EMI) than twisted pair cabling and can transmit at a greater bandwidth and distance. However, twisted pair cabling is so ubiquitous that most installations rarely use coax except in special cases, like broadband communications.

Coax can come in two types for LANs:

1. Thinnet (RG58 size)
2. Thicknet (RG8 or RG11 size)

The following are the two common types of coaxial cable transmission methods:

1. *Baseband.* The cable carries only a single channel.

2. *Broadband*. The cable carries several usable channels, such as data, voice, audio, and video.

Fiber Optic Cable. Fiber optic cable is a physical medium that is capable of conducting modulated light transmission. Fiber optic cable carries signals as light waves, thus creating higher transmission speeds and greater distances due to less attenuation. This type of cabling is much more difficult to tap than other cabling and is the most resistant to interference, especially EMI. It is sometimes called *optical fiber*.

Fiber optic cable is usually reserved for the connections between backbone devices in larger networks. In some very demanding environments, however, fiber optic cable is used to connect desktop workstations to the network or to link to adjacent buildings. Fiber optic cable is the most reliable cable type, but it is also the most expensive to install and terminate.

LAN Transmission Protocols

LAN Transmission Protocols are the rules for communication between computers on a LAN. These rules oversee the various steps in communicating, such as the formatting of the data frame, the timing and sequencing of packet delivery, and the resolution of error states.

Carrier Sense Multiple Access (CSMA). This is the foundation of the Ethernet communications protocol. It has two functional variations: CSMA/CA and CSMA/CD, which is the Ethernet standard. In CSMA, a workstation continuously monitors a line while waiting to send a packet, then transmits the packet when it thinks the line is free. If the workstation doesn't receive an acknowledgment from the destination to which it sent the packet, it assumes a collision has occurred and it resends the packet. This is defined as *persistent carrier sense*. Another version of CSMA is called *nonpersistent carrier sense* where a workstation waits a random amount of time before resending a packet, thus resulting in fewer errors.

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA). In this variation of CSMA, workstations are attached to two coaxial cables. Each coax cable carries data signals in one direction only. A workstation monitors its receive cable to see if the carrier is busy. It then communicates on its transmit cable if no carrier was detected. Thus, the workstation transmits its intention to send when it feels the line is clear due to a precedence that is based upon pre-established tables. Pure CSMA does not have a feature to avoid the problem of one workstation dominating a conversation.

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD). Under the Ethernet CSMA/CD media-access process, any computer on a CSMA/CD LAN can access the network at any time. Before sending data, CSMA/CD hosts listen for traffic on the network. A host wanting to send data waits until it does not detect any traffic before it transmits. Ethernet enables any host on a network to transmit whenever the network is quiet. In addition, the transmitting host also constantly monitors the wire to make sure that no other hosts begin transmitting. If the host detects another signal on the wire, it then sends out an extended jam signal that causes all nodes on the segment to stop sending data. These nodes respond to that jam signal by waiting a bit before attempting to transmit again.

CSMA/CD was created to overcome the problem of collisions that occur when packets are simultaneously transmitted from different nodes. Collisions occur when two hosts listen for traffic, and upon hearing none, they both transmit simultaneously. In this situation, both transmissions are damaged and the hosts must retransmit at a later time.

Polling. In the polling transmission method, a primary workstation checks a secondary workstation regularly at predetermined times to see if it has data to transmit. Secondary

workstations are not permitted to transmit until they are given permission by the primary host. Polling is commonly used in large mainframe environments where hosts are polled to see if they need to transmit. Because polling is very inexpensive, it is also used by networks that are low-level and peer-to-peer types.

Token-Passing. Used in Token Ring, FDDI, and Attached Resource Computer Network (ARCnet) networks, stations in token-passing networks cannot transmit until they receive a special frame called a *token*. This arrangement prevents the collision problems that are present in CSMA. Token-passing networks will work well if large, bandwidth-consuming applications are commonly used on the network.

Token Ring and IEEE 802.5 are two principal examples of token-passing networks. Token-passing networks move a small frame, called a token, around the network. Possession of this token grants the right to transmit. If a node that is receiving the token has no information to send, it passes the token to the next end station. Each station can then hold the token for a maximum period of time, as determined by the 802.5 specification.

Unlike CSMA/CD networks (such as Ethernet), token-passing networks are deterministic, which means that it is possible to calculate the maximum time that will pass before any end station will be able to transmit. This feature and the fact that collisions cannot occur make Token Ring networks ideal for applications where the transmission delay must be predictable and robust network operation is important. Factory automation environments are examples of such applications.

LAN Transmission Methods

There are three flavors of LAN transmission methods:

- *Unicast.* The packet is sent from a single source to a single destination address.
- *Multicast.* The source packet is copied and sent to specific multiple destinations on the network.
- *Broadcast.* The packet is copied and sent to all of the nodes on a network or segment of a network.

LAN Topologies

A network topology defines the manner in which the network devices are organized to facilitate communications. A LAN topology defines this transmission manner for a Local Area Network.

There are five common LAN topologies — BUS, RING, STAR, TREE, and MESH.

BUS Topology. In a BUS topology, all the transmissions of the network nodes travel the full length of cable and are received by all other stations (see Figure 3.17). Ethernet primarily uses this topology. This topology does have some faults. For example, when any station on the bus experiences cabling termination errors, the entire bus can cease to function.



Figure 3.17: A BUS topology.

RING Topology. In a RING topology, the network nodes are connected by unidirectional transmission links to form a closed loop (see Figure 3.18). Token Ring and FDDI both use this topology.

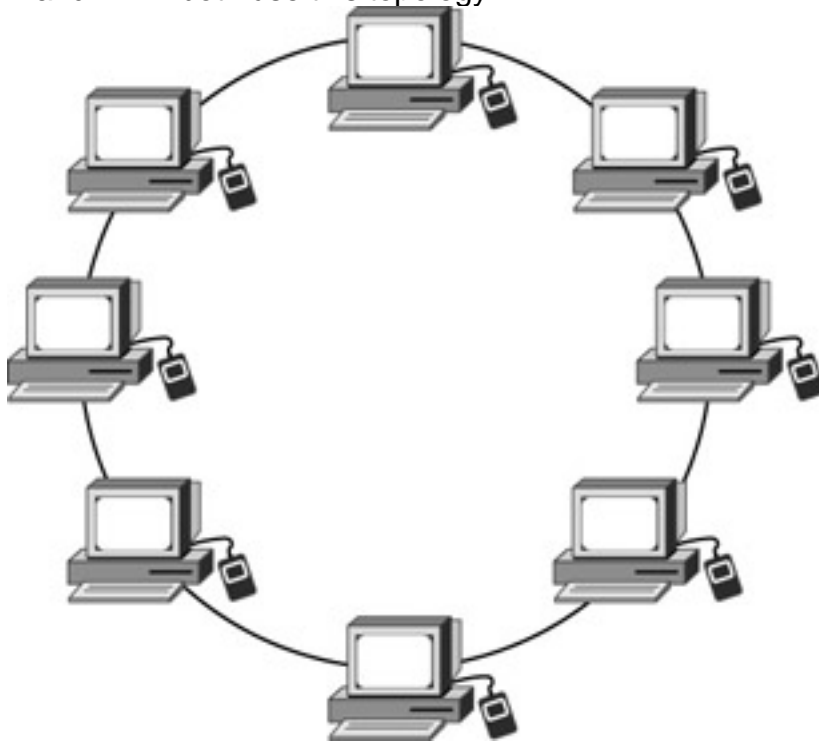


Figure 3.18: A RING topology.

STAR Topology. In a STAR topology, the nodes of a network are connected to a central LAN device directly (see Figure 3.19). Here is where it gets a little confusing: The logical BUS and RING topologies that were previously described are often implemented physically in a STAR topology. Although Ethernet is logically thought of as a BUS topology (its first implementations were Thinnet and Thicknet on a BUS), 10BaseT is actually wired as a STAR topology, which provides more resiliency for the entire topology when a station experiences errors.

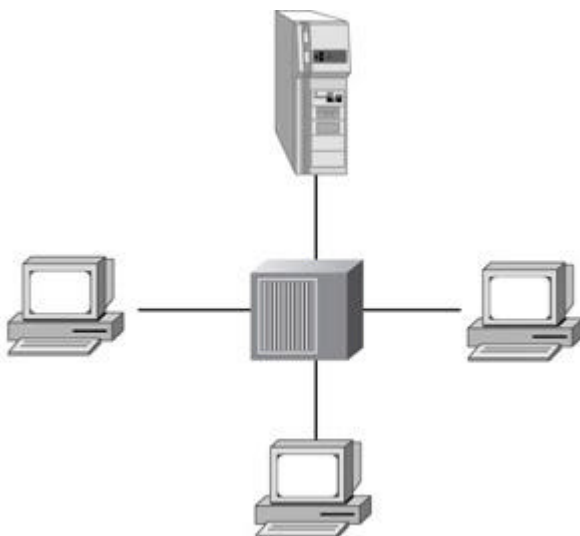


Figure 3.19: A STAR topology.

TREE topology. The TREE topology (as shown in Figure 3.20) is a BUS-type topology where branches with multiple nodes are possible.

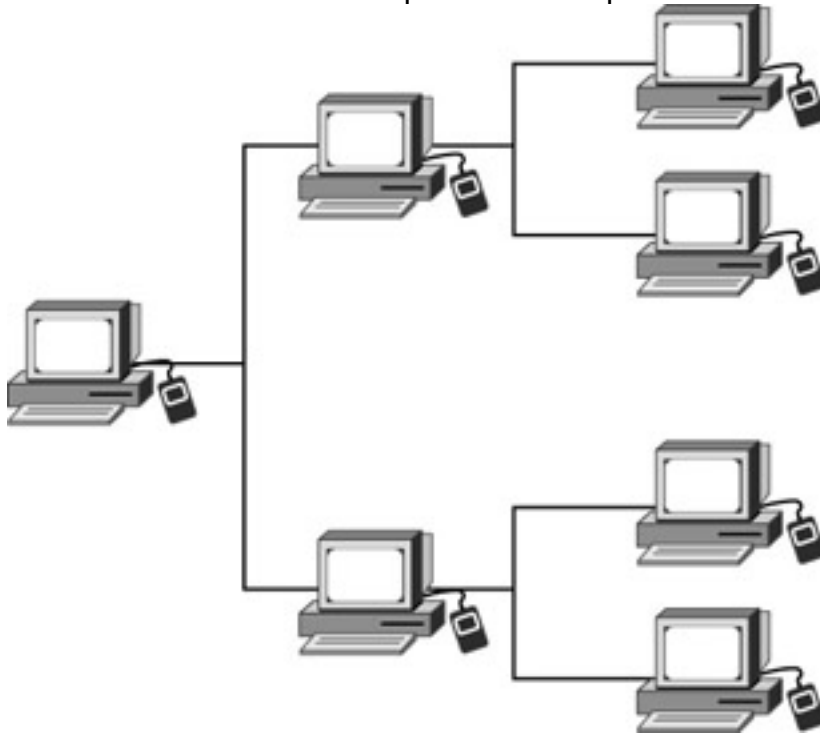


Figure 3.20: A TREE topology.

MESH Topology. In a MESH topology, all the nodes are connected to every other node in a network (see Figure 3.21). This topology may be used to create backbone redundant networks. A *full MESH* topology has every node connected to every other node. A *partial MESH* topology may be used to connect multiple full MESH networks together.

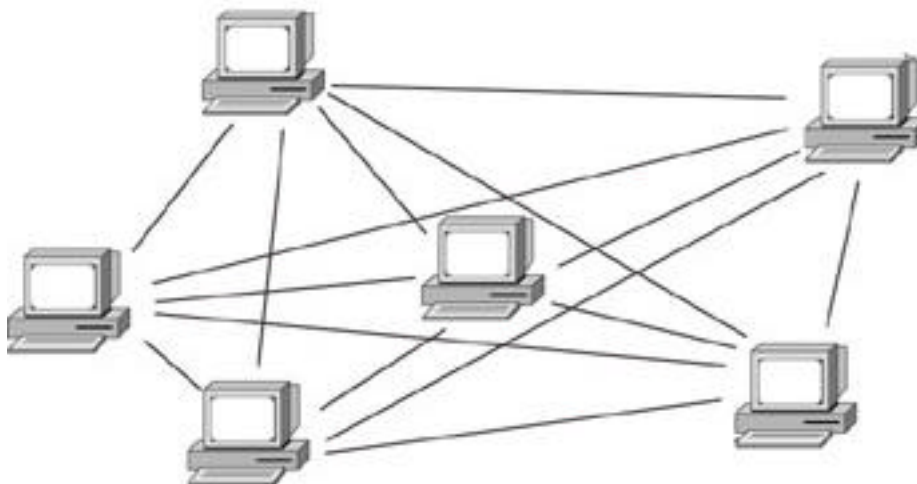


Figure 3.21: A MESH topology.

LAN Media Access Methods

LAN media access methods control the use of a network (its physical and data link layers). Now we will discuss the basic characteristics of Ethernet, ARCnet, Token Ring, and FDDI — the LAN technologies that account for virtually all deployed LANs.

Ethernet. The Ethernet media access method transports data to the LAN using CSMA/CD. Currently, this term is often used to refer to all CSMA/CD LANs. Ethernet

was designed to serve in networks with sporadic, occasionally heavy traffic requirements.

Ethernet defines a BUS-topology LAN with three cable standards:

1. *Thinnet*. Known as 10Base2, it is a coaxial cable with segments of up to 185 meters.
2. *Thicknet*. Known as 10Base5, it is a coaxial cable with segments of up to 500 meters.
3. *Unshielded Twisted Pair*. In UTP, all hosts are connected using an unshielded twisted pair cable that is connected to a central device (such as a hub or switch). UTP has three common variations: 10BaseT operates at 10 MBps, 100BaseT (Fast Ethernet) operates at 100 MBps, and 1000BaseT (Gigabit Ethernet) operates at 1 GBps.

Figure 3.22 shows an Ethernet network segment.



Figure 3.22: An Ethernet segment.

Dueling Ethernets

Digital, Intel, and Xerox teamed up to create the original Ethernet I standard in 1980. In 1984, they followed up with the release of Ethernet II. The Institute of Electrical and Electronic Engineers (IEEE) founded the 802.3 subcommittee to come up with an Ethernet standard that was almost identical to the Ethernet II version. These two standards differ only in their descriptions of the Data Link Layer: Ethernet II has a "Type" field, whereas 802.3 has a "Length" field. Otherwise, both are the same in their Physical Layer specifications and MAC addressing.

ARCnet. ARCnet is one of the earliest LAN technologies. It uses a token-passing access method in a STAR technology on coaxial cable. ARCnet provides predictable, if not slow network performance. One issue with ARCnet stations is that the node address of each station has to be manually set during installation, thus creating the possibility of duplicate and conflicting nodes.

Token Ring. The Token Ring network was originally developed by IBM in the 1970s. It is second only to Ethernet in general LAN popularity. The term *Token Ring* refers to both IBM's Token Ring network and IEEE 802.5 networks. All end stations are attached to a device called a Multistation Access Unit (MSAU). One station on a Token Ring network is designated the *Active Monitor*. The Active Monitor makes sure that there are not more than one token on the Ring at any given time. If a transmitting station fails, it probably is not able to remove a token as it makes its way back onto the ring. In this case, the Active monitor will step in and remove the token and generate a new one.

Fiber Distributed Data Interface (FDDI). Like Token Ring, FDDI is a token-passing media access topology. It consists of a dual Token Ring LAN that is operating at 100

MBps over Fiber Optic cabling. FDDI employs a token-passing media access with dual counter-rotating rings, with only one ring active at any given time. If a break or outage occurs, the ring will then wrap back the other direction, keeping the ring intact.

The following are the major advantages of FDDI:

- It can operate over long distances, at high speeds, and with minimal electromagnetic or radio frequency interference present.
- It provides predictable, deterministic delays and permits several tokens to be present on the ring concurrently.

The major drawbacks of FDDI are its expense and the expertise needed to implement it properly.

Copper Distributed Data Interface (CDDI) can be used with a UTP cable to connect servers or other stations into the ring instead of using fiber optic cable. Unfortunately, this introduces the basic problems that are inherent with the use of copper cabling (length and interference problems).

LAN Devices

Repeaters. *Repeaters* amplify the data signals to extend the length of a network segment, and they help compensate for signal deterioration due to attenuation. They do not add any intelligence to the process — they do not filter packets, examine addressing, or change anything in the data.

Hubs. *Hubs* are often used to connect multiple LAN devices (such as servers and workstations) together into a device called a concentrator. Hubs can be considered *multi-port repeaters*. See Figure 3.23.

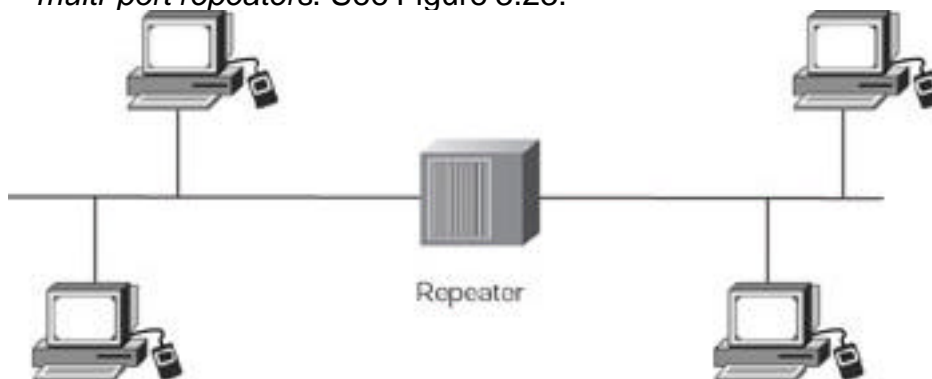


Figure 3.23: A repeater or hub.

Repeaters and Hubs operate at the Physical Layer of the OSI model.

Bridges. *Bridges* also amplify the data signals and add some intelligence. A bridge forwards the data to all other network segments if the Media Access Control (MAC) or hardware address of the destination computer is not on the local network segment. If the destination computer is on the local network segment, it does not forward the data. Because bridges operate at the Data Link Layer, Layer 2, they do not use IP addresses due to the fact that the information is attached in the Network Layer, Layer 3. One issue with bridges is that because a bridge automatically forwards all broadcast traffic, an error state known as a *broadcast storm* can develop, bringing all of the devices to a halt. Figure 3.24 shows a bridged network.

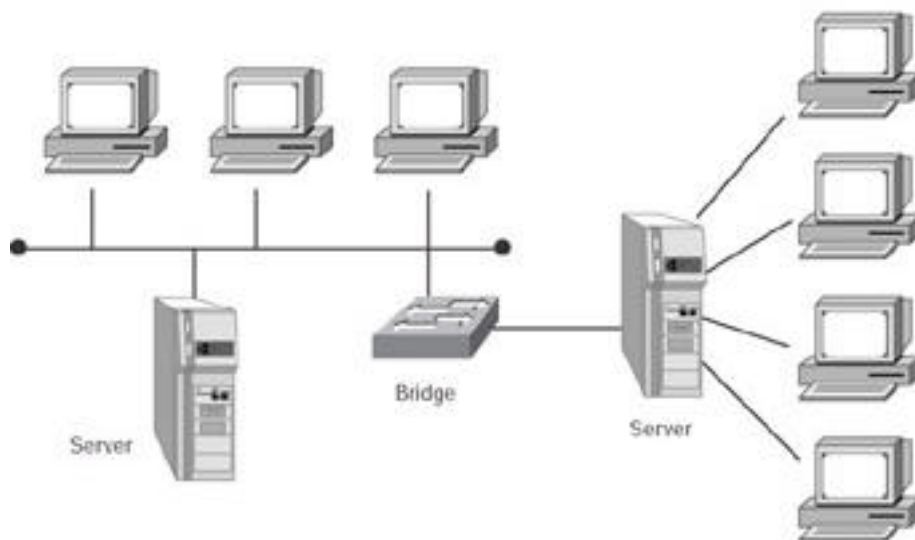


Figure 3.24: A bridged network.

Switches. A *switch* is similar to a bridge or a hub, except that a switch will only send the data packet to the specific port where the destination MAC address is located, rather than all ports that are attached to the hub or bridge. Switches can be thought of as a fast, *multi-port bridge*. Switches primarily operate at the *Data Link Layer, Layer 2*, although intelligent, extremely fast Layer 3 switching techniques (combing, switching, and routing) are being more frequently used. Tag Switching, Netflow Switching, and Cisco Express Forwarding are some examples. Figure 3.25 shows a switched network.

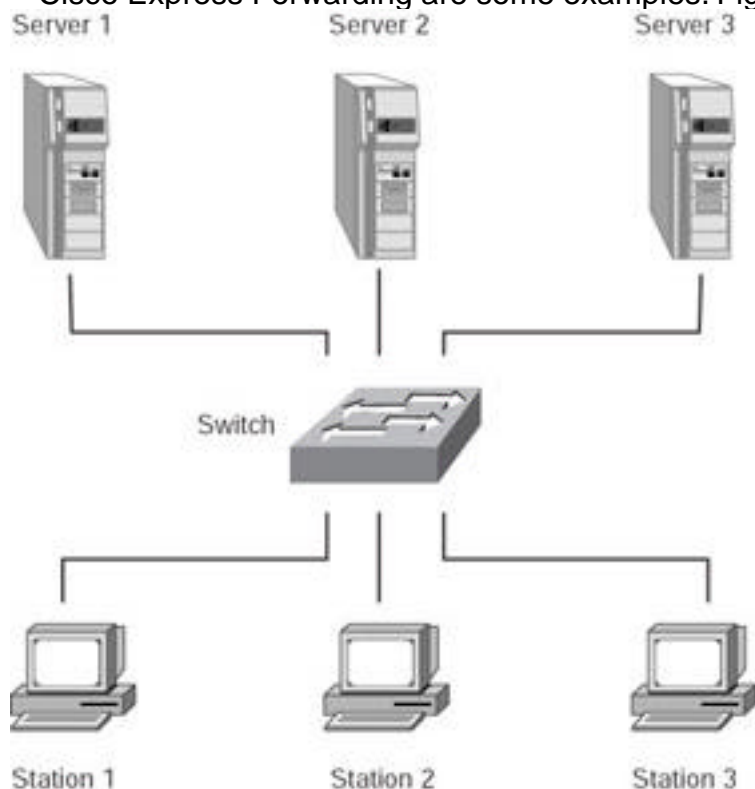


Figure 3.25: A switched network.

Routers. *Routers* add even more intelligence to the process of forwarding data packets. A router opens up a data packet, reads either the hardware or network address (*IP address*) before forwarding it, and then only forwards the packet to the network to which the packet was destined. This prevents unnecessary network traffic

from being sent over the network by blocking broadcast information and traffic to unknown addresses. This blocking does, however, create more overhead in the routing device than exists in a bridge. Routers operate at the Network Layer, Layer 3, and the lower levels of the OSI protocol model. Figure 3.26 shows a routed network.

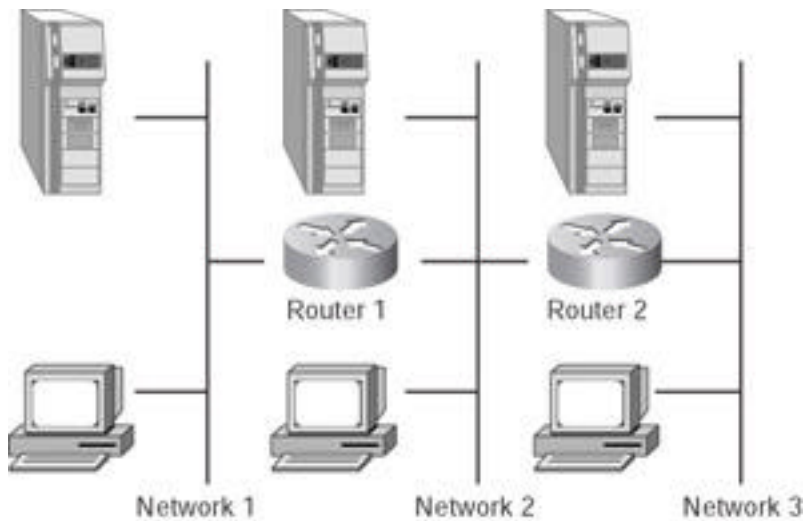


Figure 3.26: A routed network.

Broadcasts

A *broadcast* is a data packet that is sent to all network stations at the same time. Broadcasts are an essential function built into all protocols. When servers need to send data to all the other hosts on the network segment, network broadcasts are very useful. If a lot of broadcasts are occurring on a network segment, however, network performance can be seriously degraded. It is important to use these devices properly and to segment the network correctly.

Gateways. Gateways are primarily software products that can be run on computers or other network devices. They can be *multi-protocol* (link different protocols) and can examine the entire packet. *Mail gateways* are used to link dissimilar mail programs. Gateways can also be used to translate between two dissimilar network protocols.

Asynchronous Transfer Mode (ATM) Switches. Although ATM switches are more commonly used for WANs, they are beginning to be used extensively in LANs. ATM switches use a cell relay technology that combines the advantages of both conventional circuit and packet-based systems, thus providing high-speed cell switching. We will describe ATM in greater detail later when dealing with WAN Technology.

LAN Extenders. A LAN *extender* is a *remote-access, multi-layer switch* that is connected to a host router (see Figure 3.27). LAN extenders forward traffic from all the standard network-layer protocols (such as IP, IPX, and Appletalk), and filter traffic based on the MAC address or network-layer protocol type. LAN extenders scale well because the host router filters out unwanted broadcasts and multicasts. LAN extenders, however, are not capable of segmenting traffic or creating security firewalls.

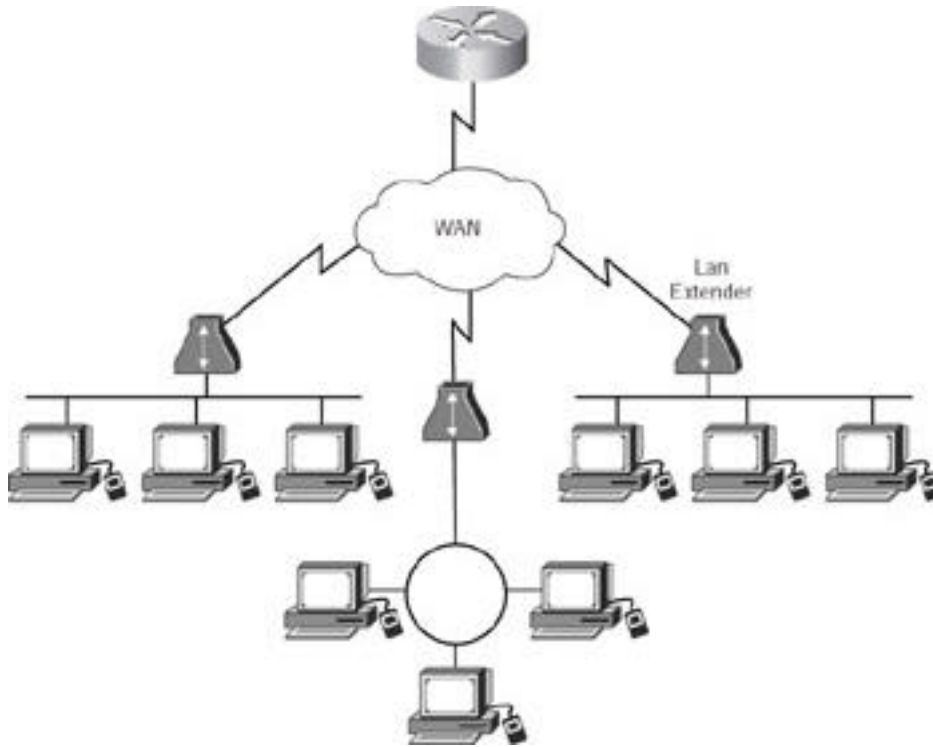


Figure 3.27: A LAN extender.

WAN Technologies

To become more familiar with the various types of WAN technologies, you must understand WAN protocols, topologies, and devices.

WAN Protocols and Topologies

Like LAN protocols, WAN protocols are the rules for communicating between computers on a WAN. Because the WAN is more often used for connecting networks together than a LAN, these protocols address the issues involved with communications between many large and disparate networks. Almost every WAN protocol is designed to run on a specific WAN topology. While some topologies can combine protocols, the list in the next section shows which protocol is native to and runs on which topology.

Private Circuit Technologies

Private circuits evolved before packet switching networks. A private circuit network is a dedicated analog or digital *point-to-point connection* joining geographically diverse networks. Examples of private circuit networks are dedicated lines, leased lines, Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP), ISDN, and xDSL.

Dedicated Line. A dedicated line is defined as a communications line that is indefinitely and continuously reserved for transmissions, rather than being switched on and off as transmission is required.

Leased Line. A dedicated line can be reserved by a communications carrier for a customer's private use. A leased line is a type of dedicated line.

Types and speeds of standard leased lines are

- Digital Signal Level 0 (*DS-0*). The framing specification used in transmitting digital signals over a single channel at 64 Kbps on a T1 facility.
- Digital Signal Level 1 (*DS-1*). The framing specification used in transmitting digital signals at 1.544 MBps on a T1 facility (in the United States) or at 2.108 MBps on an E1 facility (in Europe).

- Digital Signal Level 3 (DS-3). The framing specification used for transmitting digital signals at 44.736 MBps on a T3 facility.
- *T1*. Transmits DS-1—formatted data at 1.544 MBps through a telephone-switching network.
- *T3*. Transmits DS-3—formatted data at 44.736 MBps through a telephone-switching network.
- *E1*. Wide-area digital transmission scheme predominantly used in Europe that carries data at a rate of 2.048 MBps.
- *E3*. Same as E1 (both can be leased for private use from common carriers), but it carries data at a rate of 34.368 MBps.

Serial Line IP (SLIP). Serial Line IP (SLIP) is an industry standard that was developed in 1984 to support TCP/IP networking over low-speed serial interfaces in Berkeley Unix computers. Using the Windows NT RAS service, Windows NT computers can use TCP/IP and SLIP to communicate with remote hosts.

Point-to-Point Protocol (PPP). Point-to-Point Protocol (PPP) is a specification that is used by data communications equipment for transmitting over dial-up and dedicated links. It enables multi-vendor operability and was originally proposed as a standard to improve on Serial Line Internet Protocol (SLIP), which only supported IP. PPP takes the specifications of SLIP and builds on them by adding login, password, and error correction capabilities. PPP is a Data Link Layer protocol and has built-in security mechanisms such as CHAP and PAP.

Integrated Services Digital Network (ISDN). Integrated Services Digital Network (ISDN) is a combination of digital telephony and data-transport services that are offered by telecommunications carriers. It consists of a digitization of the telephone network by permitting voice and other digital services (data, music, video, and so forth) to be transmitted over existing telephone wires. It has recently been overtaken by the more popular xDSL types.

Digital Subscriber Line (xDSL). Digital Subscriber Line (xDSL) uses existing twisted pair telephone lines to transport high bandwidth data to remote subscribers. It consists of a point-to-point public network that is accessed through an in-home copper phone wire. It is rapidly becoming the standard for inexpensive remote connectivity.

The following are examples of the types of xDSL:

- Asymmetric Digital Subscriber Line (*ADSL*). ADSL is designed to deliver more bandwidth downstream (from the central office to the customer site) than upstream. Downstream rates range from 1.5 to 9 MBps, while upstream bandwidth ranges from 16 to 640 Kbps. ADSL transmissions work at distances of up to 18,000 feet over a single copper twisted pair (although 14,400 feet is the maximum practical length).
- Single-Line Digital Subscriber Line (*SDSL*). SDSL delivers 1.544 MBps both downstream and upstream over a single copper twisted pair. This use of a single twisted pair limits the operating range of SDSL to 10,000 feet.
- High-Rate Digital Subscriber Line (*HDSL*). HDSL delivers 1.544 MBps of bandwidth each way over two copper twisted pairs. Because HDSL provides T1 speed, telephone companies have been using HDSL to provide local access to T1 services whenever possible. The operating range of HDSL is limited to 12,000 feet.
- Very-high data-rate Digital Subscriber Line (*VDSL*). VDSL delivers 13 to 52 MBps downstream and 1.5 to 2.3 MBps upstream over a single twisted copper pair. The operating range of VDSL is limited to 1,000 to 4,500 feet.

Circuit-Switched Versus Packet-Switched Networks

Circuit-Switched Networks. *Circuit-switching* is defined as a switching system in which a dedicated physical circuit path must exist between the sender and receiver for the duration of the transmission, or the “call.” A *circuit-switched network* describes a type of WAN that consists of a physical, permanent connection from one point to another. This is older technology than packet-switching, discussed next, but it is the main choice for communications that need to be “on” constantly and have a limited scope of distribution (one transmission path only). This network type is used heavily in telephone company networks.

Packet-Switched Networks. *Packet-switching* is defined as a networking method where nodes share bandwidth with each other by sending small data units called packets. A *packet-switched network* (PSN) or (PSDN) is a network that uses packet-switching technology for data transfer. Unlike circuit-switched networks, the data in packet-switched networks is broken up into packets and then sent to the next destination, based on the router’s understanding of the best available route. At that destination, the packets are reassembled based on their originally assigned sequence numbers. Although the data is man-handled a lot in this process, it creates a network that is very resilient to error. Table 3.6 is a list of the basic differences between circuit and packet switching.

Table 3.6: Circuit Switching versus Packet Switching

Circuit Switching	Packet Switching
Constant traffic	Bursty traffic
Fixed delays	Variable delays
Connection-oriented	Connectionless
Sensitive to loss of connection	Sensitive to loss of data
Voice-oriented	Data-oriented

Note To confuse you even further, an additional new switching type has been introduced called *message switching*. Message Switching is a switching technique that involves the transmission of messages from node to node through a network. The message is stored at each node until a forwarding path is available.

Packet-Switched Technologies

Packet-switched networks can be far more cost effective than dedicated circuits because they create *virtual circuits*, which are used as needed, rather than supplying a continuous dedicated circuit. Examples of packet switching networks are X.25, Link Access Procedure-Balanced (LAPB), Frame Relay, Switched Multimegabit Data Systems (SMDS), Asynchronous Transfer Mode (ATM), and Voice over IP (VoIP).

X.25. The first packet-switching network, X.25, defines the point-to-point communication between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE , commonly a modem) or a Data Service Unit/Channel Service Unit (DSU/CSU), which supports both switched virtual circuits (SVCs) and permanent virtual circuits (PVCs). X.25 defines how WAN devices are established and maintained. X.25 was designed to operate effectively regardless of the type of systems that are connected to the network. It has become an international standard and is currently much more prevalent overseas than in the United States.

Link Access Procedure—Balanced (LAPB). Created for use with X.25, *LAPB* defines frame types and is capable of retransmitting, exchanging, and acknowledging frames as well as detecting out-of-sequence or missing frames.

Frame Relay. *Frame Relay* is a high performance WAN protocol that operates at the Physical and Data Link layers of the OSI model. Originally designed for use across ISDN interfaces, it is currently used with a variety of other interfaces and is a major standard for high-speed WAN communications. Frame Relay is an upgrade from X.25 and LAPB. It is the fastest of the WAN protocols listed because of its simplified framing approach, which utilizes no error correction. Frame Relay uses SVCs, PVCs, and Data Link Connection Identifiers (DLCIs) for addressing. Because it requires access to a high-quality digital network infrastructure, it is not available everywhere.

Virtual Circuits

Switched virtual circuits (SVCs) are virtual circuits that are dynamically established on demand and are torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. SVCs have three phases — circuit establishment, data transfer, and circuit termination (tear down). Permanent virtual circuits (PVCs) are virtual circuits that are permanently connected. PVCs save the bandwidth that is associated with circuit establishment and tear down.

Switched Multimegabit Data Service (SMDS). *SMDS* is a high-speed technology that is used over public switched networks. It is provided for companies that need to exchange large amounts of data with other enterprises over WANs on a “bursty,” or noncontinuous basis, by providing connectionless bandwidth upon demand.

Asynchronous Transfer Mode (ATM). *ATM* is a very high bandwidth, low-delay technology that uses both switching and multiplexing. It uses 53-byte, fixed size cells instead of frames like Ethernet. It can allocate bandwidth upon demand, making it a solution for bursty applications. ATM requires a high-speed, high-bandwidth medium like fiber optics. ATM is taking the place of FDDI in the campus backbone arena because it can run in both WAN and LAN environments at tremendous speeds.

Voice over IP (VoIP). *VoIP* is one of several digital, multi-service access IP technologies that combines many types of data (such as, voice, audio, and video) into a single IP packet, which provides major benefits in the areas of cost, interoperability, and performance. VoIP is a very new area of technology, and has exciting, far-reaching potential.

Other Important WAN Protocols

Synchronous Data Link Control (SDLC). SDLC is a protocol that was created by IBM to make it easier for their mainframes to connect to their remote offices. SDLC defines and uses a *polling* media-access method. It consists of a primary station, which controls all communications, and one or more secondary stations. SDLC is based on dedicated, leased lines with permanent physical connections, and it has evolved into the HDLC and Link Access Procedure—Balanced (LAPB) protocols. This protocol operates at the Data Link Layer.

High-Level Data Link Control (HDLC). Derived from SDLC, HDLC specifies the data encapsulation method on synchronous serial links using frame characters and checksums. The ISO created the HDLC standard to support both point-to-point and multi-point configurations. Vendors often implement HDLC in different ways, which sometimes makes the HDLC protocol incompatible. It also operates at the Data Link Layer.

High Speed Serial Interface (HSSI). HSSI is a DTE/DCE interface that was developed to address the need for high speed communications over WAN links. It

defines the electrical and physical interfaces to be used by DTE/DCEs and operates at the Physical Layer of the OSI model.

WAN Devices

WAN Devices are the elements that enable the use of WAN protocols and topologies. The following are examples of these device types:

- *Routers*. Although previously described as a LAN device, in the WAN environment, routers are extremely important, especially for IP Internet traffic.
- *Multiplexors*. Commonly referred to as a mux, a multiplexor is a device that enables more than one signal to be sent out simultaneously over one physical circuit.
- *WAN Switches*. Wan Switches are multi-port, networking devices that are used in carrier networks. They operate at the Data Link Layer and typically switch Frame Relay, X.25, and SMDS. These switches connect private data over public data circuits by using digital signals.
- *Access Servers*. An Access Server is a server that provides dial-in and dial-out connections to the network. These are typically asynchronous servers that enable users to dial in and attach to the LAN. Cisco's AS5200 series of communication servers are an example of such devices.
- *Modems*. A modem is a device that interprets digital and analog signals, which enables data to be transmitted over voice grade telephone lines. The digital signals are then converted to an analog form, which is suitable for transmission over an analog communications medium. These signals are then converted back to their digital form at the destination.
- *Channel Service Unit (CSU)/Data Service Unit (DSU)*. This is a digital interface device that is used to terminate the physical interface on a DTE device (such as a terminal) to the interface of a DCE device (such as a switch) in a switched carrier network. These devices connect to the closest telephone company switch in a central office (CO).

Figure 3.28 shows a network that allows Internet access with several different devices.

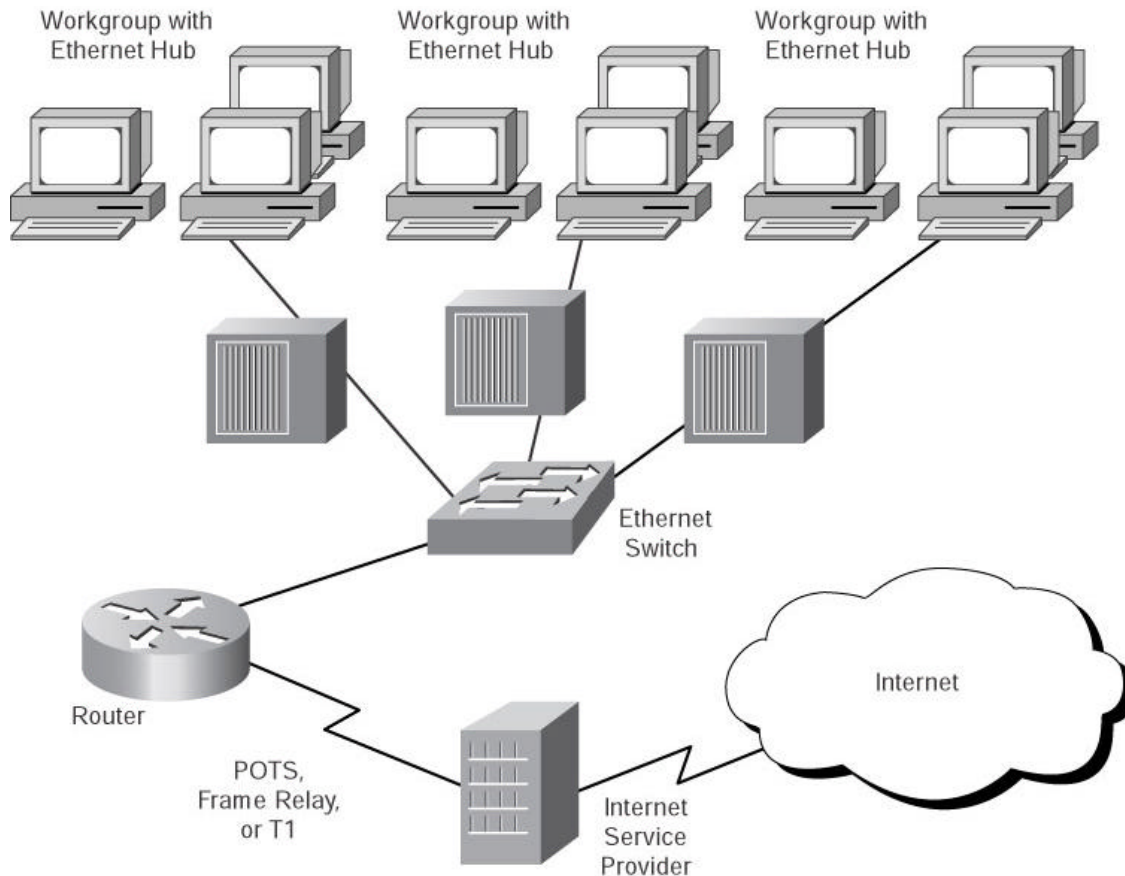


Figure 3.28: Shared Internet access with WAN and LAN devices.

Remote Access Technologies

Remote Access Technologies can be defined as those data networking technologies that are uniquely focused on providing the remote user (telecommuter, Internet/intranet user, or extranet user/partner) with access into a network, while striving to maintain the principle tenets of Confidentiality, Availability, and Integrity.

There are many obvious advantages to employing secure remote network access, such as the following:

- Reducing networking costs by using the Internet to replace expensive dedicated network lines
- Providing employees with flexible work styles such as telecommuting
- Building more efficient ties with customers, suppliers, and employees

Remote Access Types

While several of these Remote Access Types share common WAN protocols, they are listed here to indicate their importance in the area of remote access security.

Asynchronous Dial-Up Access. This is how most everyone accesses the Internet. It is the most common remote access method for personal remote users because it uses the existing public switched telephone network to access an ISP.

Integrated Services Digital Network (ISDN). Described in WAN Technologies, ISDN is a communication protocol, which is offered by telephone companies, and permits telephone networks to carry data, voice, and other source traffic. ISDN has two interface types: Basic Rate Interface (BRI), which is composed of two B channels and one D channel; and Primary Rate Interface (PRI), which consists of a single 64 Kbps D channel plus 23 (T1) or 30 (E1) B channels for voice or data.

xDSL. Described in WAN Technologies, xDSL uses regular telephone lines for high-speed digital access.

Cable Modems. A cable modem provides high speed access to the Internet by the cable company. All cable modems share a single coax line to the Internet, therefore throughput varies according to how many users are currently using the service. It is also considered one of the most insecure of the Remote Access Types because the local segment is typically not filtered or firewalled.

Wireless Technology. Wireless technology is probably the fastest growing area of network connectivity. Experts estimate that the number of Internet connected Personal Digital Assistants (PDAs, such as the Palm Pilot) will eclipse the number of personal computers in use in a few years. Security is an extreme concern here, because all wireless technologies (mobile phones, satellite transmissions, and so forth) are inherently susceptible to interception and eavesdropping. Encryption standards are rapidly being developed to combat this problem.

Some Remote Access Security Methods

Restricted Address. This procedure filters out unauthorized users based on their source protocol address (IP or other LAN protocol). It enables incoming calls only from specific addresses on an approved list. You should remember, however, that this procedure authenticates the node; it is not a user authentication method.

Caller ID. Caller ID checks the incoming phone number of the caller against an approved phone list before accepting the session. This is one of the most common security methods because it is very hard to defeat. Its major drawback is that it is hard to administer for traveling users (such as users calling from a different hotel every night).

Callback. In a callback scenario, a user attempting to initiate the session supplies a password or some type of identifying code. The Access Server then hangs up and calls the user back at a predetermined phone number. Again, this procedure authenticates the node, not the user, and is difficult to administer in traveling situations.

Remote Identification and Authentication Technologies

Remote Identification and Authentication Technologies are the processes that are necessary to securely verify *who* is remotely communicating. Because remote access presents security professionals with many issues, a variety of technologies have been developed to provide solutions to these issues. Identification embodies the concept of identifying who is attempting the connection, and Authentication embodies the concept of establishing a level of trust, which includes nonrepudiation of the network session.

Remote Node Security Protocols

The following are the two most common remote node security protocols:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

Password Authentication Protocol (PAP). *Password Authentication Protocol (PAP)* is a remote security protocol that provides identification and authentication of the node attempting to initiate the remote session. PAP uses a “static,” replayable password for this authentication, which is now considered a weak process. In addition, PAP also does not encrypt the User ID or password during communication.

Challenge Handshake Authentication Protocol (CHAP). The *Challenge Handshake Authentication Protocol (CHAP)* is the next evolution of PAP, which uses a stronger authentication process: a nonreplayable, “challenge/response” dialog that verifies the identity of the node attempting to initiate the remote session. CHAP is often used to enable network-to-network communications and is commonly used by remote access servers and xDSL, ISDN, and cable modems.

Remote Access Authentication Systems

As the demand for large remote access networks increased, two security administration systems, TACACS and RADIUS, emerged to provide security professionals with more resources. These systems provide a centralized database, which maintains user lists, passwords, and user profiles that can be accessed by remote access equipment on a network. These systems are “standards-based,” which means they are interoperable with other systems of the same type.

Common Remote Access Authentication Systems include

- Terminal Access Controller Access Control System (TACACS)
- TACACS+ (TACACS with additional features, including the use of two-factor authentication)
- Remote Authentication Dial-In User Server (RADIUS)

Terminal Access Controller Access Control System (TACACS). *Terminal Access Controller Access Control System (TACACS)* is an authentication protocol that provides remote access authentication and related services, such as event logging. In a TACACS system, user passwords are administered in a central database rather than in individual routers, which provides an easily scalable network security solution. A TACACS-enabled network device prompts the remote user for a username and static password, then the TACACS-enabled device queries a TACACS server to verify that password. TACACS does not support prompting for a password change or use of dynamic password tokens.

TACACS was superseded by Terminal Access Controller Access Control System Plus (TACACS+). TACACS+ is a proprietary Cisco enhancement to TACACS that provides the following additional features:

- The use of two-factor password authentication
- The user has the ability to change his password
- The ability for security tokens to be resynchronized
- Better audit trails and session accounting

TACACS and TACACS+ services are in the public domain and can be bundled in the operating systems of network devices.

Remote Authentication Dial-in User Service (RADIUS). RADIUS was adopted as standard protocol by the Internet Engineering Task Force (IETF). It provides similar user authentication (including the use of dynamic passwords) and password management as a TACACS+ enabled system. RADIUS is often used as a stepping stone to a more robust TACACS+ system.

RADIUS is a distributed client/server system wherein the clients send their authentication requests to a central RADIUS server that contains all of the user authentication and network service access information (network ACLs). RADIUS is a fully open protocol, is distributed in source code format, and can be modified to work with any security system that is currently available on the market. It can also be used with TACACS+ and Kerberos and provides CHAP remote node authentication.

RADIUS does not support the following protocols:

- AppleTalk Remote Access Protocol (ARAP)
- NetBIOS Frame Protocol Control Protocol (NBFCP)
- NetWare Asynchronous Services Interface (NASI)
- X.25 PAD connections

In addition, RADIUS also does not provide two-way authentication, and therefore is not commonly used for router-to-router authentication.

Sample Questions

Answers to the Sample Questions for this and the other chapters are found in Appendix C.

1. Which of the following is NOT a type of data network? ?
 - A. LAN
 - B. WAN
 - C. MAN
 - D. GAN
2. Which of the following is NOT a network cabling type? ?
 - A. Twisted Pair
 - B. Token Ring
 - C. Fiber Optic
 - D. Coaxial
3. Which of the following is NOT a property of a Packet Filtering Firewall? ?
 - A. Considered a first generation firewall
 - B. Uses ACLs
 - C. Operates at the Application Layer
 - D. Examines the source and destination addresses of the incoming packet
4. Which of the following is NOT a remote computing technology? ?
 - A. PGP
 - B. ISDN
 - C. Wireless
 - D. xDSL
5. A firewall that performs stateful inspection of the data packet across all layers is considered a ?
 - A. First generation firewall
 - B. Second generation firewall
 - C. Third generation firewall
 - D. Fourth generation firewall
6. RAID refers to the ?
 - A. Redundant Arrays of Intelligent Disks
 - B. Redundant And fault tolerant Internetworking Devices
 - C. Rapid And Inexpensive Digital tape backup

- D. Remote Administration of Internet Domains
7. Which of the following is NOT a true statement about Network Address Translation (NAT)? ?
- A. NAT is used when corporations want to use private addressing ranges for internal networks.
 - B. NAT is designed to mask the true IP addresses of internal systems.
 - C. Private addresses can easily be globally routable.
 - D. NAT translates private IP addresses to registered "real" IP addresses.
8. What does LAN stand for? ?
- A. Local Arena News
 - B. Local Area Network
 - C. Layered Addressed Network
 - D. Local Adaptive Network
9. What does CSMA stand for? ?
- A. Carrier Station Multi-port Actuator
 - B. Carrier Sense Multiple Access
 - C. Common Systems Methodology Applications
 - D. Carrier Sense Multiple Attenuation
10. Which is NOT a property of a packet-switched network? ?
- A. Packets are assigned sequence numbers
 - B. Characterized by "bursty" traffic
 - C. Connection-oriented network
 - D. Connection-less network
11. Which is NOT a layer in the OSI architecture model? ?
- A. Transport
 - B. Internet
 - C. Data Link
 - D. Session
12. Which is NOT a layer in the TCP/IP architecture model? ?

- A. Internet
B. Application
C. Host-to-host
D. Session
13. Which is NOT a backup method type? ?
- A. Differential
B. Full
C. Reactive
D. Incremental
14. What does TFTP stands for? ?
- A. Trivial File Transport Protocol
B. Transport For TCP/IP
C. Trivial File Transfer Protocol
D. Transport File Transfer Protocol
15. What does the Data Encapsulation in the OSI model do? ?
- A. Creates seven distinct layers
B. Wraps data from one layer around a data packet from an adjoining layer
C. Provides “best effort” delivery of a data packet
D. Makes the network transmission deterministic
16. What is NOT a feature of TACACS+? ?
- A. Enables two-factor authentication
B. Replaces older frame relay-switched networks
C. Enables a user to change passwords
D. Resynchronizes security tokens
17. What is NOT true of a star-wired topology? ?
- A. Cabling termination errors can crash the entire network.
B. The network nodes are connected to a central LAN device.
C. It has more resiliency than a BUS topology.
D. 10BaseT Ethernet is star-wired.

18. FDDI uses what type of network topology? ?
- A. BUS
 - B. RING
 - C. STAR
 - D. MESH
19. What does the protocol ARP do? ?
- A. Takes a MAC address and finds an IP address to match it with
 - B. Sends messages to the devices regarding the health of the network
 - C. Takes an IP address and finds out what MAC address it belongs to
 - D. Facilitates file transfers
20. What does the protocol RARP do? ?
- A. Takes a MAC address and finds an IP address to match it with
 - B. Sends messages to the devices regarding the health of the network
 - C. Takes an IP address and finds out what MAC address it belongs to
 - D. Facilitates file transfers
21. What is the protocol that supports sending and receiving email called? ?
- A. SNMP
 - B. SMTP
 - C. ICMP
 - D. RARP
22. Which of the following is NOT a VPN remote computing protocol? ?
- A. PPTP
 - B. L2F
 - C. L2TP
 - D. UTP
23. Which of the following is NOT a property of CSMA? ?
- A. The workstation continuously monitors the line.
 - B. The workstation transmits the data packet when it thinks the

line is free.

- C. Workstations are not permitted to transmit until they are given permission from the primary host.
 - D. It does not have a feature to avoid the problem of one workstation dominating the conversation.
24. Which of the following is NOT a property of Token Ring networks? ?
- A. Workstations cannot transmit until they receive a token.
 - B. These networks were originally designed to serve large, bandwidth-consuming applications.
 - C. These networks were originally designed to serve sporadic and only occasionally heavy traffic.
 - D. All end stations are attached to a MSAU.
25. Which is NOT a property of Fiber Optic cabling? ?
- A. Carries signals as light waves
 - B. Transmits at higher speeds than copper cable
 - C. Easier to tap than copper cabling
 - D. Very resistant to interference
26. Which is NOT a property of a bridge? ?
- A. Forwards the data to all other segments if the destination is not on the local segment
 - B. Operates at Layer 2, the Data Link Layer
 - C. Operates at Layer 3, the Network Layer
 - D. Can create a broadcast storm
27. Which is NOT a standard type of DSL? ?
- A. ADSL
 - B. FDSL
 - C. VDSL
 - D. HDSL
28. Which is a property of a circuit-switched ?

network, as opposed to a packet-switched network?

- A. Physical, permanent connections exist from one point to another in a circuit-switched network.
- B. The data is broken up into packets.
- C. The data is sent to the next destination, which is based on the router's understanding of the best available route.
- D. Packets are reassembled according to their originally assigned sequence numbers

29. Which is NOT a packet-switched technology?

?

- A. SMDS
- B. T1
- C. Frame Relay
- D. X.25

30. Which is NOT a remote security method?

?

- A. VoIP
- B. Callback
- C. Caller ID
- D. Restricted Address

31. What does covert channel eavesdropping refer to?

?

- A. Using a hidden, unauthorized network connection to communicate unauthorized information
- B. Nonbusiness or personal use of the Internet
- C. Socially engineering passwords from an ISP
- D. The use of two-factor passwords

32. What does logon abuse refer to?

?

- A. Breaking into a network primarily from an external source
- B. Legitimate users accessing networked services that would normally be restricted to them
- C. Nonbusiness or personal use of the Internet

- D. Intrusions via dial-up or asynchronous external network connections
33. What is probing used for? ?
- A. To induce a user into taking an incorrect action
 - B. To give an attacker a road map of the network
 - C. To use up all of a target's resources
 - D. To covertly listen to transmissions
34. Which is NOT a property of or issue with tape backup? ?
- A. Slow data transfer during backups and restores
 - B. Server disk space utilization expands
 - C. Possible that some data re-entry may need to be performed after a crash
 - D. One large disk created by using several disks
35. What is a Server Cluster? ?
- A. A primary server that mirrors its data to a secondary server
 - B. A group of independent servers that are managed as a single system
 - C. A tape array backup implementation
 - D. A group of WORM optical jukeboxes
36. In which OSI layer does the MIDI digital music protocol standard reside? ?
- A. Application Layer
 - B. Presentation Layer
 - C. Session Layer
 - D. Transport Layer

Answers

1. *Answer:* d) GAN does not exist. LAN stands for Local Area Network, WAN stands for Wide Area Network, and MAN stands for Metropolitan Network.
2. *Answer:* b) Token Ring. Token Ring is a LAN media access method, not a cabling type.

3. *Answer:* c). A packet filtering firewall can operate at the Network or Transport Layers.
4. *Answer:* a). PGP stands for Pretty Good Privacy, an e-mail encryption technology.
5. *Answer:* c). A stateful inspection firewall is considered a third generation firewall.
6. *Answer:* a). Redundant Arrays of Intelligent Disks. The other acronyms do not exist.
7. *Answer:* c). Private addresses are not easily routable, thereby the reason for using NAT.
8. *Answer:* b).
9. *Answer:* b). The other acronyms do not exist.
10. *Answer:* c). Packet-switched networks are considered connection-less networks, circuit-switched networks are considered connection-oriented.
11. *Answer:* b). The Internet Layer is a TCP/IP architecture model layer.
12. *Answer:* d). The Session Layer is a OSI model layer.
13. *Answer:* c) Reactive is not a backup method.
14. *Answer:* c) The other acronyms do not exist.
15. *Answer:* b) Data Encapsulation attaches information from one layer to the packet as it travels from an adjoining layer. a) The OSI layered architecture model creates seven layers. c) the TCP/IP protocol UDP provides “best effort” packet delivery, and d) a token-passing transmission scheme creates a deterministic network because it’s possible to compute the maximum predictable delay.
16. *Answer:* b). TACACS+ has nothing to do with frame relay networks.
17. *Answer:* a) Cabling termination errors are an inherent issue with bus topology networks.
18. *Answer:* b). FDDI is a RING topology, like Token Ring.
19. *Answer:* c). Address Resolution Protocol starts with an IP address, then queries the network to find the MAC, or hardware address of the workstation it belongs to. ICMP does b), RARP does a), and FTP does d).
20. *Answer:* a). The reverse of ARP. The Reverse Address Resolution Protocol knows a MAC (Media Access Control) address and asks the RARP server to match it with an IP address.
21. *Answer:* b). Simple Mail Transport Protocol, queues and transfers email. SNMP stands for Simple Network Management Protocol. ICMP stands for Internet Control Message Protocol. RARP stands for Reverse Address Resolution Protocol
22. *Answer:* d). UTP stands for unshielded twisted pair wiring.
23. *Answer:* c). The Polling transmission type uses primary and secondary hosts, and the secondary must wait for permission from the primary before transmitting.
24. *Answer:* c). Ethernet networks were originally designed to work with more sporadic traffic than token ring networks.

25. *Answer:* c) Fiber Optic cable is much harder to tap than copper cable.
26. *Answer:* c). A bridge operates at Layer 2, and therefore does not use IP addressing to make routing decisions.
27. *Answer:* b). FDSL does not exist.
28. *Answer:* a) Permanent connections are a feature of circuit-switched networks.
29. *Answer:* b). A T1 line is a type of leased line, which uses a dedicated, point-to-point technology.
30. *Answer:* a) VoIP stands for Voice-Over-IP, a digital telephony technology.
31. *Answer:* a). A Covert Channel is a connection intentionally created to transmit unauthorized information from inside a trusted network to a partner at an outside, untrusted node. c) is called Masquerading.
32. *Answer:* b). Logon abuse entails an otherwise proper user attempting to access areas of the network that are deemed off-limits. a) is called network intrusion and d) is called a back-door attack.
33. *Answer:* b) Probing is a procedure where the intruder runs programs that scan the network to create a network map for later intrusion. a) is spoofing, c) is the objective of a denial of service attack, and d) is passive eavesdropping.
34. *Answer:* d). RAID level 0, striping is the process of creating a large disk out of several smaller disks.
35. *Answer:* b). A server cluster is a group of servers that appear to be a single server to the user. a) refers to Redundant Servers.
36. *Answer:* b). MIDI is a Presentation layer protocol.

Chapter 4: Cryptography

Overview

The information system professional should have a fundamental comprehension of the following areas in cryptography:

- Definitions
- History
- Cryptology Fundamentals
- Symmetric Key Cryptosystem Fundamentals
- Asymmetric Key Cryptosystem Fundamentals
- Key Distribution and Management Issues
- Public Key Infrastructure Definitions and Concepts

This chapter will address each of these areas to the level required of a practicing information system security professional.

Introduction

The purpose of cryptography is to protect transmitted information from being read and understood by anyone except the intended recipient. In the ideal sense, unauthorized individuals can never read an enciphered message. In practice, reading an enciphered communication can be a function of time — the effort and corresponding time, which is required for an unauthorized individual to decipher an encrypted message may be so large that it can be impractical. By the time the message is decrypted, the information within the message may be of minimal value.

Definitions

Block Cipher. Obtained by segregating plaintext into blocks of n characters or bits and applying the identical encryption algorithm and key, K , to each block. For example, if a plaintext message, M , is divided into blocks M_1, M_2, \dots, M_p , then

$$E(M, K) = E(M_1, K) E(M_2, K) \dots E(M_p, K)$$

where the blocks on the right-hand side of the equation are concatenated to form the ciphertext.

Cipher. A cryptographic transformation that operates on characters or bits.

Ciphertext or Cryptogram. An unintelligible message.

Clustering. A situation in which a plaintext message generates identical ciphertext messages using the same transformation algorithm, but with different cryptovariabes or keys.

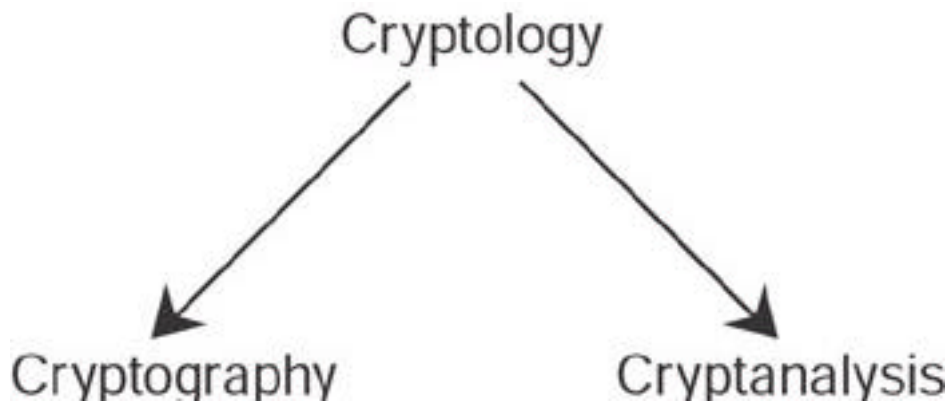
Codes. A cryptographic transformation that operates at the level of words or phrases.

Cryptanalysis. The act of obtaining the plaintext or key from the ciphertext that is used to obtain valuable information to pass on altered or fake messages in order to deceive the original intended recipient; breaking the ciphertext.

Cryptographic Algorithm. A step-by-step procedure used to encipher plaintext and decipher ciphertext.

Cryptography. The art and science of hiding the meaning of a communication from unintended recipients. The word cryptography comes from the Greek, *kryptos* (hidden) and *graphein* (to write).

Cryptology. Encompasses cryptography and cryptanalysis.



Cryptosystem. A set of transformations from a message space to a ciphertext space
For example, if

M = Plaintext, C = Ciphertext, E = the encryption transformation, and D = the decryption transformation,

$$E(M) = C$$

$$D[E(M)] = M$$

To specifically show the dependence of the encipherment and decipherment transformation on the cryptovvariable or key, K ,

$$E(M, K) = C$$

$$D(C, K) = D[E(M, K), K] = M$$

Decipher. To undo the encipherment process and make the message readable.

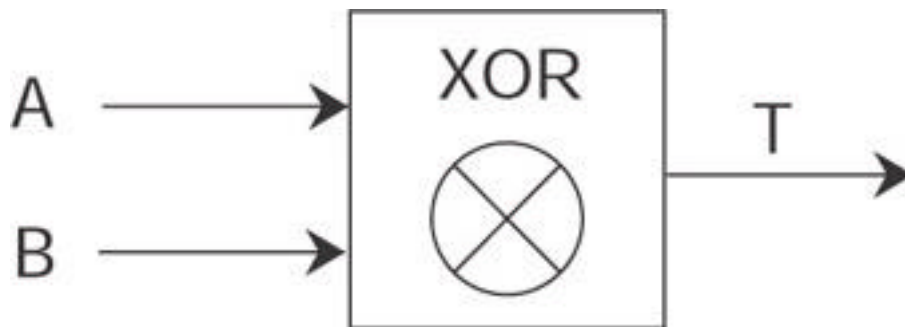
Encipher. To make the message unintelligible to all but the intended recipients.

End-to-End Encryption. Encrypted information that is sent from the point of origin to the final destination. In symmetric key encryption, this requires the sender and receiver to have the identical key for the session.

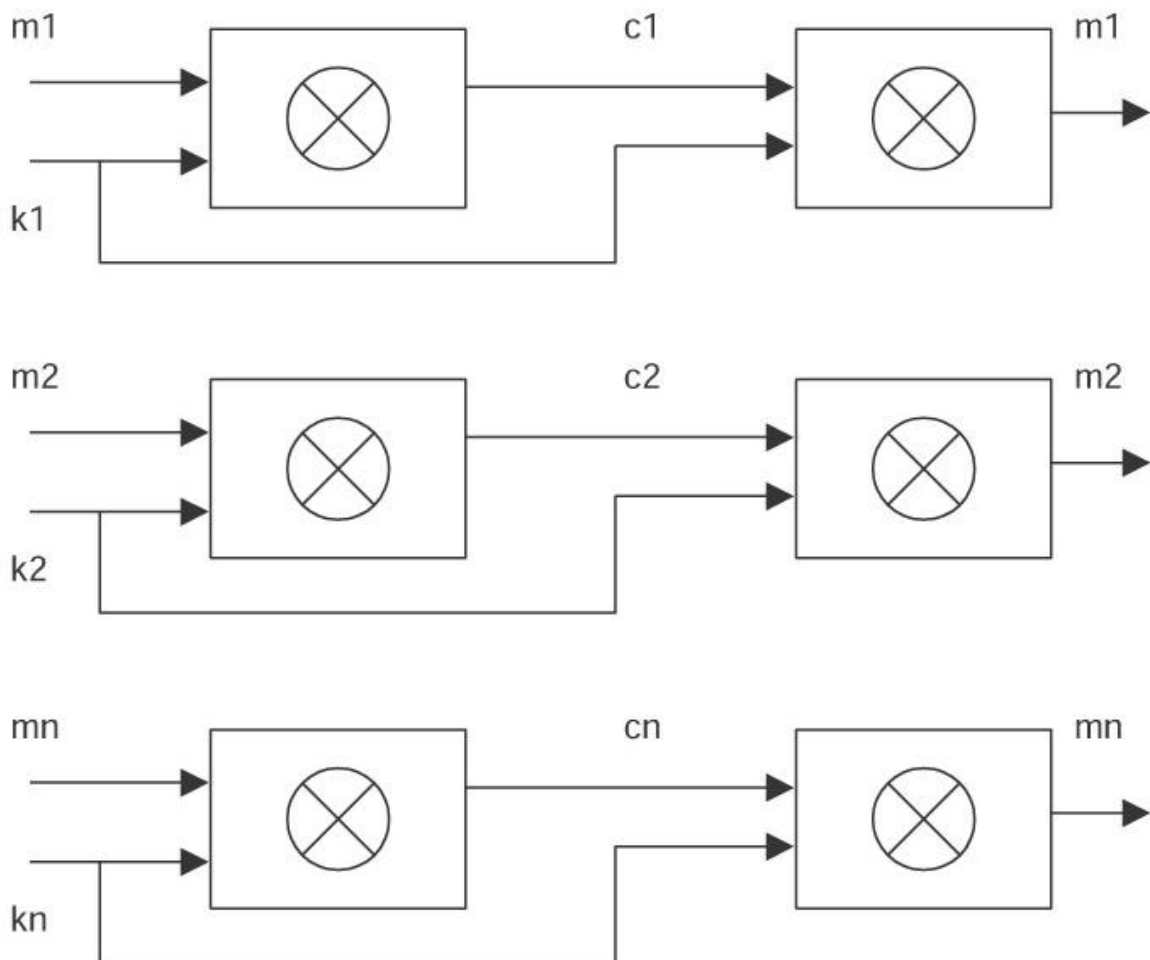
Exclusive Or. Boolean operation that essentially performs binary addition without carry on the input bits as shown in Table 4.1. For two binary input variables, A and B , the Exclusive Or function produces a binary 1 output when A and B are not equal and a binary 0 when A and B are equal. The symbol \wedge or the acronym XOR indicates the Exclusive Or operation.

Table 4.1: Exclusive OR (XOR)

	INPUTS	OUTPUT
A	B	T
0	0	0
0	1	1
1	0	1
1	1	0



The Exclusive Or function is easily implemented in hardware and, therefore, can be executed at hardware speeds. A valuable property of the Exclusive Or function is that the inverse of the function can be obtained by performing another Exclusive Or on the output. For example, assume a transformation is performed on a stream cipher by applying the Exclusive Or operation, bit by bit, on the plaintext bits with the bits of a keystream. Then, the decipherment of the enciphered stream is accomplished by applying the Exclusive Or of the keystream, bit by bit, to the enciphered stream. This property is illustrated in Figure 4.1 .



$$E(M,K) = M \text{ XOR } K = C,$$

$$D(C) = C \text{ XOR } K = (M \text{ XOR } K) \text{ XOR } K = M$$

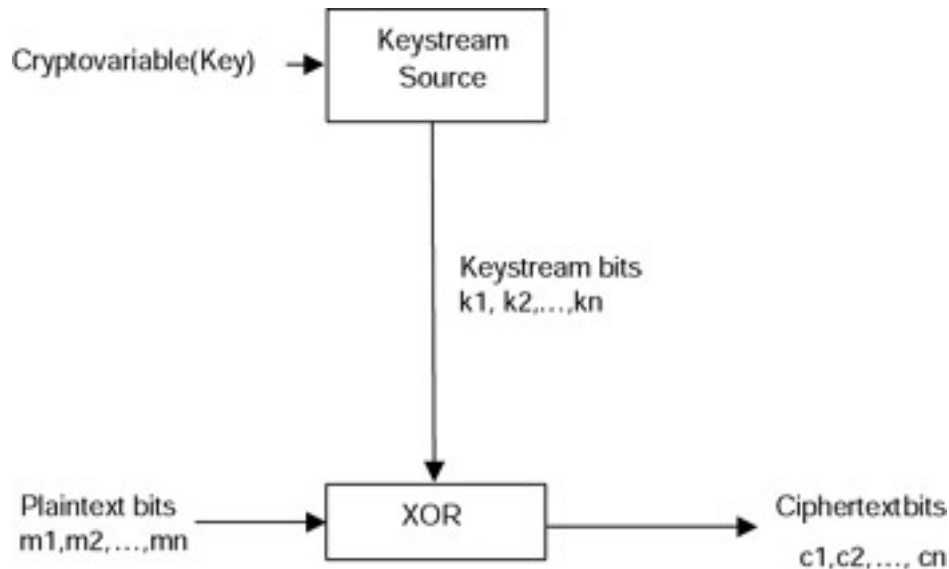
Figure 4.1: Exclusive Or encipherment and decipherment.

If the bits of the message stream M are m_1, m_2, \dots, m_n , the bits of the keystream K are k_1, k_2, \dots, k_n , and the bits of the ciphertext stream C are c_1, c_2, \dots, c_n , then

$$E(M,K) = M \text{ XOR } K = C, \text{ and}$$

$$D(C) = D[M \text{ XOR } K] = [M \text{ XOR } K] \text{ XOR } K$$

Schematically, the process is illustrated in Figure 4.2.



Keystream bits	1 0 1 1 0 1 1 0
Plaintext bits	1 1 0 0 0 0 1 1
Ciphertext bits	0 1 1 1 0 1 0 1

Figure 4.2: Encipherment process using Keystream with an XOR operation.

Key or Cryptovvariable. Information or a sequence that controls the enciphering and deciphering of messages

Link Encryption. Each entity has keys in common with its two neighboring nodes in the transmission chain. Thus, a node receives the encrypted message from its predecessor (the neighboring node), decrypts it, and then re-encrypts it with another key that is common to the successor node. Then, the encrypted message is sent on to the successor node where the process is repeated until the final destination is reached. Obviously, this mode does not provide protection if the nodes along the transmission path can be compromised. A general representation of link encryption is shown in Figure 4.3.

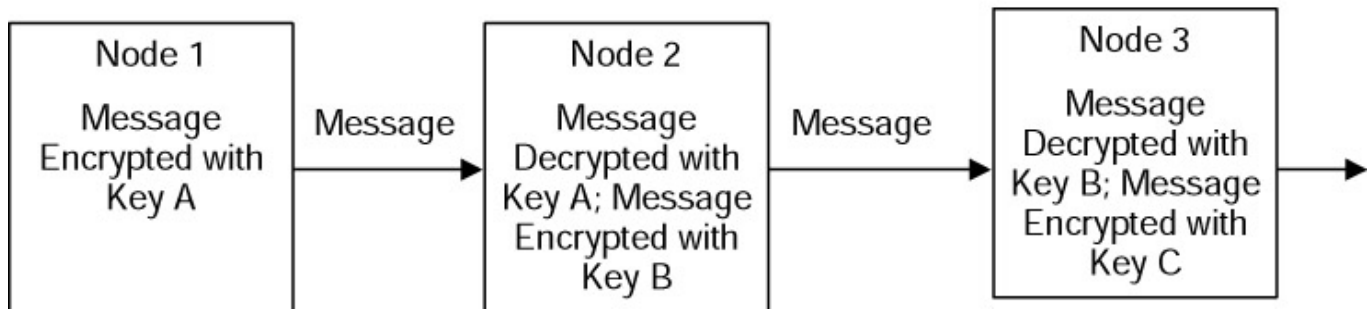


Figure 4.3: Link Encryption.

One Time Pad. Assuming an encryption key, K , with components k_1, k_2, \dots, k_n , the encipherment operation performed using each component k_i of the key, K , to encipher exactly one character of the plaintext. Therefore, the key has the same length as the message. Also, the key is used only once and is never used again. Ideally, the key's components are truly random and have no periodicity or predictability, thus making the ciphertext unbreakable. The one time pad is usually implemented as a stream cipher using the XOR function. The elements, k_1, k_2, \dots, k_n , of the key stream are independent and are uniformly distributed random variables. This requirement of a single, independently chosen value of k_i to encipher each plaintext character is stringent and may not be practical for most commercial Information Technology (IT) applications. The one-time pad was invented in 1917 by Major Joseph Mauborgne of the United States Army Signal Corps and Gilbert Vernam of AT&T.

Plaintext. A message in cleartext readable form.

Steganography. Secret communications where the existence of the message is hidden. For example, in a digital image, the least significant bit of each word can be used to comprise a message without causing any significant change in the image.

Work Function (Factor). The difficulty in recovering the plaintext from the ciphertext as measured by cost and/or time. A system's security is directly proportional to the value of the work function. The work function only needs to be large enough to suffice for the intended application. If the message to be protected loses its value after a short time period, the work function only needs to be large enough to ensure that the decryption would be highly infeasible in that period of time.

History

Secret writing can be traced back to 3000 B.C. when it was used by the Egyptians. They employed hieroglyphics to conceal writings from unintended recipients. *Hieroglyphics* is derived from the Greek word *hieroglyphica* that means sacred carvings. Hieroglyphics evolved into *hieratic*, which was a stylized script that was easier to use. Around 400 B.C., military cryptography was employed by the Spartans in the form of a strip of papyrus or parchment wrapped around a wooden rod. This system is called a Scytale and is shown in Figure 4.4.

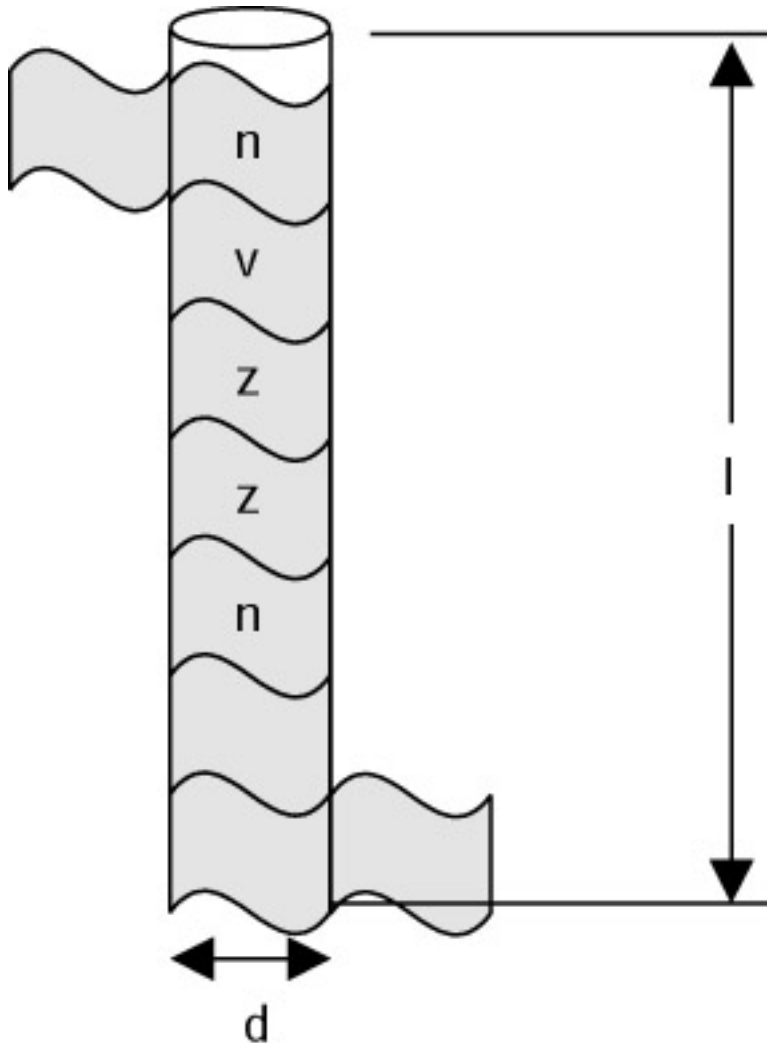


Figure 4.4: A Spartan Scytale.

The message to be encoded was written lengthwise down (or up) the rod on the wrapped material. Then, the material was unwrapped and carried to the recipient. In its unwrapped form, the writing appeared to be random characters. When the material was rewound on a rod of the same diameter, d , and minimum length, l , the message could be read. Thus, as shown in Figure 4.4, the keys to deciphering the message are d and l .

Around 50 B.C., Julius Caesar, the Emperor of Rome, used a *substitution* cipher to transmit messages to Marcus Tullius Cicero. In this cipher, letters of the alphabet are substituted for other letters of the same alphabet. Because only one alphabet was used, this cipher was a *monoalphabetic substitution*. This particular cipher involved shifting the alphabet three letters and substituting those letters. This substitution, sometimes known as C3 (for Caesar shifting three places) is shown in Figure 4.5.



Figure 4.5: Caesar C3 substitution cipher.

In general, the Caesar system of ciphers can be written as

$$Z_i = C_n(P_i),$$

where the Z_i are ciphertext characters, C_n is a monoalphabetic substitution transformation, n is the number of letters shifted, and the P_i are plaintext characters.

Thus, the message, ATTACK AT DAWN, would be enciphered using C3 as follows:

ATTACK AT DAWN
↓
DWWDFN DW GDZQ

Disks have played an important part in cryptography for the last 500 years. In Italy, around 1460, Leon Battista Alberti developed cipher disks for encryption (Figure 4.6). His system consisted of two concentric disks. Each disk had an alphabet around its periphery and by rotating one disk with respect to the other, a letter in one alphabet could be transformed to a letter in another alphabet.

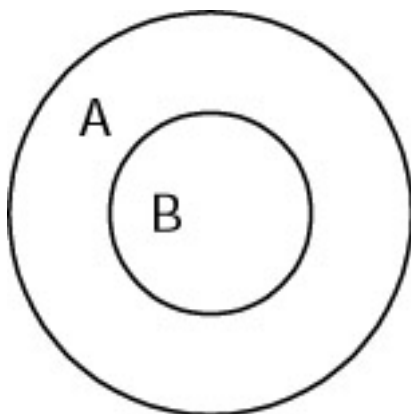


Figure 4.6: Cipher disks.

The Arabs invented cryptanalysis because of their expertise in mathematics, statistics and linguistics. Because every Muslim is required to seek knowledge, they studied earlier civilizations and translated their writings into Arabic. In 815, the Caliph al-Mámun established the House of Wisdom in Baghdad that was the focal point of translation efforts. In the ninth century, the Arab philosopher, al-Kindi, wrote a treatise, which was rediscovered in 1987, entitled *A Manuscript on Deciphering Cryptographic Messages*. In 1790, Thomas Jefferson developed an encryption device using a stack of 26 disks that could be rotated individually. A message was assembled by rotating each disk to the proper letter under an alignment bar that ran the length of the disk stack. Then, the alignment bar was rotated through a specific angle, A , and the letters under the bar were the encrypted message. The recipient would align the enciphered characters under the alignment bar, rotate the bar back through the angle A and read the plaintext message. This Jeffersonian system is shown in Figure 4.7.

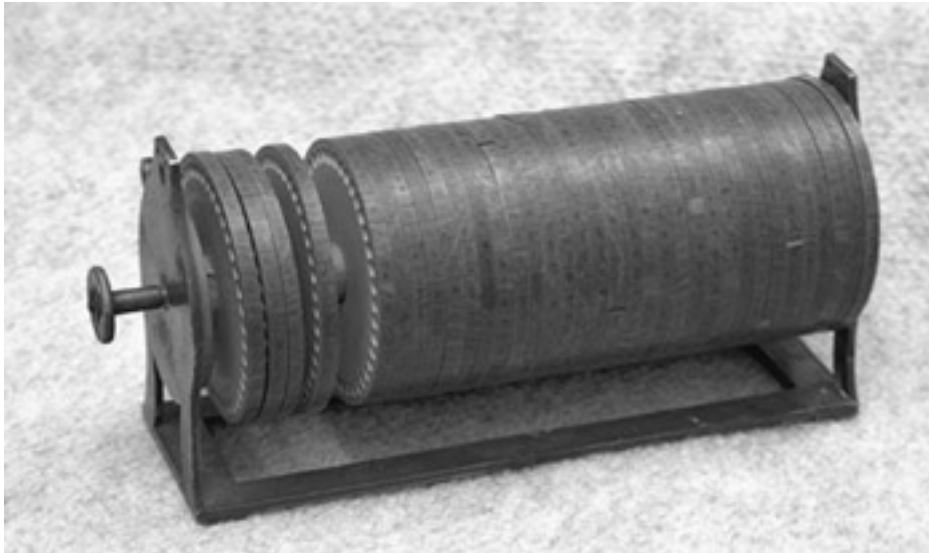


Figure 4.7: Jefferson disks. *(Courtesy of the National Cryptologic Museum)*

Disk systems were used extensively during the U.S. Civil War. A Federal Signal Officer obtained a patent on a disk system similar to the one invented by Leon Battista Alberti in Italy, and he used it to encode and decode flag signals among units.

Unix systems use a substitution cipher called ROT 13 that shifts the alphabet by 13 places. Another shift of 13 places brings the alphabet back to its original position, thus decoding the message.

A mechanical cryptographic machine called the Hagelin Machine, shown in Figure 4.8, was developed in 1920 by Boris Hagelin in Stockholm, Sweden. In the United States, the Hagelin Machine is known as the M-209.

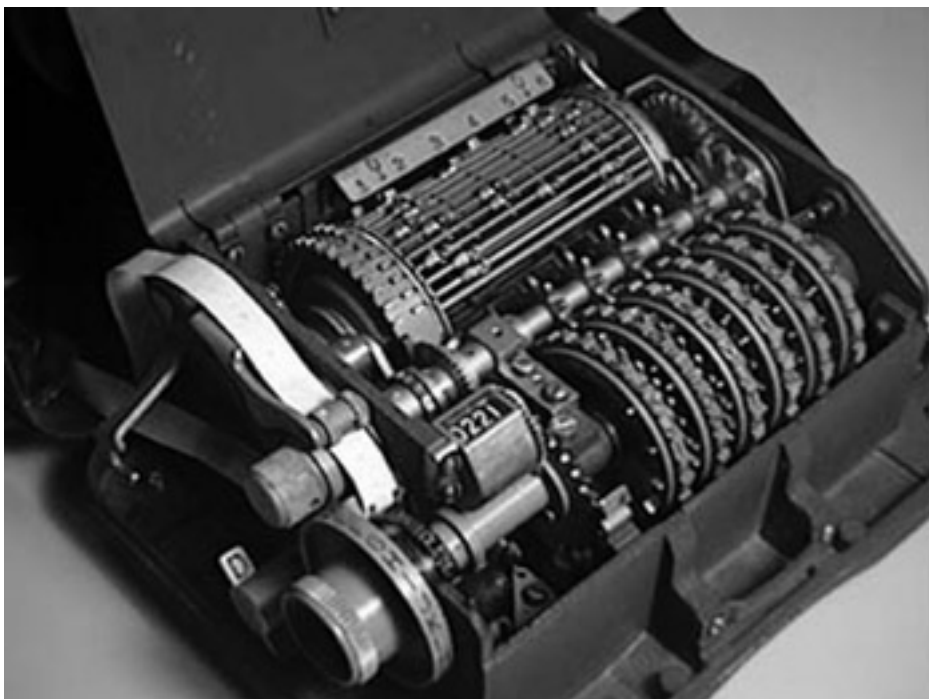


Figure 4.8: The Hagelin Machine.



Figure 4.9: Herbert Yardley’s Black Chamber.
 (Courtesy of the National Cryptologic Museum)

In the 1920s, Herbert O. Yardley was in charge of the secret U.S. MI-8 organization, also known as the “Black Chamber.” MI-8 cracked the codes of a number of nations. During the 1921—1922 Washington Naval Conference, the United States had an edge in the Japanese negotiations because MI-8 was supplying the U.S. Secretary of State with the intercepted Japanese negotiating plans. The U.S. State Department closed MI-8 in 1929, much to the chagrin of Yardley. In retaliation, Yardley published the book, *The American Black Chamber* (Yardley, Herbert O., *The American Black Chamber* (Laguna Hills, CA: Aegean Park Press, 1931)), which described to the world the secrets of MI-8. As a consequence, the Japanese installed new codes. Because of his pioneering contributions to the field, Yardley is known as the “Father of American Cryptology.” Figure 4.9 shows a display concerning Yardley in the U.S. National Cryptologic Museum at the National Security Agency (NSA) site near Baltimore, Maryland.

The Japanese Purple Machine

Following Yardley’s departure, William F. Friedman resumed cryptanalysis efforts for the U.S. Army. Friedman’s team broke the new Japanese diplomatic cipher.

Yardley’s counterpart in the U.S. Navy was Laurance Stafford. Stafford headed the team that broke the Japanese Purple Machine naval codes during World War II. A group of these code breakers worked in dark basement rooms at Naval District Headquarters in Pearl Harbor. Commander Joseph J. Rochefort led this group in the spring of 1942 when his cryptanalysts intercepted and deciphered a Japanese coded message. This message described a forthcoming major Japanese attack on a location known as AF. Rochefort believed that AF referred to the U.S.-held Midway Island. Midway was a key U.S. base that projected U.S. power into the mid-Pacific.

Rochefort could not convince his superiors that AF was Midway Island. As a ruse, Rochefort asked Midway personnel to transmit a message that Midway was having a water problem. The message was sent in the clear and in weak code that was sure to

be intercepted and broken by the Japanese. Later on May 22, Japanese Naval intelligence transmitted a message read by the United States that AF was having a water problem. As a result of this brilliant effort in code breaking, Admiral Chester W. Nimitz authorized the strategy for the U.S. fleet to surprise the Japanese fleet at Midway. This bold undertaking resulted in a resounding U.S. victory that was the turning point of the war in the Pacific.

The German Enigma Machine

The German military used a polyalphabetic substitution cipher machine called the Enigma as its principal encipherment system during World War II. The Enigma incorporated mechanical rotors for encipherment and decipherment. A Dutchman, Hugo Koch, developed the machine in 1919, and it was produced for the commercial market in 1923 by Arthur Scherbius. Scherbius obtained a U.S. patent on the Enigma machine for the Berlin firm of Chiffriermaschinen Aktiengesellschaft. Polish cryptanalyst Marian Rejewski, working with the French from 1928 to 1938 solved the wiring of the three-rotor system that was used by the Germans at the time and created a card file that could anticipate the 63 17,576 possible rotor positions. The Germans changed the indicator system and the number of rotors to six in 1938, thus tremendously increasing the difficulty of breaking the Enigma cipher. In their work in 1938, the Poles and French constructed a prototype machine called "The Bombe" for use in breaking the Enigma cipher. The name was derived from the ticking noises the machine made.

The work on breaking the Enigma cipher was then taken over by the British at Bletchley Park in England, and was led by many distinguished scientists, including Alan Turing. The Turing prototype Bombe appeared in 1940 and high speed Bombes were developed by the British and Americans in 1943.

The Enigma Machine as shown in Figure 4.10 consists of a plugboard, three rotors, and a reflecting rotor.



Figure 4.10: Enigma Machine. *(Courtesy of the National Cryptologic Museum)*

The three rotors' rotational positions changed with encipherments. A rotor is illustrated in Figure 4.11. It is constructed of an insulating material and has 26 electrical contacts that are evenly spaced around the circumference on both sides. A conductor through the disk connects a contact on one side of the disk to a noncorresponding contact on the other side of the disk, effecting a monoalphabetic substitution. This connection is illustrated in Figure 4.12.



Figure 4.11: An Enigma rotor.

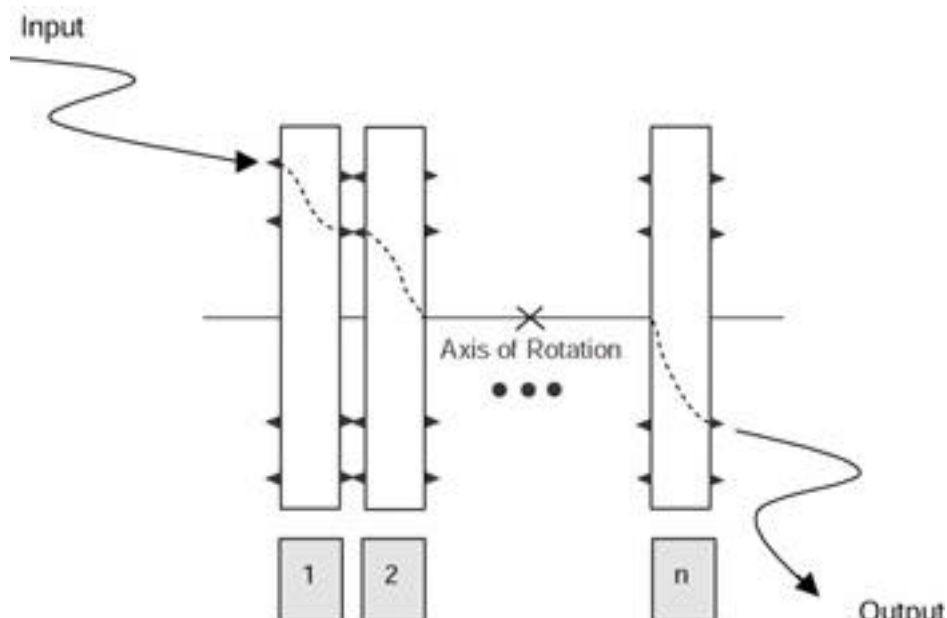


Figure 4.12: An illustration of Enigma rotor connections.

Turning the rotor places the results in another substitution. These substitutions come from rotor to rotor. The rotors are turned $360/26$ degrees for each increment.

Thus, current entering the input point on rotor 1 travels through the subsequent rotors and emerges at the output. This traverse implements a *monoalphabetic substitution*. To further complicate the decryption, the position of the rotor is changed after the encryption of each letter. Actually, when one rotor makes a complete revolution, it increments the next “higher position” rotor in much the same manner as counters increment on a gasoline pump. This rotation accomplishes a *polyalphabetic substitution* since the plaintext is being transformed into a different alphabet. The rotational displacements were implemented by gears in the World War II Enigma Machine. In practice, the rotors had an initial rotational displacement. These rotors were the primary key and the rotational displacement was the secondary key. An initial permutation was performed on the plaintext by means of the plugboard prior to its being passed through the three substitution rotors. Then, this result was further enciphered by the reflecting rotor, which has contacts only on one side. The path was then returned through the three rotors in this backward direction. The final resulting ciphertext was subjected to the inverse permutation of the initial plaintext permutation.

Rotor systems are also referred to as Hebern Machines. In addition to the German Enigma, the Japanese Red and Purple Machines and the American SIGABA (Big Machine) (Figure 4.13) were rotor machines. As far as it is known, SIGABA ciphers were never broken.



Figure 4.13: American SIGABA “Big Machine.” (Courtesy of National Cryptographic Museum)

Cryptographic Technologies

The two principal types of cryptographic technologies are symmetric key (secret key or private key) cryptography and asymmetric (public key) cryptography. In symmetric key cryptography, both the receiver and sender share a common secret key. In asymmetric key cryptography, the sender and receiver respectively share a public and private key. The public and private keys are related mathematically and, in an ideal case, have the characteristic where an individual, who has the public key, cannot derive the private key.

Because of the amount of computation involved in public key cryptography, private key cryptography is on the order of 1,000 times faster than public key cryptography.

Classical Ciphers

In this section, the basic encipherment operations are discussed in detail in order to provide a basis for understanding the evolution of encryption methods and the corresponding cyptanalysis efforts.

Substitution

The Caesar Cipher, as we discussed earlier in this chapter, is a simple substitution cipher, that involves shifting the alphabet three positions to the right. The Caesar Cipher is a subset of the Vigenère polyalphabetic cipher. In the Caesar cipher, the message's characters and repetitions of the key are added together, modulo 26. In modulo 26 addition, the letters A to Z of the alphabet are given a value of 0 to 25, respectively. Two parameters have to be specified for the key:

D, the number of repeating letters representing the key

K, the key

In the following example, $D = 3$ and $K = \text{BAD}$.

The message is: ATTACK AT DAWN

Assigning numerical values to the message yields

0 19 19 0 2 10 0 19 3 0 22 13
A T T A C K A T D A W N

The numerical values of K are

1 0 3
B A D

Now, the repetitive key of 103 is added to the letters of the message as follows:

1 0 3 1 0 3 1 0 3 1 0 3 Repeating Key
0 19 19 0 2 10 0 19 3 0 22 13 Message
1 19 22 1 2 13 1 19 6 1 22 15 Ciphertext Numerical Equivalents
B T W B C N B T G B W P Ciphertext

Converting the numbers back to their corresponding letters of the alphabet produces the ciphertext as shown.

For the special case of the Caesar Cipher, D is 1 and the Key is D (2).

Taking the same message as an example using the Caesar cipher yields:

2 2 2 2 2 2 2 2 2 2 2 Repeating Key
0 19 19 0 2 10 0 19 3 0 22 13 Message
2 21 21 2 4 12 2 21 5 2 24 15 Ciphertext Numerical Equivalents
C V V C E M C V F C Y P Ciphertext

Converting the numbers back to their corresponding letters of the alphabet produces the ciphertext, which is the letters of the original message text shifted three positions to the right.

If the sum of any of the additions yields a result greater than or equal to 26, the additions would be modulo 26, in which the final result is the remainder over 26. The following examples illustrate modulo 26 addition.

14 12 22 24
12 22 8 5
26 32 30 29 Apparent Sum
0 6 4 3 Result of modulo 26 addition

These ciphers can be described by the general equation,

$C = (M + b) \bmod N$ where

b is a fixed integer

N is the size of the alphabet

M is the Plaintext message in numerical form

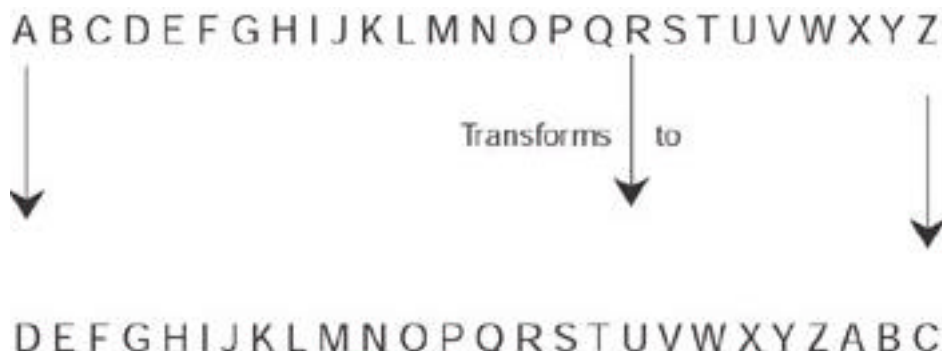
C is the Ciphertext in numerical form

This representation is a special case of an Affine Cryptosystem, which is described in the following equation:

$C = (aM + b) \bmod N$ where

a and b comprise the key

Recall that the following transformation is implemented by the Caesar Cipher:



This type of cipher can be attacked by using frequency analysis. In frequency analysis, the frequency characteristics shown in the use of the alphabet's letters in a particular language are used. This type of cryptanalysis is possible because the Caesar cipher is a monoalphabetic or simple substitution cipher where a character of ciphertext is substituted for each character of the plaintext.

A polyalphabetic cipher is accomplished through the use of multiple substitution ciphers. For example, using the alphabet shown in Figure 4.14, a Caesar cipher with D 5 3, and the Key 5 BAD (103), the plaintext EGGA is enciphered into YGZR. Blaise de Vigenère, a French diplomat born in 1523, consolidated the cryptographic works of Alberti, Trithemius, and Porta to develop the very strong polyalphabetic cipher at that time. Vigenère's cipher used 26 alphabets. An example of a polyalphabetical substitution using four alphabets is shown in Figure 4.14.

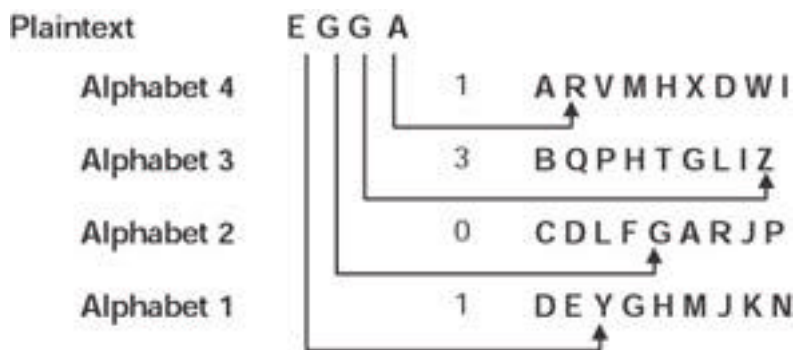


Figure 4.14: Polyalphabetic Substitution.

Because multiple alphabets are used, this approach counters frequency analysis. It can, however, be attacked by discovery of the periods — when the substitution repeats.

Transposition (Permutation)

Another type of cipher is the transposition cipher. In this cipher, the letters of the plaintext are permuted.

For example, the letters of the plaintext A T T A C K A T D A W N could be permuted to D C K A A W N A T A T T.

A columnar transposition cipher is one where the plaintext is written horizontally across the paper and is read vertically as shown in Figure 4.15.

NOWISTHE
 TIMEFORA
 LLGOODME
 NTOCOMET
 OTHEAIDO
 FTHEIRPA
 RTY

Figure 4.15: A columnar transposition cipher.

Reading the ciphertext vertically yields: NTLNOFROILTTTTWMGOHHY . . .

The transposition cipher can be attacked through frequency analysis, but it hides the statistical properties of letter pairs and triples such as IS and TOO.

Vernam Cipher (One-Time Pad)

The one-time pad or Vernam cipher is implemented through a key that consists of a random set of non-repeating characters. Each key letter is added modulo 26 to a letter of the plaintext. In the one-time pad, each key letter is used one time for only one message and is never used again. The length of the key character stream is equal to the length of the message. For megabyte and gigabyte messages, this one-time pad is not practical, but it is approximated by shorter random sets of characters with very long periods.

An example of a one-time pad encryption is

Plaintext	HOWAREYOU	7	14	22	0	17	4	24	14	20
One-time pad key	XRAQZTBCN	23	17	0	16	25	19	1	2	13
Apparent sum		30	31	22	16	42	23	25	16	33
Sum Mod 26		4	5	22	16	16	23	25	16	7
Ciphertext		E	F	W	Q	Q	X	Z	Q	H

The Vernam machine (shown in Figure 4.16) was developed at AT&T and the original system performed an XOR of the message bits in a Baudot code with the key bits.

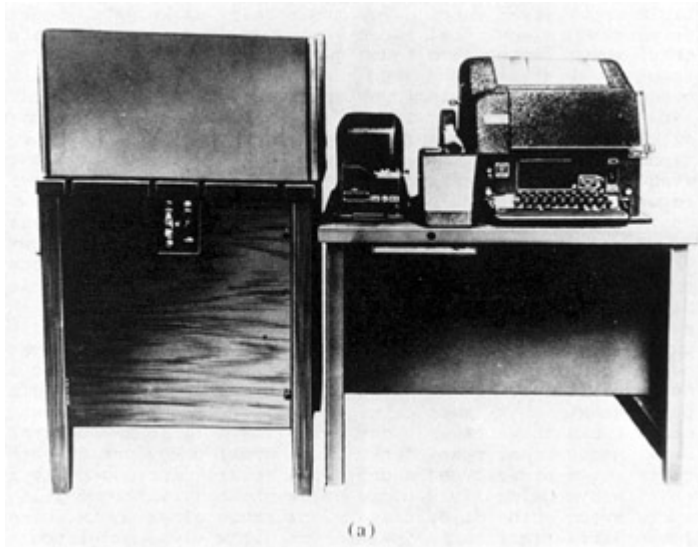


Figure 4.16: A Vernam machine.

Book or Running Key Cipher

This cipher uses text from a source, say a book, to encrypt the plaintext. The key, known to the sender and the intended receiver, may be the page and line number of text in the book. This text is matched, character for character, with the plaintext and modulo 26 addition is performed to effect the encryption.

The Running Key Cipher eliminates periodicity, but it is attacked by exploiting the redundancy in the key.

Codes

Codes deal with words and phrases and relate these words as phrases to corresponding groups of numbers or letters. For example, the numbers 526 may mean "Attack at Dawn."

Steganography

Steganography is the art of hiding the existence of a message. The word Steganography comes from the greek words *steganos*, meaning "covered," and *graphein*, which means "to write." An example is the microdot, which compresses a message into the size of a period or dot. Steganography can be used to make a digital "watermark" to detect illegal copying of digital images.

Secret Key Cryptography (Symmetric Key)

Secret key cryptography is the type of encryption that is familiar to most people. In this type of cryptography, the sender and receiver both know a secret key. The sender encrypts the plaintext message with the secret key, and the receiver decrypts the message with the same secret key. Obviously, the challenge is to make the secret key available to both the sender and receiver without compromising it. For increased security, the secret key should be changed at frequent intervals. Ideally, a particular secret key should only be used once.

Figure 4.17 illustrates a secret (symmetric) key cryptographic system.

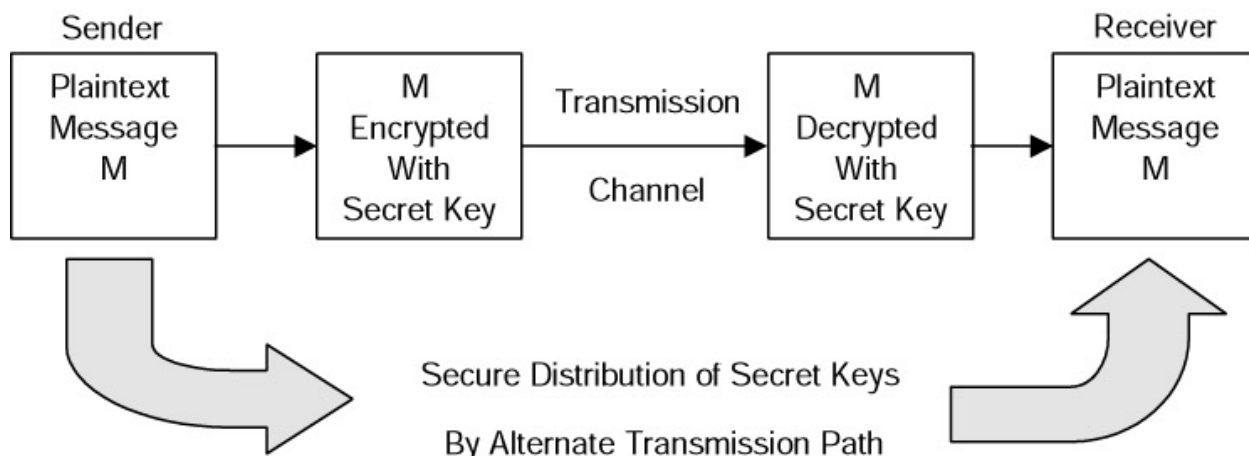


Figure 4.17: A symmetric (secret) key cryptographic system.

A secret key cryptographic system is comprised of information that is public and private. The public information usually consists of the following:

- The algorithm for enciphering the plaintext copy of the enciphered message
- Possibly, a copy of plaintext and an associated ciphertext
- Possibly, an encipherment of the plaintext that was chosen by an unintended receiver

Private information is

- The key or cryptovvariable
- One particular cryptographic transformation out of many possible transformations

An important property of any secret key cryptographic system is that the same key can encipher and decipher the message. If large key sizes (. 128 bits) are used, secret key systems are very difficult to break. These systems are also relatively fast and are used to encrypt large volumes of data. There are many symmetric key algorithms available because of this feature. One problem with using a symmetric key system is that, because the sender and receiver must share the same secret key, the sender requires a different key for each intended receiver. One commonly used approach is to use public key cryptography to transmit a symmetric session key that can be used for a session between the sender and receiver. Time stamps can be associated with this session key so that it is valid only for a specified period of time. Time stamping is a counter to *replay*, wherein a session key is somehow intercepted and used at a later time. Symmetric key systems, however, do not provide mechanisms for authentication and non-repudiation. The best known symmetric key system is probably the Data Encryption Standard (DES). DES evolved from the IBM Lucifer cryptographic system in the early 1970s for commercial use.

Data Encryption Standard (DES)

DES is a symmetric key cryptosystem that was devised in 1972 as a derivation of the Lucifer algorithm developed by Horst Feistel at IBM. He obtained a patent on the technique (H. Feistel, "Block Cipher Cryptographic System," U.S. Patent #3,798,539, 19 March, 1974.) DES is used for commercial and non-classified purposes. DES describes the Data Encryption Algorithm (DEA) and is the name of the Federal Information Processing Standard (FIPS) 46-1 that was adopted in 1977 [*Data Encryption Standard*, FIPS PUB 46-1 (Washington, D.C.: National Bureau of Standards, Jan 15, 1977.)] DEA is also defined as the ANSI Standard X3.92 [ANSI X3.92 American National Standard for Data Encryption Algorithm, (DEA)," American National Standards Institute, 1981.] The National Institute of Standards and Technology (NIST) recertified DES in 1993.

DES will not be recertified again. It will, however, be replaced by the Advanced Encryption Standard (AES).

DEA uses a 64-bit block size and uses a 56-bit key. It begins with a 64-bit key and strips off eight parity bits. DEA is a 16-round cryptosystem and was originally designed for implementation in hardware. With a 56-bit key, one would have to try 256 or 70 quadrillion possible keys in a brute force attack. Even though this number is huge, large numbers of computers cooperating over the Internet could try all possible key combinations. Due to this vulnerability, the U.S. government has not used DES since November 1998. Triple DES—three encryptions using the DEA — has replaced DES and will be used until the AES is adopted.

As previously stated, DES uses 16 rounds of transposition and substitution. It implements the techniques that were suggested by Claude Shannon, the father of Information Theory. Shannon proposed two techniques, confusion and diffusion, for improving the encryption of plaintext. Confusion conceals the statistical connection between ciphertext and plaintext. It is accomplished in DES through a substitution by means of non-linear substitution S-boxes. An S-box is non-linear because it generates a 4-bit output string from a 6-bit input string.

The purpose of diffusion is to spread the influence of a plaintext character over many ciphertext characters. Diffusion can be implemented by means of a *Product Cipher*. In a Product Cipher, a cryptosystem (E1) is applied to a message (M) to yield ciphertext (C1). Then, another cryptosystem (E2) is applied to ciphertext (C1) to yield ciphertext C2. Symbolically, this product is generated by: $E1(M) = C1$; $E2(C1) = C2$. DES implements this product 16 times. Diffusion is performed in DES by permutations in P-Boxes.

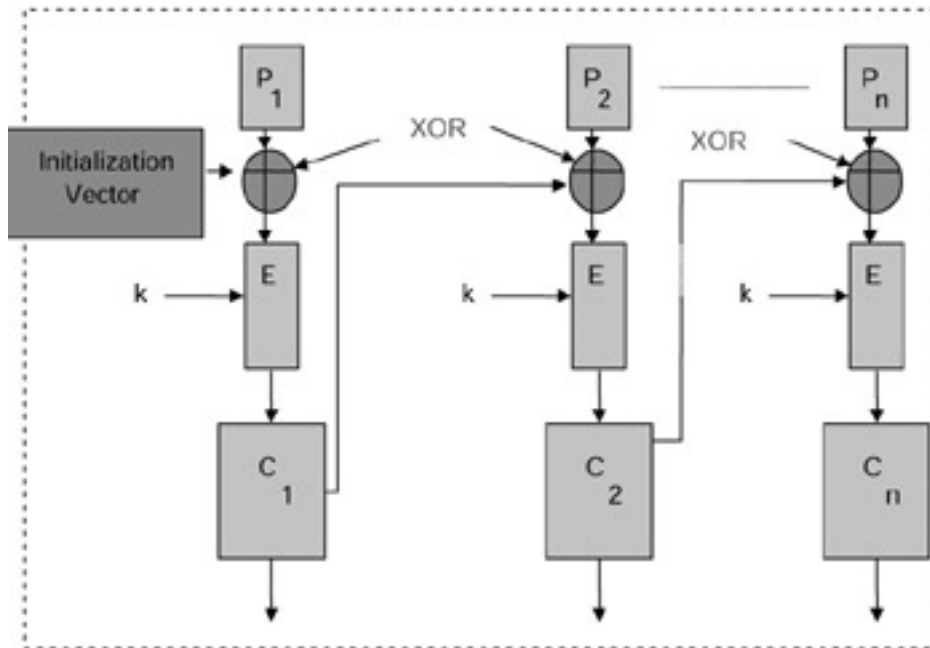
DES operates in four modes:

1. Cipher Block Chaining (CBC)
2. Electronic Code Book (ECB)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)

Cipher Block Chaining

Cipher Block Chaining (CBC) operates with plaintext blocks of 64 bits. A randomly generated 64-bit initialization vector is XORed with the first block of plaintext used to disguise the first part of the message that may be predictable (such as Dear Sir). The result is encrypted using the DES key. The first ciphertext will then XOR with the next 64-bit plaintext block. This encryption continues until the plaintext is exhausted. Note that in this mode, errors propagate.

A schematic diagram of Cipher Block Chaining is shown in Figure 4.18.



k=key

Figure 4.18: Cipher block chaining.

Electronic Code Book (ECB)

Electronic Code Book (ECB) is the “native” mode of DES and is a block cipher. ECB is best suited for use with small amounts of data. It is usually applied to encrypt initialization vectors or encrypting keys. ECB is applied to 64-bit blocks of plaintext, and it produces corresponding 64-bit blocks of ciphertext. ECB operates by dividing the 64-bit input vector into two 32-bit blocks called a Right Block and a Left Block. The bits are then recopied to produce two 48-bit blocks. Then, each of these 48-bit blocks is XORed with a 48-bit encryption key. The nomenclature “code book” is derived from the notion of a code book in manual encryption wherein there exist pairs of plaintext and the corresponding code. For example, the word “RETREAT” in the code book may have the corresponding code 5374.

Cipher Feedback Mode (CFB)

The Cipher Feedback Mode (CFB) of DES is a stream cipher where the ciphertext is used as feedback into the key generation source to develop the next key stream. The ciphertext generated by performing an XOR of the plaintext with the key stream has the same number of bits as the plaintext. In this mode, errors will propagate. A diagram of the CFB is shown in Figure 4.19.

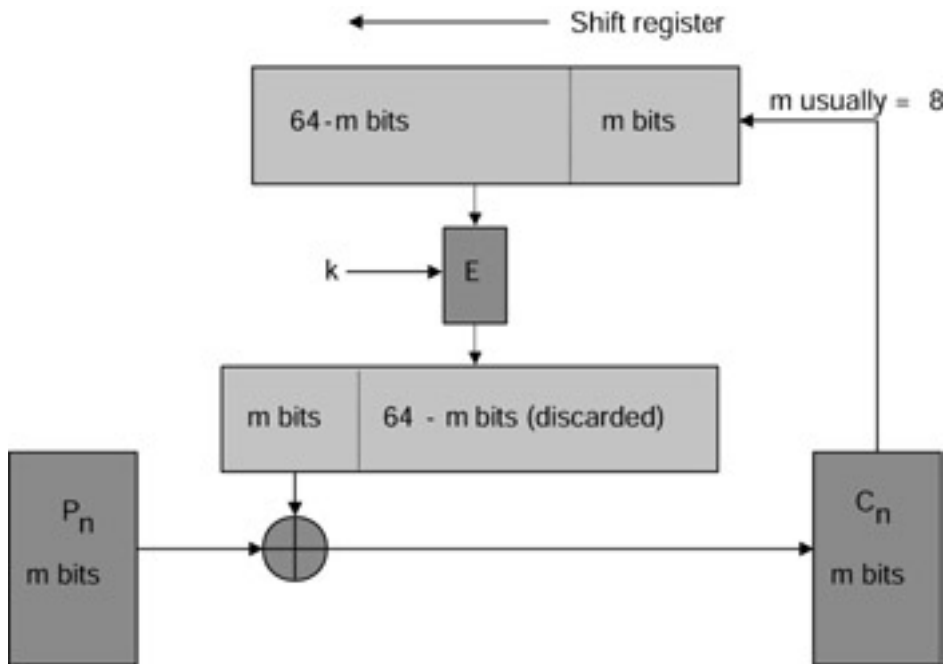


Figure 4.19: DES Cipher Feedback operation.

Output Feedback

The DES Output Feedback Mode (OFB) is also a stream cipher that generates the ciphertext key by XORing the plaintext with a key stream. In this mode, errors will not propagate. Feedback is used to generate the key stream, therefore the key stream varies. An initialization vector is required in OFB. OFB is depicted in Figure 4.20.

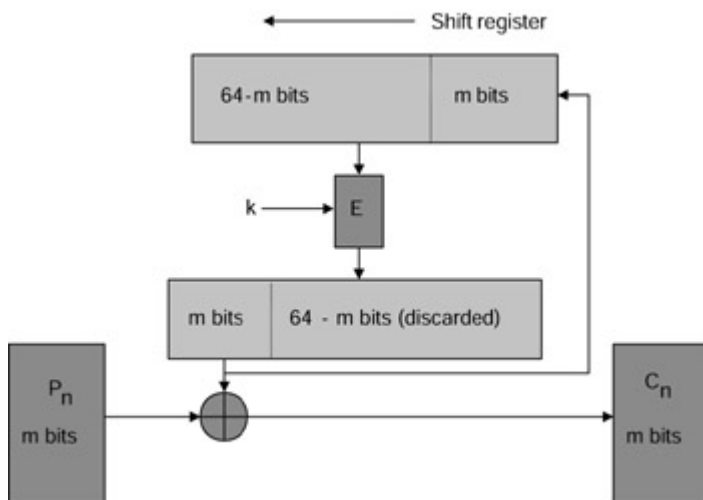


Figure 4.20: DES Output Feedback operations.

DES Security

Due to the increase in computing power that is capable of being integrated onto (Very Large Scale Integration (VLSI) chips and the corresponding decrease in cost, DES has been broken. Through the use of the Internet, a worldwide network of PCs was used to crack DES.

The consensus of the information security community is that DES is vulnerable to attack by an exhaustive research for the 56-bit key. Therefore, DES is being replaced by Triple DES, and then by the Advanced Encryption Standard (AES).

Triple DES

It has been shown that encrypting plaintext with one DES key and then encrypting it with a second DES key is no more secure than using a single DES key. It would seem, at first glance, that if both keys have n bits, a brute force attack of trying all possible keys will require trying $2^n \cdot 2^n$ or 2^{2n} different combinations. However, Merkle and Hellman showed that a known plaintext, *Meet-in-the-Middle* attack could break the double encryption in 2^{n+1} attempts. This type of attack is effected by encrypting from one end, decrypting from the other, and comparing the results in the middle. Therefore, Triple DES is used to obtain stronger encryption.

Triple DES encrypts a message three times. This encryption can be accomplished in several ways. For example, the message can be encrypted with Key 1, decrypted with Key 2 (essentially another encryption) and encrypted again with Key 1:

$[E\{D[E(M, K1)], K2\}, K1]$

A Triple DES encryption in this manner is denoted as DES — EDE2. If these encryptions are performed using the two keys, it is referred to as DES — EE2

$[E\{E[E(M, K1)], K2\}, K1]$

Similarly,

$E\{E[E(M, K1)], K2\}, K3]$

describes a triple encryption DES — EE3 with three different keys. This encryption is the most secure form of Triple DES.

The Advanced Encryption Standard (AES)

AES is a block cipher that will replace DES, but it is anticipated that Triple DES will remain an approved algorithm for U.S. Government use. Triple DES and DES are specified in FIPS 46-3. The AES initiative was announced in January 1997 by the National Institute of Standards and Technology (NIST) and candidate encryption algorithm submissions were solicited. On August 29, 1998, a group of fifteen AES candidates were announced by NIST. In 1999, NIST announced five finalist candidates. These candidates were MARS, RC6, Rijndael, Serpent, and Twofish. NIST closed Round 2 of public analyses of these algorithms on May 15, 2000.

On October 2, 2000, NIST announced the selection of the Rijndael Block Cipher, developed by the Belgian cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen, as the proposed AES algorithm. As such, it will be the new Federal Information Processing Standard (FIPS) Publication that will specify a cryptographic algorithm for use by the U.S. Government to protect sensitive but unclassified information. It is expected that AES will be adopted by other private and public organizations inside and outside of the United States.

The Rijndael Block Cipher

The Rijndael algorithm was designed to have the following properties:

- Resistance against all known attacks
- Design simplicity
- Code compactness and speed on a wide variety of platforms

The Rijndael cipher can be categorized as an iterated block cipher with a variable block length and key length that can be independently chosen as 128, 192, or 256 bits.

In decimal terms, there are approximately 3.4×10^{38} possible 128 bit keys, 6.2×10^{57} possible 192-bit keys, and 1.1×10^{77} possible 256 bit keys.

As a measure of the relative strength of the Rijndael encryption algorithm, if a computer could crack the DES encryption by trying 256 keys in one second, the same computer would require 149 trillion (149×10^{12}) years to crack Rijndael. For a comparison, the universe is estimated to be less than 20 billion (20×10^9) years old.

Rijndael defines an intermediate cipher result as a *State* upon which the transformations that are defined in the cipher operate.

Instead of a Feistel network that takes a portion of the modified plaintext and transposes it to another position, the Rijndael Cipher employs a round transformation that is comprised of three *layers* of distinct and invertible transformations. These transformations are also defined as uniform, which means that every bit of the State is treated the same. Each of the layers has the following, respective functions:

- *The non-linear layer.* The parallel application of S-boxes that have optimum worst-case nonlinearity properties
- *The linear mixing layer.* Layer that provides a guarantee of a high diffusion of multiple rounds
- *The key addition layer.* An Exclusive Or of the Round Key to the intermediate State

Round keys are derived from the Cipher key through a key schedule, which consists of a key expansion and Round key selection, defined as follows in the Rijndael Block Cipher AES Proposal (*AES Proposal: Rijndael*, Joan Daemen and Vincent Rijmen, version2, 9/8/99), submitted to the National Institute of Standards and Technology (NIST).

The total number of Round key bits is equal to block length multiplied by the number of rounds plus 1, (e.g., for a block length of 128 bits and 10 rounds, 1408 Round Key bits are needed.) The Cipher Key is expanded into an Expanded Key. Round Keys are taken from the Expanded Key . . .

The Rijndael Block Cipher is suited for the following types of implementations:

- High speed chips with no area restrictions
- A compact co-processor on a smart card

The Twofish Algorithm

Another example of the evolution of cryptographic technology is found in the Twofish algorithm, one of the finalists in the AES competition.

In summary, Twofish is a symmetric block cipher that operates on 128-bit blocks in 16 rounds that works in all standard modes. It can accept key lengths up to 256 bits.

Twofish is a Feistel network in that in each round, one-half of the 128-bit block of plaintext or modified plaintext is fed into an element called the F Function box and, then, is XORed with the other half of the text in the network. This one-half block is broken into two 32-bit units that are, in turn, broken into four bytes. These four bytes are fed into four, different, key-dependent S boxes that emerge from the S-boxes as four transformed output bytes.

The four output bytes of the S boxes are combined in a Maximum Distance Separable (MDS) matrix to form two 32-bit units. These two 32-bit units are then combined using a Pseudo-Hadamard Transform (PHT) and are added to two round subkeys. The PHT is a linear operation of the form

$$d_1 = (2b_1 + b_2) \bmod 256$$

where b_1 and b_2 are the inputs, and d_1 is the output.

These results are XORed with the right half of the 64 bits of the plaintext. In addition, 1-bit rotations are performed before and after the XOR. These operations are then repeated for 15 more rounds.

Twofish also employs what is termed as “prewhitening” and “postwhitening” where additional subkeys are XORed with the plaintext before the first round and after the sixteenth round. This approach makes cryptanalysis more difficult because the whitening subkeys have to be determined in addition to the algorithm key.

In the Twofish algorithm, the MDS matrix, the PHT, and key additions provide diffusion.

The IDEA Cipher

The International Data Encryption Algorithm (IDEA) cipher is a secure, secret, key block encryption algorithm that was developed by James Massey and Xuejia Lai. (X. Lai, “On the Design and Security of Block Ciphers,” *ETH Series on Information Processing*, v.1, Konstanz: Hartung-Gorre Verlag, 1992) It evolved in 1992 from earlier algorithms called the Proposed Encryption Standard and the Improved Proposed Encryption Standard. IDEA operates on 64-bit Plaintext blocks and uses a 128 bit key. It applies both confusion and diffusion.

The IDEA algorithm performs eight rounds and operates on 16-bit sub-blocks using algebraic calculations that are amenable to hardware implementation. These operations are modulo 216 addition, modulo 216 1 1 multiplication and the Exclusive Or.

With its 128 bit key, an IDEA cipher is much more difficult to crack than DES. IDEA operates in the modes described for DES and is applied in the Pretty Good Privacy (PGP) email encryption system that was developed by Phil Zimmerman.

RC5

RC5 is a family of cryptographic algorithms invented by Ronald Rivest in 1994. It is a block cipher of variable block length, encrypts through integer addition, the application of a bit-wise Exclusive Or, and variable rotations. The key size and number of rounds are also variable. Typical block sizes are 32, 64, or 128 bits. The number of rounds can range from 0 to 255 and the key size can range from 0 to 2048 bits. RC5 was patented by RSA Data Security in 1997.

Public (Asymmetric) Key Cryptosystems

Unlike secret key cryptosystems, which make use of a single key that is known to a sender and receiver, public key systems employ two keys, a public key and a private key. The public key is made available to anyone wanting to encrypt and send a message. The private key is used to decrypt the message. Thus, the need to exchange secret keys is eliminated. The following are the important points to note:

- The public key cannot decrypt the message that it encrypted.
- Ideally, the private key cannot be derived from the public key.
- A message that is encrypted by one of the keys can be decrypted with the other key.
- The private key is kept private.

When K_p is the public key and K_s is the private key, the process is illustrated as

$$C = K_p(P) \text{ and } P = K_s(C)$$

where C is the ciphertext and P is the plaintext.

In addition, the reverse is also true where,

$$C = K_s(P) \text{ and } P = K_p(C)$$

One-Way Functions

Public key cryptography is possible through the application of a *one-way function*. A one-way function is a function that is easy to compute in one direction, yet is difficult to compute in the reverse direction. For such a function, if $y = f(x)$, it would be easy to compute y if given x, yet it would be very difficult to derive x given y. A simple example would be in the use of the telephone directory. It is easy to find a number given a name, but it is difficult to find the name given a number. For a one-way function to be useful in the context of public key cryptography, it should have a *trapdoor*. A trapdoor is a secret mechanism that enables you to easily accomplish the reverse function in a one-way function. Thus, if you know the trapdoor, you can easily derive x in the previous example, when given y.

In the context of public key cryptography, it is very difficult to calculate the private key from the public key unless you know the trapdoor.

Public Key Algorithms

A number of public key algorithms have been developed. Some of these algorithms are applicable to digital signatures, encryption, or both. Because there are more calculations associated with public key cryptography, it is 1,000 to 10,000 times slower than secret key cryptography. Thus, *hybrid* systems have evolved that use public key cryptography to safely distribute the secret keys used in symmetric key cryptography.

Some of the important public key algorithms that have been developed include the Diffie—Hellman key exchange protocol, RSA, El Gamal, Knapsack, and Elliptic Curve.

RSA

RSA is derived from the last names of its inventors, Rivest, Shamir, and Adleman (R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public -Key Cryptosystems," *Communications of the ACM*, v. 21, n.2, Feb 1978, pp. 120-126). This algorithm is based on the difficulty of factoring a number, N, which is the product of two large prime numbers. These numbers may be 200 digits each. Thus, the difficulty in obtaining the private key from the public key is a hard, one-way function that is equivalent to the difficulty of finding the prime factors of N.

In RSA, public and private keys are generated as follows:

- Choose two large prime numbers, p and q, of equal length, compute $p \cdot q = n$, which is the public modulus.
- Choose a random public key, e, so that e and $(p - 1)(q - 1)$ are relatively prime.
- Compute $e \cdot d = 1 \pmod{(p - 1)(q - 1)}$, where d is the private key.
- Thus, $d = e^{-1} \pmod{[(p - 1)(q - 1)]}$

From these calculations, (d, n) is the private key and (e, n) is the public key.

The plaintext, P, is thus encrypted to generate ciphertext C as

$$C = P^e \pmod n,$$

and is decrypted to recover the plaintext, P , as

$$P = C^d \text{ mod } n.$$

Typically, the plaintext will be broken into equal length blocks, each with fewer digits than n , and each block will be encrypted and decrypted as shown.

RSA can be used for encryption, key exchange, and digital signatures.

Diffie—Hellman Key Exchange

The Diffie—Hellman Key Exchange is a method where subjects exchange secret keys over a nonsecure medium without exposing the keys. The method was disclosed by Dr. W. Diffie and Dr. M.E. Hellman in their seminal 1976 paper entitled “New Directions in Cryptography [Whitfield Diffie and Martin Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory*, Vol. IT-22 (November 1976), pp. 644-54].

The method enables two users to exchange a secret key over an insecure medium without an additional session key. It has two system parameters, p and g . Both parameters are public and may be used by all the system’s users. Parameter p is a prime number and parameter g (which is usually called a generator) is an integer less than p that has the following property: For every number n between 1 and $p - 1$ inclusive, there is a power k of g such that $gk = n \text{ mod } p$.

For example, when given the following public parameters:

p = prime number

g = generator

Generating Equation $y = gx \text{ mod } p$

Alice and Bob can securely exchange a common secret key as follows:

Alice can use her private value “ a ” to calculate

$$y_a = g^a \text{ mod } p$$

Also, Bob can use his private value “ b ” to calculate the following:

$$y_b = g^b \text{ mod } p.$$

Alice can now send y_a to Bob, and Bob can send y_b to Alice. Knowing her private value, a , Alice can calculate $(y_b)^a$ which yields the following:

$$g^{ba} \text{ mod } p.$$

Similarly, with his private value, b , Bob can calculate $(y_a)^b$ as

$$g^{ab} \text{ mod } p.$$

Because $g^{ba} \text{ mod } p$ is equal to $g^{ab} \text{ mod } p$, Bob and Alice have securely exchanged the secret key.

In their paper, Diffie and Hellman primarily described key exchange, yet they also provided a basis for the further development of public key cryptography.

EI Gamal

Dr. T. El Gamal extended the Diffie-Hellman concepts to apply to encryption and digital signatures (T. El Gamal, “A Public-Key Crypto System and a Signature Scheme Based on Discrete Logarithms,” *Advances in Cryptography: Proceedings of CRYPTO 84*,

Springer-Verlag, 1985, pp 10-18.) The El Gamal system is a non-patented public-key cryptosystem that is based on the discrete logarithm problem. Encryption with El Gamal is illustrated in the following example:

Given the prime number, p , and the integer, g , Alice uses her private key, a , to compute her public key as $y = g^a \text{ mod } p$

For Bob to send message M to Alice:

Bob generates random $\#b < p$

Bob computes $y_b = g^b \text{ mod } p$ and $y_m = M \text{ XOR } y^b = M \text{ XOR } g^{ab} \text{ mod } p$.

Bob sends y_b, y_m to Alice and Alice computes $y_b^a = g^{ab} \text{ mod } p$.

Therefore, $M = y_b^a \text{ XOR } y_m = g^{ab} \text{ mod } p \text{ XOR } M \text{ XOR } g^{ab} \text{ mod } p$.

Merkle-Hellman Knapsack

The Merkle-Hellman Knapsack (R.C. Merkle and M. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks," *IEEE Transactions on Information Theory*, v.24, n. 5, Sep 1978, pp. 525-530.) is based on the problem of having a set of items with fixed weights and determining which of these items can be added to in order to obtain a given total weight.

This concept can be illustrated using a superincreasing set of weights. Superincreasing means that each succeeding term in the set is greater than the sum of the previous terms. The set [2,3,6,12,27,52] has these properties. If we have a knapsack with a total weight of 69 for this example, the problem would be to find the terms whose sum is equal to 69. The solution to this simple example is that terms 52, 12, 3, and 2 would be in the knapsack. Or equivalently, if we represent the terms that are in the knapsack by 1s and those that are not by 0s, the "ciphertext" representing the "plaintext 69" is 110101.

Elliptic Curve (EC)

Elliptic curves are another approach to public key cryptography. This method was developed independently by Neal Koblitz (N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, v. 48, n. 177, 1987, pp. 203-209) and V.S. Miller (V.S. Miller, "Use of Elliptic Curves in Cryptography," *Advances in Cryptology-CRYPTO '85 Proceedings*, Springer-Verlag, 1986, pp. 417-426). Elliptic curves are usually defined over finite fields such as real and rational numbers and implement an analog to the discrete logarithm problem.

An elliptic curve is defined by the following equation:

$$y^2 = x^3 + ax + b \text{ along with a single point } O, \text{ the point at infinity.}$$

The space of the elliptic curve has the properties where

- Addition is the counterpart of modular multiplication.
- Multiplication is the counterpart of modular exponentiation.

Thus, given two points, P and R , on an elliptic curve where $P = KR$, finding K is the hard problem that is known as the elliptic curve discrete logarithm problem.

Because it is more difficult to compute elliptic curve discrete logarithms than conventional discrete logarithms or to factor the product of large prime numbers, smaller key sizes in the elliptic curve implementation can yield higher levels of security.

For example, an elliptic curve key of 160 bits is equivalent to 1024-bit RSA key. This characteristic means less computational and memory requirements. Therefore, elliptic curve cryptography is suited to hardware applications such as smart cards and wireless devices. Elliptic curves can be used to implement digital signatures, encryption, and key management capabilities.

Public Key Cryptosystems Algorithm Categories

Public key encryption utilizes hard, one-way functions. The problems using this type of encryption are

- Factoring the product of large prime numbers
 - RSA
- Finding the discrete logarithm in a finite field
 - El Gamal
 - Diffie-Hellman
 - Schnorr's signature algorithm
 - Elliptic curve
 - Nyberg-rueppel's signature algorithm

Asymmetric and Symmetric Key Length Strength Comparisons

A comparison of the approximate equivalent strengths of public and private key cryptosystems is provided in Table 4.2.

ASYMMETRIC KEY SIZE	SYMMETRIC KEY SIZE
512 Bits	64 Bits
1792 Bits	112 Bits
2304 Bits	128 Bits

Digital Signatures

The purpose of digital signatures is to detect unauthorized modifications of data, and to authenticate the identity of the signatories and non-repudiation. These functions are accomplished by generating a block of data that is usually smaller than the size of the original data. This smaller block of data is bound to the original data and to the identity of the sender. This binding verifies the integrity of data and provides non-repudiation. To quote the National Institute Standards and Technology (NIST) Digital Signature Standard (DSS) [National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U.S. Department of Commerce, May 1994]:

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory.

To generate a digital signature, the digital signal program passes the file to be sent through a one-way *hash* function. This hash function produces a fixed size output from a variable size input. The output of the hash function is called a *message digest*. The message digest is uniquely derived from the input file and, if the hash algorithm is strong, the message digest has the following characteristics:

- The hash function is considered one-way because the original file cannot be created from the message digest.

- Two files should not have the same message digest.
- Given a file and its corresponding message digest, it should not be feasible to find another file with the same message digest.
- The message digest should be calculated using all of the original file's data.

After the message digest is calculated, it is encrypted with the sender's private key. The encrypted message digest is then attached to the original file and is sent to the receiver. The receiver, then, decrypts the message digest using the sender's public key. If this public key opens the message digest and it is the true public key of the sender, verification of the sender is then accomplished. Verification occurs because the sender's public key is the only key that can decrypt the message digest encrypted with the sender's private key. Then, the receiver can compute the message digest of the received file using the *identical hash* function as the sender. If this message digest is identical to the message digest that was sent as part of the signature, the message has not been modified.

Digital Signature Standard (DSS) and Secure Hash Standard (SHS)

NIST announced the Digital Signature Standard (DSS) Federal Information Processing Standard (FIPS) 186-1. This standard enables the use of the RSA digital signature algorithm or the Digital Signature Algorithm (DSA.) The DSA is based on a modification of the El Gamal digital signature methodology and was developed by Claus Schnorr (C.P.Schnorr, "Efficient Signature Generation for Smart Cards," *Advances in Cryptology-CRYPTO '89 Proceedings*, Springer-Verlag, 1990, pp. 239-252).

Both of these digital signature algorithms use the Secure Hash Algorithm (SHA-1) as defined in FIPS 180 (National Institute of Standards and Technology, NIST FIPS PUB 180, "Secure Hash Standard," U.S. Department of Commerce, May 1993).

The Secure Hash Algorithm (SHA-1) computes a fixed length message digest from a variable length input message. This message digest is then processed by the DSA to either generate or verify the signature. Applying this process to the shorter message digest is more efficient than applying it to the longer message.

As previously discussed, any modification to the message being sent to the receiver results in a different message digest being calculated by the receiver. Thus, the signature will not be verified.

SHA-1 produces a message digest of 160 bits when any message less than 264 bits is used as an input.

SHA-1 has the following properties:

- It is computationally infeasible to find a message that corresponds to a given message digest.
- It is computationally infeasible to find two different messages that produce the same message digest.

For SHA-1, the *length* of the message is the number of bits in a message. Padding bits are added to the message to make the total length of the message, including padding, a multiple of 512. To quote from the NIST DSS/SHS document:

*The SHA-1 sequentially processes blocks of 512 bits when computing a message digest. The following specifies how the padding shall be performed. As a summary, a "1" followed by m "0's" followed by a 64-bit integer are applied to the end of the message to produce a padded message of length 512*n. The 64-bit integer is l, the length of the original message. The padded message is then processed by the SHA-1 as n 512-bit blocks.*

MD5

MD5 is a message digest algorithm that was developed by Ronald Rivest in 1991. MD5 takes a message of an arbitrary length and generates a 128-bit message digest. In MD5, the message is processed in 512-bit blocks in four distinct rounds.

Sending a Message with a Digital Signature

In summary, to send a message

1. A hash algorithm is used to generate the message digest from the message.
2. The message digest is fed into the digital signature algorithm that generates the signature of the message. The signing of the message is accomplished by encrypting the message digest with the sender's private key and attaching the result to the message. Thus, the message is a signed message.
3. The message and the attached message digest are sent to the receiver. The receiver then decrypts the attached message digest with sender's public key. The receiver also calculates the message digest of the received message using the identical hash function as the sender. The two message digests should be identical. If they are not identical, the message was modified in transmission. If the two message digests are identical, then the message sent is identical to the message received, the sender is verified, and the sender cannot repudiate the message.

Hashed Message Authentication Code (HMAC)

An HMAC is a hash algorithm that uses a key to generate a Message Authentication Code (MAC). A MAC is a type of check sum that is a function of the information in the message. The MAC is generated before the message is sent, appended to the message, and then both are transmitted.

At the receiving end, a MAC is generated from the message alone using the same algorithm as used by the sender and this MAC is compared to the MAC sent with the message. If they are not identical, the message was modified en route. Hashing algorithms can be used to generate the MAC and hash algorithms using keys provide stronger protection than an ordinary MAC generation.

Hash Function Characteristics

As described in the previous section, a hash function (H) is used to condense a message of an arbitrary length into a fixed length message digest. This message digest should uniquely represent the original message, and it will be used to create a digital signature. Furthermore, it should not be computationally possible to find two messages, M1 and M2, such that $H(M1) = H(M2)$. If this situation were possible, then an attacker could substitute another message (M2) for the original message (M1) and the message digest would not change. Because the message digest is the key component of the digital signature authentication and integrity process, a false message could be substituted for the original message without detection. Specifically, it should not be computationally possible to find

- A message (M2) that would hash to a specific message digest generated by a different message (M1)
- Two messages that hash to any common message digest

These two items refer to an attack against the hash function known as a *birthday attack*. This attack relates to the paradoxes that are associated with the following questions:

1. If you were in a room with other people, what would be the sample size, n , of individuals in the room to have a better than 50/50 chance of someone having the same birthday as you? (The answer is 253.)
2. If you were in a room with other people, what would be the sample size, n , of individuals in the room to have a better than 50/50 chance of at least two people having a common birthday? (The answer is 23, since, with 23 people in a room, there are $n(n-1)/2$ or 253 pairs of individuals in the room.)

Cryptographic Attacks

As defined earlier, cryptanalysis is the act of obtaining the plaintext or key from the ciphertext. Cryptanalysis is used to obtain valuable information and to pass on altered or fake messages in order to deceive the original intended recipient. This attempt at “cracking” the cipher is also known as an attack. The following are example of some common attacks:

- *Brute Force*. Trying every possible combination of key patterns — the longer the key length, the more difficult it is to find the key with this method
- *Known Plaintext*. The attacker has a copy of the plaintext corresponding to the ciphertext
- *Chosen Plaintext*. Chosen plaintext is encrypted and the output ciphertext is obtained
- *Adaptive Chosen Plaintext*. A form of a chosen plaintext attack where the selection of the plaintext is altered according to the previous results
- *Ciphertext Only*. Only the ciphertext is available
- *Chosen Ciphertext*. Portions of the ciphertext are selected for trial decryption while having access to the corresponding decrypted plaintext
- *Adaptive Chosen Ciphertext*. A form of a chosen ciphertext attack where the selection of the portions of ciphertext for the attempted decryption is based on the results of previous attempts
- *Birthday Attack*. Usually applied to the probability of two different messages using the same hash function that produces a common message digest; or given a message and its corresponding message digest, finding another message that when passed through the same hash function generates the same specific message digest. The term “birthday” comes from the fact that in a room with 23 people, the probability of two or more people having the same birthday is greater than 50%.
- *Meet-in-the-Middle*. Is applied to double encryption schemes by encrypting known plaintext from one end with each possible key (K) and comparing the results “in the middle” with the decryption of the corresponding ciphertext with each possible K
- *Man-in-the-Middle*. An attacker taking advantage of the store-and-forward nature of most networks by intercepting messages and forwarding modified versions of the original message while in between two parties attempting secure communications

- *Differential Cryptanalysis.* Is applied to private key cryptographic systems by looking at ciphertext pairs, which were generated through the encryption of plaintext pairs, with specific differences and analyzing the effect of these differences
- *Linear Cryptanalysis.* Using pairs of known plaintext and corresponding ciphertext to generate a linear approximation of a portion of the key
- *Differential Linear Cryptanalysis.* Using both differential and linear approaches
- *Factoring.* Using a mathematical approach to determine the prime factors of large numbers
- *Statistical.* Exploiting the lack of randomness in key generation

Public Key Certification Systems

A source that could compromise a public key cryptographic system is an individual (A) who is posting a public key under the name of another individual (B). In this scenario, the people who are using this public key to encrypt the messages that were intended for individual B will actually be sending messages to individual A. Because individual A has the private key that corresponds to the posted public key, individual A can decrypt the messages that were intended for individual B.

Digital Certificates

To counter this type of attack, a certification process can be used to bind individuals to their public keys. A Certificate Authority (CA) acts as notary by verifying a person’s identity and issuing a certificate that vouches for a public key of the named individual. This certification agent signs the certificate with its own private key. Therefore, the individual is verified as the sender if that person’s public key opens the data. The certificate contains the subject’s name, the subject’s public key, the name of the certificate authority, and the period in which the certificate is valid. To verify the CA’s signature, its public key must be cross-certified with another CA. (The X.509 standard defines the format for public key certificates.) This Certificate is then sent to a Repository, which holds the Certificates and Certificate Revocation Lists (CRLs) that denote the revoked certificates. The diagram shown in Figure 4.21 illustrates the use of digital certificates in a transaction between a subscribing entity and a transacting party.



Figure 4.21: A transaction with digital certificates.

Public Key Infrastructure (PKI)

The integration of digital signatures and certificates, and the other services required for E-commerce is called the Public Key Infrastructure (PKI). These services provide integrity, access control, confidentiality, authentication, and non-repudiation for electronic transactions. The PKI includes the following elements:

- Digital certificates
- Certificate Authority (CA)
- Registration authorities
- Policies and procedures
- Certificate revocation
- Non-repudiation support
- Timestamping
- Lightweight Directory Access Protocol (LDAP)
- Security-enabled applications
- Cross certification

The Lightweight Directory Access Protocol (LDAP) provides a standard format to access the certificate directories. These directories are stored on LDAP servers on a network and the servers on these networks provide public keys and corresponding X.509 certificates for the enterprise. A directory contains information such as the individuals' names, addresses, phone numbers, and public key certificates. LDAP enables a user to search these directories over the Internet. A series of standards under X.500 defines the protocols and information models for computer directory services that are independent of the platforms and other related entities.

The primary security concerns relative to LDAP servers are availability and integrity. For example, denial of service attacks on an LDAP server could prevent access to the Certification Revocation Lists and, thus, permit the use of a revoked certificate for transactions.

Approaches to Escrowed Encryption

In some instances, there is a need for law enforcement agencies to have access to information transmitted electronically over computer networks. To have this access, law enforcement agencies need the encryption keys to read the enciphered messages. At the same time, the privacy of citizens must be protected from illegal and unauthorized surveillance of their digital communications. This section describes two approaches to this issue.

The Escrowed Encryption Standard

This standard (National Institute of Standards and Technology, NIST FIPS PUB 185, "Escrowed Encryption Standard," U.S. Department of Commerce, Feb 1994) strives to achieve individual privacy and, at the same time, strives to provide for legal monitoring of the encrypted transmissions. The idea is to divide the key into two parts, and to escrow two portions of the key with two separate "trusted" organizations. Then, law enforcement officials, after obtaining a court order, can retrieve the two pieces of the key from the organizations and decrypt the message. The Escrowed Encryption Standard is embodied in the U.S. Government's Clipper Chip, which is implemented in tamper-proof hardware. The Skipjack Secret Key algorithm performs the encryption. Figure 4.22 is a block diagram of the clipper chip and the components of a transmitted message.

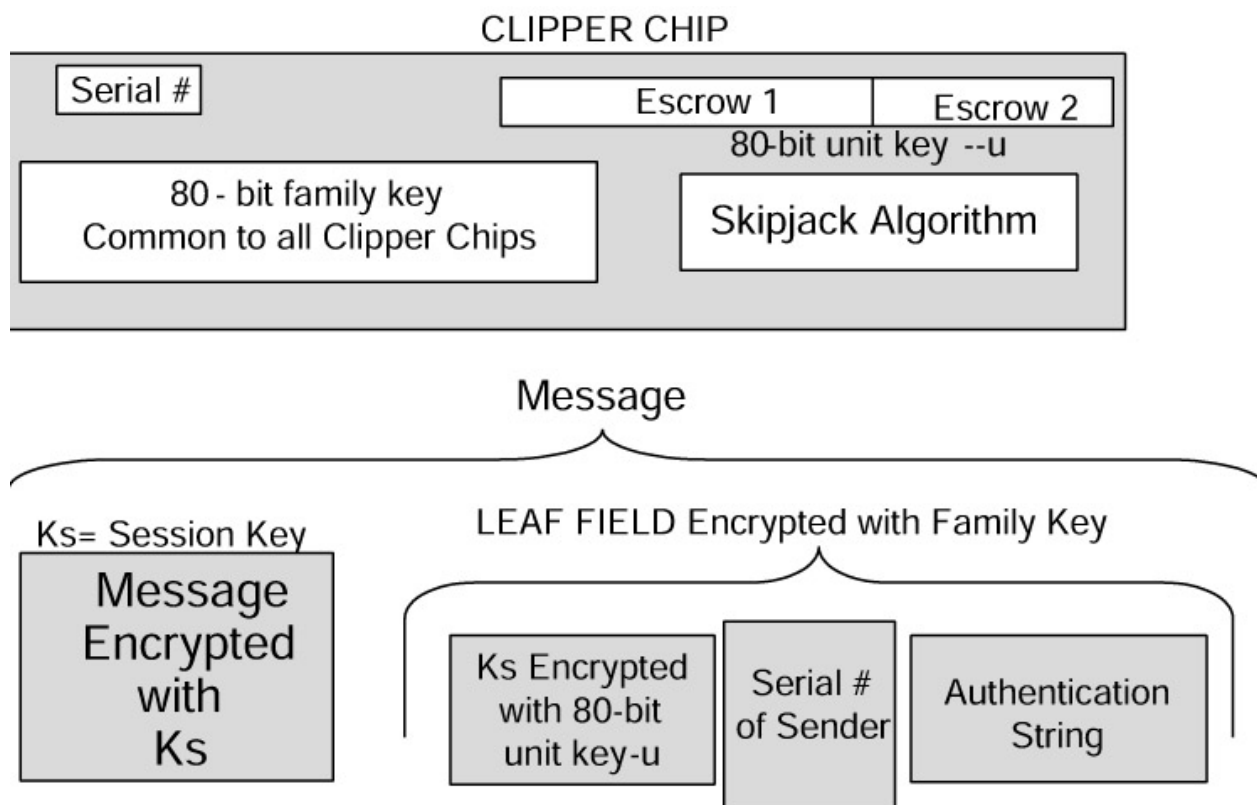


Figure 4.22: A Clipper Chip block diagram.

Each Clipper Chip has a unique serial number and an 80-bit unique unit or secret key. The unit key is divided into two parts and is stored at two separate organizations with the serial number that uniquely identifies that particular Clipper Chip. Initially, two parties that wish to exchange information agree on a session key, K_s . K_s can be exchanged using a Diffie-Hellman or an RSA key exchange. The plaintext message, M , is encrypted with the session key, K_s . K_s is not escrowed. In addition, a Law Enforcement Access Field (LEAF) is also transmitted along with the encrypted message, M . The LEAF is encrypted with the family key, which is common to all Clipper Chips, and contains the following:

- K_s encrypted with secret key, u
- The serial number of sender Clipper Chip
- An authentication string

When the intended individual receives the transmitted items, this person decrypts the message with the mutually known session key, K_s .

A law enforcement agency can obtain the session key as follows:

1. Decrypt the LEAF with a family key to obtain the particular Clipper Chip serial number and encrypted session key. K_s is still encrypted with secret family key, u .
2. Present an authorization court order to the two escrow agencies and obtain the two portions of the key, u .
3. Decrypt K_s with the key, u .
4. Decrypt the message, M , with K_s .

The 80-bit key of the Clipper Chip is weak. In fact, concerns exist over the escrow agencies' abilities to protect the escrowed keys, and whether these agencies may divulge them in unauthorized ways.

Key Escrow Approaches Using Public Key Cryptography

Another key escrow approach is Fair Cryptosystems.

In 1992, Sylvio Micali introduced the concept of Fair Cryptosystems (S. Micali, "Fair Cryptosystems," MIT/LCS/TR-579.b, MIT Laboratory for Computer Science, Nov 1993) where the private key of a public/private key pair is divided into multiple parts and distributed to different trustees. In 1994, Micali obtained patents on this approach that were eventually purchased by Banker's Trust. One valuable characteristic of Micali's approach is that each portion of the secret key can be verified as correct without having to reconstruct the entire key. This is accomplished by giving each trustee a piece of each public key and private key. Micali also developed calculations, which can be used on the each trustee's private/public key pieces to verify that they are correct. If authorities have the legal permission to decrypt a message that is encrypted with the secret key, they can obtain all the portions of the private key and read the message. Micali also proposed a threshold approach where some subset of the trustee's set would be sufficient to recover the entire secret key.

Micali's approach can be applied by voluntary trustees in different countries or business areas rather than by a controlled, governmental entity.

Key Management Issues

Obviously, when dealing with encryption keys, the same precautions must be used as with physical keys to secure the areas or the combinations to the safes. These precautions include the following:

- Key control measures
- Key recovery
- Key storage
- Key retirement/destruction
- Key change
- Key generation
- Key theft
- Frequency of key use

Email Security Issues and Approaches

The main objectives of email security are to ensure the following:

- Non-repudiation
- Messages are read only by their intended recipients
- Integrity of the message
- Authentication of the source
- Verification of delivery
- Labeling of sensitive material
- Control of access

The following "standards" have been developed to address some or all of these issues.

Secure Multipurpose Internet Mail Extensions (S/MIME)

S/MIME is a specification that adds secure services to email in a MIME format. S/MIME provides authentication through digital signatures and the confidentiality of encryption. S/MIME follows the Public Key Cryptography Standards (PKCS) and uses the X.509 standard for its digital certificates.

MIME Object Security Services (MOSS)

MOSS provides flexible email security services by supporting different trust models. Introduced in 1995, MOSS provides authenticity, integrity, confidentiality, and non-repudiation to email. It uses MD2/MD5, RSA Public Key, and DES. MOSS also permits user identification outside of the X.509 Standard.

Privacy Enhanced Mail (PEM)

Privacy Enhanced Mail (PEM) is a standard that was proposed by the IETF to be compliant with the Public Key Cryptography Standards (PKCS) which were developed by a consortium that included Microsoft, Novell, and Sun Microsystems. PEM supports the encryption and authentication of Internet email. For message encryption, PEM applies Triple DES—EDE using a pair of symmetric keys. RSA Hash Algorithms MD2 or MD5 are used to generate a message digest, and RSA public key encryption implements digital signatures and secure key distribution. PEM employs certificates that are based on the X.509 standard and are generated by a formal CA.

Pretty Good Privacy (PGP)

In order to bring email security to the “masses,” Phil Zimmerman developed the Pretty Good Privacy (PGP) software (Zimmerman, Philip R., *The Official PGP User’s Guide* Cambridge, MA: MIT Press, 1995). Zimmerman derived the PGP name from Ralph’s Pretty Good Groceries, which sponsored Garrison Keillor’s *Prairie Home Companion* radio show. In PGP, the symmetric cipher IDEA is used to encipher the message, and RSA is used for symmetric key exchange and for digital signatures.

Instead of using a CA, PGP uses a “Web of Trust.” Users can certify each other in a mesh model, which is best applied to smaller groups (as shown in Figure 4.23).

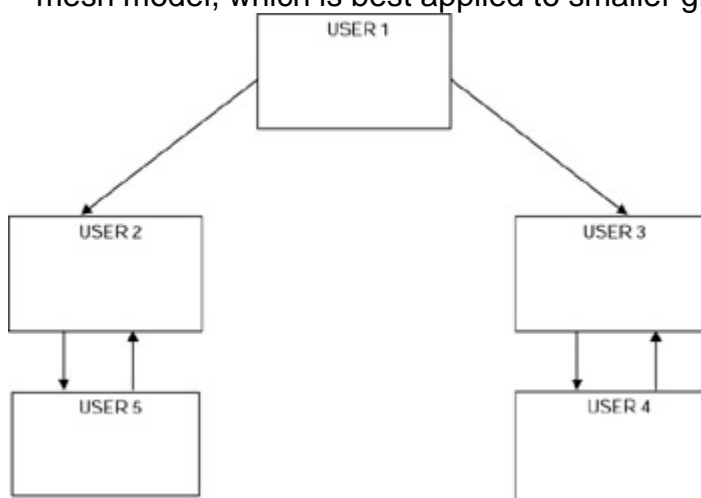


Figure 4.23: A PGP Web of Trust.

Internet Security Applications

With the growing use of the Internet and World Wide Web for commercial transactions, there is a need for providing confidentiality, integrity and authentication of information. This section describes some of the approaches to obtain secure Internet and World Wide Web ecommerce.

Message Authentication Code (MAC) or the Financial Institution Message Authentication Standard (FIMAS)

In order to protect against fraud in electronic fund transfers, the Message Authentication Code (MAC), ANSI X9.9, was developed. The MAC is a check value, which is derived from the contents of the message itself, that is sensitive to the bit changes in a message. It is similar to a Cyclic Redundancy Check (CRC). A MAC is appended to the message before it is transmitted. At the receiving end, a MAC is generated from the received message and is compared to the MAC of an original message. A match indicates that the message was received without any modification occurring while en route.

To strengthen the MAC algorithm, a keyed MAC can be generated using a symmetric key encryption, such as DES. Typically, the Exclusive Or function of the DES key with a message is performed on the sequential, 8-byte blocks of the message to generate the MAC. As with all symmetric key applications, the key must be distributed securely so that sender and receiver have the same key.

Secure Electronic Transaction (SET)

A consortium including MasterCard and Visa developed SET in 1997 as a means of preventing fraud from occurring during electronic payments. SET provides confidentiality for purchases by encrypting the payment information. Thus, the seller cannot read this information. SET uses a DES symmetric key system for encryption of the payment information and uses RSA for the symmetric key exchange and digital signatures. SET covers the end-to-end transactions from the cardholder to the financial institution.

Secure Sockets Layer (SSL)/Transaction Layer Security (TLS)

The SSL protocol was developed by Netscape in 1994 to secure Internet client-server transactions. The SSL protocol authenticates the server to the client using public key cryptography and digital certificates. In addition, this protocol also provides for optional client to server authentication. It supports the use of RSA public key algorithms, IDEA, DES and 3DES private key algorithms, and the MD5 hash function. Web pages using the SSL protocol start with HTTPS. SSL 3.0 and its successor, the Transaction Layer Security (TLS) 1.0 protocol are defacto standards, but they do not provide the end-to-end capabilities of SET. TLS implements confidentiality, authentication, and integrity above the Transport Layer, and it resides between the application and TCP layer. Thus, TLS, as with SSL, can be used with applications such as Telnet, FTP, HTTP, and email protocols. Both SSL and TLS use certificates for public key verification that are based on the X.509 standard.

Internet Open Trading Protocol (IOTP)

IOTP is an Internet protocol that is aimed at the consumer-to-business transactions. It provides a buyer with the same options as in the ordinary, non-ecommerce marketplace. IOTP is similar to shopping in the real world because it gives buyers the option to choose their method of payment. It supports public and private encryption key algorithms and can use digital certificates. IOTP is designed to be flexible and to accommodate other payment models that may emerge in the future.

MONDEX

The MONDEX International Corporation operates the MONDEX payment system. This system is an example of a cash smart card application. The value of the amount of currency is stored in smart cards and a proprietary encryption algorithm provides security. Because the algorithm is not subject to public scrutiny, its strength and vulnerabilities are not known. The smart card, then, can be used in financial transactions instead of cash. Funds can be transferred among cards using digital signatures. The smart cards are designed to preclude tampering and modifying the stored currency amount. However, if a card is lost, the finder can use it as cash.

IPSec

IPSec is a standard that provides encryption, access control, non-repudiation, and authentication of messages over an IP. It is designed to be functionally compatible with IPv6. The two main protocols of IPSec are the *Authentication Header (AH)* and the *Encapsulating Security Payload (ESP)*. The AH provides integrity, authentication, and non-repudiation. An ESP primarily provides encryption, but it can also provide limited authentication.

At the heart of IPSec is the *Security Association (SA)*. An SA is required for communication between two entities. It provides a one-way (simplex) connection and is comprised of a *Security Parameter Index (SPI)*, destination IP address, and the identity of the security protocol (AH or ESP.) The SPI is a 32-bit number that is used to distinguish among various SAs terminating at the receiving station. Because an SA is simplex, two SAs are required for bi-directional communication between entities. Thus, if the AH protocol is used and bi-directional communication is required, two SAs must be established. Similarly, if both the AH and ESP protocols are to be employed bi-directionally, four SAs are needed.

IPSec in a VPN implementation can operate in either the *transport* or *tunnel mode*. In the transport mode, the data in the IP packet is encrypted, but the header is not encrypted. In the tunnel mode, the original IP header is encrypted and a new IP header is added to the beginning of the packet. This additional IP header has the address of the VPN gateway, and the encrypted IP header points to the final destination on the internal network behind the gateway.

The hashing algorithms HMAC-MD5 and HMAC-SHA-1 are used for authentication and integrity, and IPSEC standard enables for the use of a variety of symmetric key systems.

Security Associations (SAs) can be combined into “bundles” to provide authentication, confidentiality, and layered communication. An SA bundle can be developed using *transport adjacency* or *iterated tunneling*. Transport adjacency uses the transport mode for communication wherein iterated tunneling provides for the multiple levels of encapsulation as the protocol stack is being traversed.

In order to set up and manage SAs on the Internet, a standard format called the Internet Security Association and Key Management Protocol (ISAKMP) was established. ISAKMP provides for secure key exchange and data authentication. However, ISAKMP is independent of the authentication protocols, security protocols, and encryption algorithms. Strictly speaking, a combination of three protocols is used to define the key management for IPSEC. These protocols are ISAKMP, Secure Key Exchange Mechanism (SKEME) and Oakley. When combined and applied to IPSEC, these protocols are called the Internet Key Exchange (IKE) protocol. In general, ISAKMP defines the phases for establishing a secure relationship, SKEME describes a secure exchange mechanism, and Oakley defines the modes of operation needed to establish a secure connection.

An initiative to specify a standard IPSEC implementation for VPNs on the Internet is known *Secure Wide Area Network (S/WAN)*. By defining a common set of IPSEC algorithms and modes of operation, S/WAN promotes the widespread use of VPNs on the Internet.

Secure Hypertext Transfer Protocol (S-HTTP)

S-HTTP is an alternative to SSL for providing security for World Wide Web (WWW) transactions. While SSL is applied to an entire session, S-HTTP can be used to protect individual WWW documents, and it provides authentication, confidentiality, integrity, and non-repudiation. S-HTTP supports a variety of encryption algorithms.

Secure Shell (SSH-2)

Secure Shell (SSH-2) is a set of protocols that are primarily used for remote access over a network by establishing an encrypted tunnel between an SSH client and an SSH server. This protocol can be used to authenticate the client to the server. In addition, it can also provide confidentiality and integrity services. It is comprised of a Transport Layer protocol, a User Authentication protocol, and a Connection protocol.

Wireless Security

With the increasing use and popularity of Personal Digital Assistants (PDAs) and cellular telephones to access the Internet, wireless security is important. Because information is broadcast like radio transmissions, it is susceptible to interception and can be compromised. As storage and processor technologies improve, Mobile Commerce (M-commerce) will be more common. Issues that are associated with wireless security include

- Physical security of wireless devices
- Proliferation of many different platforms
- Protection of sensitive financial transactions
- Limitations of processing power and memory due to space and weight considerations
- No standard method for securing wireless transactions
- Public Key Infrastructure (PKI)
- Wireless Application Protocol (WAP)

The Wireless Application Protocol (WAP) is widely used by mobile devices to access the Internet. Because it is aimed at small displays and systems with limited bandwidth, it is not designed to display large volumes of data on a small, mobile display. In addition to cellular phones and PDAs, WAP is applied to network browsing through TV and in automotive displays. It has analogies to TCP/IP, IP, and HTML in wired Internet connections and is actually a set of protocols that covers layer 7 to layer 3 of the OSI model. Due to the memory and processor limitations on mobile devices, WAP has less overhead than TCP/IP. The WAP protocol stack contains the following:

- Wireless Markup Language (WML) and Script
- Wireless Application Environment (WAE)
- Wireless Session Protocol (WSP)
- Wireless Transaction Protocol (WTP)
- Wireless Transport Layer Security Protocol (WTLS)
- Wireless Datagram Protocol (WDP)

For wireless security, WAP uses the Wireless Transport Layer Security Protocol (WTLS.) WTLS provides the following three classes of security:

1. *Class 1 (Anonymous Authentication)*. The client logs on to the server, but, in this mode, neither the client nor the server can be certain of the identity of the other.
2. *Class 2 (Server Authentication)*. The server is authenticated to the client, but the client is not authenticated to the server.
3. *Class 3 (Two-Way Client and Server Authentication)*. The server is authenticated to the client and the client is authenticated to the server.

Authentication and authorization can be performed on the mobile device using smart cards to execute PKI-enabled transactions.

A specific security issue that is associated with WAP is the “WAP GAP.” A WAP GAP results from the requirement to change security protocols at the carrier’s WAP gateway from the wireless WTLS to SSL for use over the wired network. At the WAP gateway, the transmission, which is protected by WTLS, is decrypted and then re-encrypted for transmission using SSL. Thus, the data is temporarily in the clear on the gateway and can be compromised if the gateway is not adequately protected. Improvements in WAP are aimed at eliminating this problem by using a client-side proxy server to transmit authentication and authorization information to the server of the wireless network. Another alternative is to encrypt the data at the application layer above the transport layer of WTLS and to maintain encryption throughout the transmission. In addition to performing conversion from WTLS to SSL, the WAP gateway also compiles applets and scripts due to the fact that most mobile devices do not have the capacity to incorporate interpreters in their browsers.

The Handheld Device Markup Language (HDML) is a simpler alternative to WML that actually preceded the Wireless Markup Language (WML). HDML contains minimal security features, however. A direct competitor to WAP is Compact HTML (C-HTML). Used primarily in Japan through NTT DoCoMo’s I-mode service, C-HTML is essentially a stripped-down version of HTML. Due to this approach, C-HTML can be displayed on a standard Internet browser.

The Public Key Infrastructure (PKI) for mobile applications provides for the encryption of communications and mutual authentication of the user and application provider. One concern associated with the “mobile PKI” relates to the possible time lapse between the expiration of a public key certificate and the re-issuing of a new valid certificate and associated public key.

This “dead time” may be critical in disasters or in time-sensitive situations. One solution to this problem is to generate one-time keys for use in each transaction.

The IEEE 802.11 Wireless Standard

The IEEE 802.11 specification is a wireless LAN standard that specifies an interface between a wireless client and a base station or access point, as well as among wireless clients. Work on the standard began in 1990 and has evolved from various draft versions; approval of the final draft occurred on June 26, 1997.

802.11 Layers

The IEEE 802.11 standard places specifications on the parameters of both the physical (PHY) and medium access control (MAC) layers of the network. The PHY Layer is responsible for the transmission of data among nodes. It can use direct sequence (DS) spread spectrum, frequency-hopping (FH) spread spectrum, or infrared (IR) pulse position modulation. The standard supports data rates of 1 Mbps or 2 Mbps, 2.4—

2.4835 GHz frequency band for spread-spectrum transmission, and 300—428,000 GHz for IR transmission. Infrared is generally considered to be more secure to eavesdropping than multidirectional radio transmissions, because infrared requires direct line-of-sight paths.

The MAC Layer is a set of protocols responsible for maintaining order in the use of a shared medium. The 802.11 standard specifies a carrier sense multiple access with collision avoidance (CSMA/CA) protocol as described in Chapter 3, “Telecommunications and Network Security,” for LANs. The MAC Layer provides the following services:

Data transfer. CSMA/CA media access.

Association. Establishment of wireless links between wireless clients and access points in infrastructure networks.

Reassociation. This action takes place in addition to association when a wireless client moves from one Basic Service Set (BSS) to another, such as in roaming.

Authentication. The process of proving a client identity through the use of the 802.11 option, Wired Equivalent Privacy (WEP). In WEP, a shared key is configured into the access point and its wireless clients. Only those devices with a valid shared key will be allowed to be associated to the access point.

Privacy. In the 802.11 standard, data is transferred in the clear by default. If confidentiality is desired, the WEP option encrypts data before it is sent wirelessly, using the RC4 40-bit encryption algorithm.

Power management. Two power modes are defined in the IEEE 802.11 standard: an active mode used in transmitting and receiving and a power save mode that conserves power but does not enable the user to transmit or receive.

The 802.11 standard has been ratified for IR, FH, and DH spread spectrum at 2.4 GHz. As of this writing, the IEEE 802.11 committee is addressing higher speed PHYs beyond the 2 Mbps data rate.

Sample Questions

Answers to the Sample Questions for this and the other chapters are found in Appendix C.

1. The Secure Hash Algorithm (SHA) is specified in the ?
 - A. Data Encryption Standard
 - B. Digital Signature Standard
 - C. Digital Encryption Standard
 - D. Advanced Encryption Standard
2. What does Secure Sockets Layer (SSL)/Transaction Security Layer (TSL) do? ?
 - A. Implements confidentiality, authentication, and integrity above the Transport Layer
 - B. Implements confidentiality, authentication, and integrity below the Transport Layer
 - C. Implements only confidentiality above the Transport Layer
 - D. Implements only confidentiality below the Transport Layer
3. What are MD4 and MD5? ?
 - A. Symmetric encryption algorithms
 - B. Asymmetric encryption algorithms
 - C. Hashing algorithms
 - D. Digital certificates
4. Elliptic curves, which are applied to public key cryptography, employ modular exponentiation that characterizes the ?
 - A. Elliptic curve discrete logarithm problem
 - B. Prime factors of very large numbers
 - C. Elliptic curve modular addition
 - D. Knapsack problem
5. Which algorithm is used in the Clipper Chip? ?
 - A. IDEA
 - B. DES
 - C. SKIPJACK
 - D. 3 DES
6. The hashing algorithm in the Digital Signature Standard (DSS) generates a message digest of ?

- A. 120 bits
B. 160 bits
C. 56 bits
D. 130 bit
7. The protocol of the Wireless Application Protocol (WAP), which performs functions similar to SSL in the TCP/IP protocol, is called the ?
- A. Wireless Application Environment (WAE)
B. Wireless Session Protocol (WSP)
C. Wireless Transaction Protocol (WTP)
D. Wireless Transport Layer Security Protocol (WTLS)
8. A Security Parameter Index (SPI) and the identity of the security protocol (AH or ESP) are the components of ?
- A. SSL
B. IPSec
C. S-HTTP
D. SSH-2
9. When two different keys encrypt a plaintext message into the same ciphertext, this situation is known as (a) ?
- A. Public key cryptography
B. Cryptanalysis
C. Key clustering
D. Hashing
10. What is the result of the Exclusive Or operation, 1XOR 0? ?
- A. 1
B. 0
C. Indeterminate
D. 10
11. A block cipher ?
- A. Encrypts by operating on a continuous data stream
B. Is an asymmetric key algorithm
C. Converts a variable-length of plaintext into a fixed length ciphertext
D. Breaks a message into fixed

- length units for encryption
12. In most security protocols that support authentication, integrity and confidentiality, ?
- A. Public key cryptography is used to create digital signatures.
 - B. Private key cryptography is used to create digital signatures.
 - C. DES is used to create digital signatures.
 - D. Digital signatures are not implemented.
13. Which of the following is an example of a symmetric key algorithm? ?
- A. Rijndael
 - B. RSA
 - C. Diffie-Hellman
 - D. Knapsack
14. Which of the following is a problem with symmetric key encryption? ?
- A. Is slower than asymmetric key encryption
 - B. Most algorithms are kept proprietary
 - C. Work factor is not a function of the key size
 - D. Secure distribution of the secret key
15. Which of the following is an example of an asymmetric key algorithm? ?
- A. IDEA
 - B. DES
 - C. 3 DES
 - D. ELLIPTIC CURVE
16. In public key cryptography ?
- A. Only the private key can encrypt and only the public key can decrypt
 - B. Only the public key can encrypt and only the private key can decrypt
 - C. The public key is used to encrypt and decrypt
 - D. If the public key encrypts, then only the private key can

- decrypt
17. In a hybrid cryptographic system, usually ?
- A. Public key cryptography is used for the encryption of the message.
 - B. Private key cryptography is used for the encryption of the message.
 - C. Neither public key nor private key cryptography is used.
 - D. Digital certificates cannot be used.
18. What is the block length of the Rijndael Cipher? ?
- A. 64 bits
 - B. 128 bits
 - C. Variable
 - D. 256 bits
19. A polyalphabetic cipher is also known as a ?
- A. One-time pad
 - B. Vigenère cipher
 - C. Steganography
 - D. Vernam cipher
20. The classic Caesar cipher is a ?
- A. Polyalphabetic cipher
 - B. Monoalphabetic cipher
 - C. Transposition cipher
 - D. Code group
21. In Steganography, ?
- A. Private key algorithms are used.
 - B. Public key algorithms are used.
 - C. Both public and private key algorithms are used.
 - D. The fact that the message exists is not known.
22. What is the key length of the Rijndael Block Cipher? ?
- A. 56 or 64 bits
 - B. 512 bits
 - C. 128, 192, or 256 bits
 - D. 512 or 1024 bits
23. In a block cipher, diffusion ?

- A. Conceals the connection between the ciphertext and plaintext
- B. Spreads the influence of a plaintext character over many ciphertext characters
- C. Is usually implemented by non-linear S-boxes
- D. Cannot be accomplished
24. The NIST Advanced Encryption Standard uses the ?
- A. 3 DES algorithm
- B. Rijndael algorithm
- C. DES algorithm
- D. IDEA algorithm
25. The modes of DES do NOT include ?
- A. Electronic Code Book
- B. Cipher Block Chaining
- C. Variable Block Feedback
- D. Output Feedback
26. Which of the following is true? ?
- A. The work factor of triple DES is the same as for double DES.
- B. The work factor of single DES is the same as for triple DES.
- C. The work factor of double DES is the same as for single DES.
- D. No successful attacks have been reported against double DES.
27. The Rijndael Cipher employs a round transformation that is comprised of three *layers* of distinct, invertible transformations. These transformations are also defined as uniform, which means that every bit of the State is treated the same. Which of the following is NOT one of these layers? ?
- A. The non-linear layer, which is the parallel application of S-boxes that have the optimum worst-case nonlinearity properties
- B. The linear mixing layer, which provides a guarantee of the high diffusion of multiple rounds

- C. The key addition layer, which is an Exclusive Or of the Round Key to the intermediate State
- D. The key inversion layer, which provides confusion through the multiple rounds
28. The Escrowed Encryption Standard describes the ?
- A. Rijndael Cipher
- B. Clipper Chip
- C. Fair Public Key Cryptosystem
- D. Digital certificates
29. Enigma was ?
- A. An English project created to break German ciphers
- B. The Japanese rotor machine used in WWII
- C. Probably the first programmable digital computer
- D. The German rotor machine used in WWII
30. Which of the following characteristics does a one-time pad have if used properly? ?
- A. It can be used more than once.
- B. The key does not have to be random.
- C. It is unbreakable.
- D. The key has to be of greater length than the message to be encrypted.
31. The DES key is ?
- A. 128 bits
- B. 64 bits
- C. 56 bits
- D. 512 bits
32. In a digitally-signed message transmission using a hash function ?
- A. The message digest is encrypted in the private key of the sender.
- B. The message digest is encrypted in the public key of the sender.
- C. The message is encrypted in

- the private key of the sender.
- D. The message is encrypted in the public key of the sender.
33. The strength of RSA public key encryption is based on the ?
- A. Difficulty in finding logarithms in a finite field
 - B. Difficulty of multiplying two large prime numbers
 - C. Fact that only one key is used
 - D. Difficulty in finding the prime factors of very large numbers
34. Elliptic curve cryptosystems ?
- A. Have a higher strength per bit than an RSA
 - B. Have a lower strength per bit than an RSA
 - C. Cannot be used to implement digital signatures
 - D. Cannot be used to implement encryption
35. Which of the following is NOT a key management issue? ?
- A. Key recovery
 - B. Key storage
 - C. Key change
 - D. Key exchange

Answers

1. *Answer:* b). Answer a) refers to DES; a symmetric encryption algorithm; answer c) is a distractor, there is no such term; answer d) is the Advanced Encryption Standard, which has replaced DES and is now the Rijndael algorithm.
2. *Answer:* a) by definition. Answer b) is incorrect since SSL/TLS operate above the Transport Layer; answer c is incorrect since authentication and integrity are provided also, and answer d) is incorrect since it cites only confidentiality and SSL/TLS operate above the Transport Layer.
3. *Answer:* c). Answers a) and b) are incorrect since they are general types of encryption systems and answer d) is incorrect since hashing algorithms are not digital certificates
4. *Answer:* a). Modular exponentiation in elliptic curves is the analog of the modular discrete logarithm problem. Answer b) is incorrect since prime factors are involved with RSA public key systems; answer c is incorrect since modular addition in elliptic curves is the analog of modular multiplication; and answer d is incorrect since the knapsack problem is not an elliptic curve problem.

5. *Answer: c).* Answers a), b) and d) are other symmetric key algorithms.
6. *Answer: b).*
7. *Answer: d).* SSL performs security functions in TCP/IP. The other answers refer to protocols in the WAP protocol stack, also, but their primary functions are not security.
8. *Answer: b).* The SPI, AH and/or ESP and the destination IP address are components of an IPSec Security Association (SA.) The other answers describe protocols other than IPSec.
9. *Answer: c).* Answer a) describes a type of cryptographic system using a public and a private key; answer b) is the art/science of breaking ciphers; answer d) is the conversion of a message of variable length into a fixed length message digest.
10. *Answer: a).* An XOR operation results in a 0 if the two input bits are identical and a 1 if one of the bits is a 1 and the other is a 0.
11. *Answer: d).* Answer a) describes a stream cipher; answer b) is incorrect since a block cipher applies to symmetric key algorithms; and answer c describes a hashing operation.
12. *Answer: a).* Answer b) is incorrect since private key cryptography does not create digital signatures; answer c) is incorrect since DES is a private key system and therefore, follows the same logic as in b; and answer d) is incorrect since digital signatures are implemented to obtain authentication and integrity.
13. *Answer: a).* The other answers are examples of asymmetric key systems.
14. *Answer: d).* Answer a) is incorrect since the opposite is true, answer b) is incorrect since most symmetric key algorithms are published, and answer c) is incorrect since work factor is a function of key size. The larger the key, the larger the work factor.
15. *Answer: d).* All the other answers refer to symmetric key algorithms.
16. *Answer: d).* Answers a) and b) are incorrect since, if one key encrypts, the other can decrypt and answer c) is incorrect since, if the public key encrypts, it cannot decrypt.
17. *Answer: b).* Answer a) is incorrect since public key cryptography is usually used for encryption and transmission of the secret session key. Answer c) is incorrect since both public and private key encryption are used and answer d) is incorrect since digital certificates can be used and normally, are used.
18. *Answer: c).* The other answers with fixed numbers are incorrect.
19. *Answer: b).* Answer a) is incorrect since a one-time pad uses a random key with length equal to the plaintext message and is used only once. Answer c) is the process of sending a message with no indication that a message even exists. Answer d) is incorrect since it applies to stream ciphers that are XOR'ed with a random key string.
20. *Answer: b).* It uses one alphabet shifted 3 places. Answers a)

and c) are incorrect since in a, multiple alphabets are used and in c, the letters of the message are transposed. Answer d) is incorrect since code groups deal with words and phrases and ciphers deal with bits or letters.

21. *Answer: d).* The other answers are incorrect since neither of the algorithms are used.
22. *Answer: c).*
23. *Answer: b).* Answer a) defines confusion; answer c) defines how confusion is accomplished; answer d is incorrect since it can be accomplished.
24. *Answer: b).* By definition, the others are incorrect.
25. *Answer: c).* There is no such encipherment mode.
26. *Answer: c).* The Meet-in-the-Middle attack has been successfully applied to double DES with the work factor is equivalent to that of single DES. Thus, answer d) is incorrect. Answer a) is false since the work factor of triple DES is greater than that for double DES. In triple DES, three levels of encryption and/or decryption are applied to the message. The work factor of double DES is equivalent to the work factor of single DES. Answer b) is false since the work factor of single DES is less than for triple DES. In triple DES, three levels of encryption and/or decryption are applied to the message in triple DES.
27. *Answer: d).* This answer is a distractor and does not exist.
28. *Answer: b).*
29. *Answer: d).* Answer a) describes the Ultra Project based in Bletchley Park, England, answer b) describes the Japanese Purple Machine, and answer c) refers to Colossus.
30. *Answer: c).* If the one-time-pad is used only once and its corresponding key is truly random and does not have repeating characters, it is unbreakable. Answer a) is incorrect since, if used properly, the one-time-pad should be used only once. Answer b) is incorrect since the key should be random. Answer d) is incorrect since the key has to be of the same length as the message.
31. *Answer: c).*
32. *Answer: a).* The hash function generates a message digest. The message digest is encrypted with the private key of the sender. Thus, if the message can be opened with the sender's public key that is known to all, the message must have come from the sender. The message is not encrypted with the public key since the message is usually longer than the message digest and would take more computing resources to encrypt and decrypt. Since the message digest uniquely characterizes the message, it can be used to verify the identity of the sender. Answers b) and d) will not work since a message encrypted in the public key of the sender can only be read using the private key of the sender. Since the sender is the only one who knows this key, no one else can read the message. Answer c) is incorrect since the message is not encrypted, but the message digest is encrypted
33. *Answer: d).* Answer a) applies to such public key algorithms as

Diffie-Hellman and Elliptic Curve. Answer b) is incorrect since it is easy to multiply two large prime numbers. Answer c) refers to symmetric key encryption.

- 34.** *Answer:* a). It is more difficult to compute elliptic curve discrete logarithms than conventional discrete logarithms or factoring. Smaller key sizes in the elliptic curve implementation can yield higher levels of security. Therefore, answer b) is incorrect. Answers c) and d) are incorrect since elliptic curve cryptosystems can be used for digital signatures and encryption.
- 35.** *Answer:* d). The other answers are key management issues, but key exchange is a function of the encryption system.

Chapter 5: Security Architecture and Models

Security Architecture

The security architecture of an information system is fundamental to enforcing the organization's information security policy. Therefore, it is important for security professionals to understand the underlying computer architectures, protection mechanisms, distributed environment security issues, and formal models that provide the framework for the security policy. In addition, professionals should have knowledge of the assurance evaluation, certification and accreditation guidelines, and standards. The following topics are addressed in this chapter:

- Computer organization
- Hardware components
- Software/firmware components
- Open systems
- Distributed systems
- Protection mechanisms
- Evaluation criteria
- Certification and accreditation
- Formal security models
- Confidentiality models
- Integrity models
- Information flow models

Computer Architecture

The term computer architecture refers to the organization of the fundamental elements comprising the computer. From another perspective, it refers to the view that a programmer has of the computing system when viewed through its instruction set. The main hardware components of a digital computer are the Central Processing Unit (CPU), memory, and input/output devices. A basic CPU of a general-purpose digital computer is comprised of an *Arithmetic Logic Unit (ALU)*, control logic, one or more accumulators, multiple general-purpose registers, an instruction register, a program counter, and some on-chip local memory. The ALU performs arithmetic and logical operations on the binary words of the computer.

These computer elements are interconnected by a group of conductors called a *bus*. The bus runs in a common plane with the different computer elements connected to the bus. A bus can be organized into subunits, such as the *address bus*, the *data bus*, and the *control bus*. A diagram of the organization of a bus is shown in Figure 5.1.

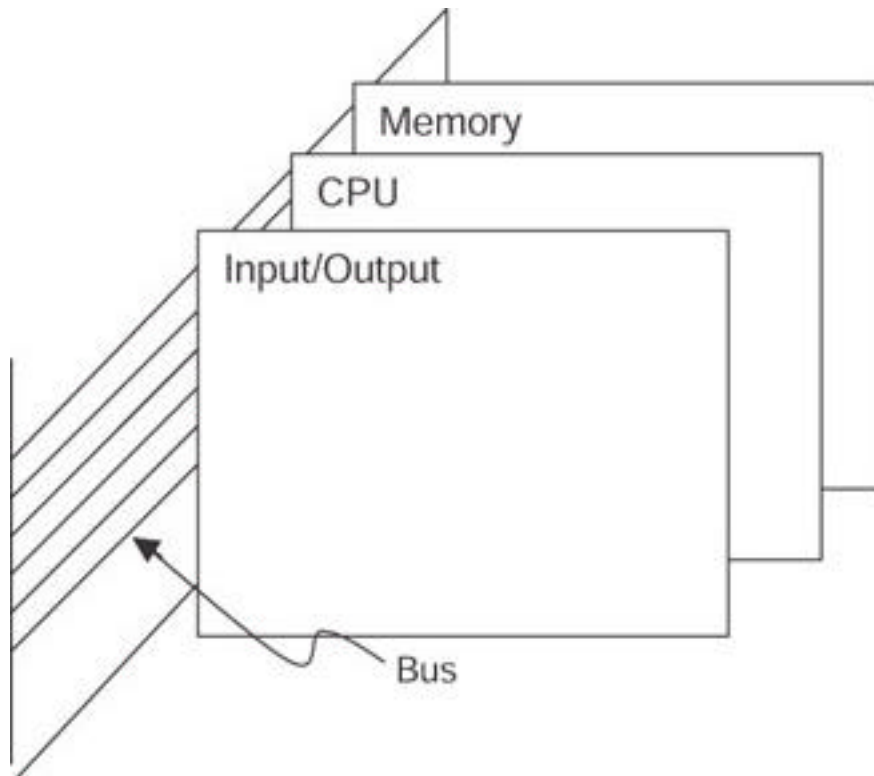


Figure 5.1: A computer bus.

Memory

Several types of memory are used in digital computer systems. The principal types of memory and their definitions are as follows:

Cache memory. A relatively small amount (when compared to primary memory) of very high speed RAM, which holds the instructions and data from primary memory that have a high probability of being accessed during the currently executing portion of a program. Cache logic attempts to predict which instructions and data in main memory will be used by a currently executing program. It then moves these items to the higher speed cache in anticipation of the CPU requiring these programs and data. Properly designed caches can significantly reduce the apparent main memory access time and thus, increase the speed of program execution.

Random Access Memory (RAM). Memory where locations can be directly addressed and the data that is stored can be altered. RAM is *volatile* due to the fact that the data is lost if power is removed from the system. *Dynamic RAM* (DRAM) stores the information on parasitic capacitance that decays over time. Therefore, the data on each RAM bit must be periodically refreshed. Refreshing is accomplished by reading and rewriting each bit every few milliseconds. Conversely, *static* RAM (SRAM) uses latches to store the bits and does not need to be refreshed. Both types of RAM, however, are volatile.

Programmable Logic Device (PLD). An integrated circuit with connections or internal logic gates that can be changed through a programming process. Examples of a PLD are a *Read Only Memory (ROM)*, a *Programmable Array Logic (PAL)* device, the *Complex Programmable Logic Device (CPLD)*, and the *Field Programmable Gate Array (FPGA)*. Programming of these devices is accomplished by blowing fuse connections on the chip, using an *antifuse* that makes a connection when a high voltage is applied to the junction, through mask programming when a chip is fabricated, and by using SRAM latches to turn an Metal Oxide Semiconductor (MOS) transistor on or off. This last technology is volatile because the power to the chip must be maintained for the chip to operate.

Read Only Memory (ROM). Non-volatile storage where locations can be directly addressed. In a basic ROM implementation, data cannot be altered dynamically. Non-

volatile storage retains its information even when it loses power. Some ROMs are implemented with one-way fusible links and their contents cannot be altered. Other types of ROMs — such as Erasable Programmable Read Only Memories (EPROMs), Electrically Alterable Read Only Memories (EAROMs), Electrically Erasable Programmable Read Only Memories (EEPROMs), Flash memories, and their derivatives — can be altered by various means, but only at a relatively slow rate when compared to normal computer system reads and writes. ROMs are used to hold programs and data that should normally not be changed or are changed infrequently. Programs stored on these types of devices are referred to as *firmware*.

Real or primary memory. The memory directly addressable by the CPU and used for the storage of instructions and data associated with the program that is being executed. This memory is usually high-speed, Random Access Memory (RAM).

Secondary memory. This type of memory is a slower memory (such as magnetic disks) that provides non-volatile storage.

Sequential memory. Memory from which information must be obtained by sequentially searching from the beginning rather than directly accessing the location. A good example of a sequential memory access is reading information from a magnetic tape.

Virtual memory. This type of memory uses secondary memory in conjunction with primary memory to present a CPU with a larger, apparent address space of the real memory locations.

A typical memory hierarchy is shown in Figure 5.2.

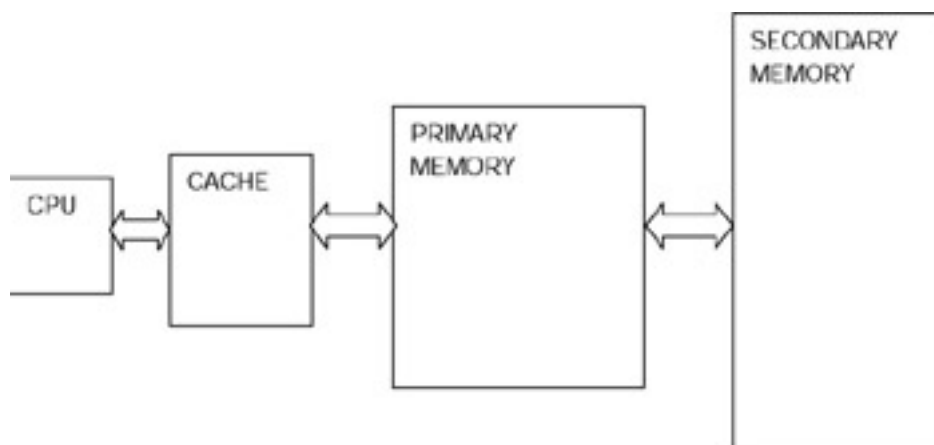


Figure 5.2: A computer memory hierarchy.

There are a number of ways that a CPU can address memory. These options provide flexibility and efficiency when programming different types of applications, such as searching through a table or processing a list of data items. The following are some of the commonly used addressing modes:

- *Register addressing.* Addressing the registers within a CPU or other special purpose registers that are designated in the primary memory.
- *Direct addressing.* Addressing a portion of primary memory by specifying the actual address of the memory location. The memory addresses are usually limited to the memory page that is being executed or page zero.
- *Absolute addressing.* Addressing all of the primary memory space.
- *Indexed addressing.* Developing a memory address by adding the contents of the address defined in the program's instruction to that of an *index register*. The computed, effective address is used to access the desired memory location. Thus, if an index register is incremented or decremented, a range of memory locations can be accessed.

- *Implied addressing.* Used when operations that are internal to the processor must be performed such as clearing a carry bit that was set as a result of an arithmetic operation. Because the operation is being performed on an internal register that is specified within the instruction itself, there is no need to provide an address.
- *Indirect addressing.* Addressing where the address location that is specified in the program instruction contains the address of the final desired location

An associated definition is the definition of memory protection.

Memory protection. Means to prevent one program from accessing and modifying the memory space contents that belong to another program. Memory protection is implemented by the operating system or by hardware mechanisms.

Instruction Execution Cycle

A basic machine cycle consists of two phases, fetch and execute. In the fetch phase, the CPU presents the address of the instruction to memory, and it retrieves the instruction located at that address. Then, during the execute phase, the instruction is decoded and executed. This cycle is controlled by and synchronized with the CPU clock signals. Because of the need to refresh dynamic RAM, multiple clock signals known as *multi-phase clock signals* are needed. Static RAM does not require refreshing and uses *single-phase clock signals*. In addition, some instructions may require more than one machine cycle to execute, depending on their complexity. A typical machine cycle showing a single-phase clock is shown in Figure 5.3. Note that in this example, four clock periods are required to execute a single instruction.

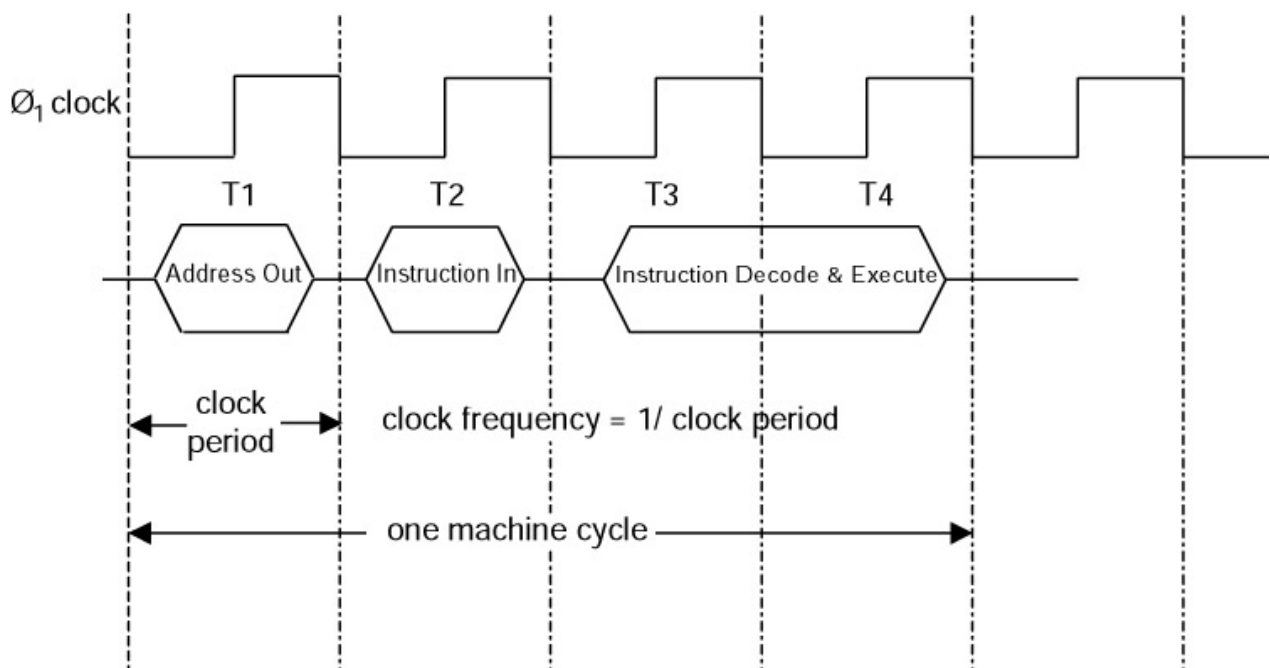


Figure 5.3: A typical machine cycle.

A computer can be in a number of different states during its operation. When a computer is executing instructions, this is sometimes called the *run* or *operating state*. When application programs are being executed, the machine is in the *application* or *problem* state because it is hopefully calculating the solution to a problem. For security purposes, users are permitted to access only a subset of the total instruction set that is available on the computer in this state. This subset is known as the *non-privileged* instructions. *Privileged* instructions are executed by the system administrator or an

individual who authorized to use those instructions. A computer is in a *supervisory* state when it is executing these privileged instructions. The computer can be in a *wait* state, for example, if it is accessing a slow memory relative to the instruction cycle time, which causes it to extend the cycle.

After examining a basic machine cycle, it is obvious that there are opportunities for enhancing the speed of retrieving and executing instructions. Some of these methods include overlapping the fetch and execute cycles, exploiting opportunities for parallelism, anticipating instructions that will be executed later, fetching and decoding instructions in advance, and so on. Modern computer design incorporates these methods and their key approaches are provided in the following definitions:

Pipelining. Increases the performance in a computer by overlapping the steps of different instructions. For example, if the instruction cycle is divided into three parts — fetch, decode, and execute — instructions can be overlapped as shown in Figure 5.4 to increase the execution speed of the instructions.

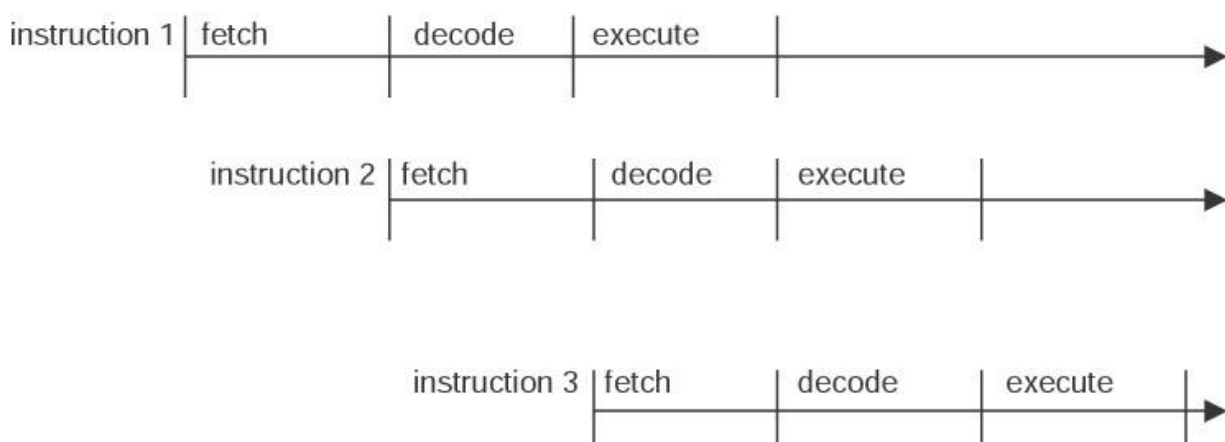


Figure 5.4: Instruction pipelining.

Complex-Instruction-Set-Computer (CISC). Uses instructions that perform many operations per instruction. This concept was based on that fact that in earlier technologies, the instruction fetch was the longest part of the cycle. Therefore, by packing the instructions with several operations, the number of fetches could be reduced.

Reduced-Instruction-Set-Computer (RISC). Uses instructions that are simpler and require fewer clock cycles to execute. This approach was a result of the increase in the speed of memories and other processor components, which enabled the fetch part of the instruction cycle to be no longer than any other portion of the cycle. In fact, performance was limited by the decoding and execution times of the instruction cycle.

Scalar Processor. A processor that executes one instruction at a time.

Superscalar Processor. A processor that enables concurrent execution of multiple instructions in the same pipeline stage as well as in different pipeline stages.

Very-Long Instruction-Word Processor (VLIW). A processor in which a single instruction specifies more than one concurrent operation. For example, the instruction may specify and concurrently execute two operations in one instruction. VLIW processing is illustrated in Figure 5.5.

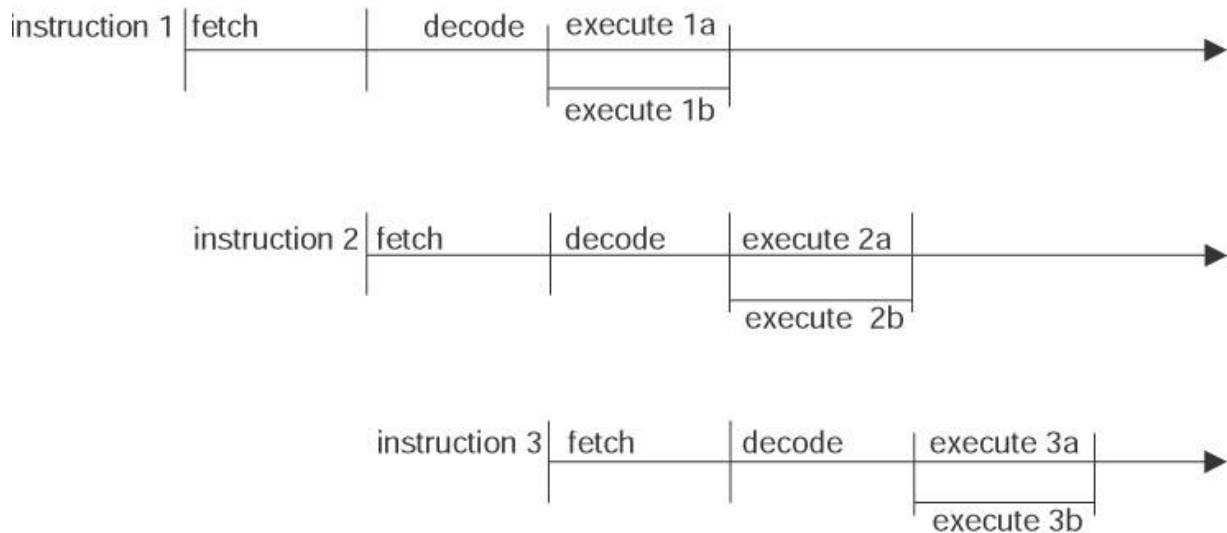


Figure 5.5: Very-Long Instruction Word (VLIW) processing.

Multiprogramming. Executes two or more programs simultaneously on a single processor (CPU) by alternating execution among the programs.

Multitasking. Executes two or more subprograms or tasks at the same time on a single processor (CPU) by alternating execution among the tasks.

Multiprocessing. Executes two or more programs at the same time on multiple processors.

Input/Output Structures

A processor communicates with outside devices through interface devices called input/output (I/O) *interface adapters*. In many cases, these adapters are complex devices that provide data buffering, and timing and interrupt controls. Adapters have addresses on the computer bus and are selected by the computer instructions. If an adapter is given an address in the memory space and, thus, takes up a specific memory address, this design is known as *memory-mapped I/O*. The advantage of this approach is that a CPU sees no difference in instructions for the I/O adapter and any other memory location. Therefore, all the computer instructions that are associated with memory can be used for the I/O device. On the other hand, in *isolated I/O*, a special signal on the bus indicates that an I/O operation is being executed. This signal distinguishes an address for an I/O device from an address to memory. The signal is generated as a result of the execution of a few, selected I/O instructions in the computer instruction's set. The advantage of an isolated I/O is that its addresses do not use up any addresses that could be used for memory. The disadvantage is that the I/O data accesses and manipulations are limited to a small number of specific I/O instructions in the processor's instruction set. Both memory-mapped and isolated I/Os are termed *programmed I/Os*.

In a programmed I/O, data transfers are a function of the speed of the instruction's execution, which manipulates the data that goes through a CPU. A faster alternative is *direct memory access (DMA)*. With DMA, data is transferred directly to and from memory without going through a CPU. DMA controllers accomplish this direct transfer in the time interval between the instruction executions. The data transfer rate in DMA is limited primarily by the memory cycle time. The path of the data transfer between memory and a peripheral device is sometimes referred to as a *channel*.

Another alternative to moving data into and out of a computer is through the use of *interrupts*. In *interrupt processing*, an external signal interrupts the normal program flow and requests service. The service may consist of reading data or responding to an emergency situation. Adapters provide the interface for handling the interrupts and the means for establishing priorities among multiple interrupt requests. When a CPU

receives an interrupt request, it will save the current state of the information related to the program that is currently running, and it will then jump to another program that services the interrupt. When the interrupt service is completed, the CPU restores the state of the original program and continues processing. Multiple interrupts can be handled concurrently by *nesting* the interrupt service routines. Interrupts can be turned off or *masked* if a CPU is executing a high priority code and does not want to be delayed in its processing.

Software

The CPU of a computer is designed to support the execution of a set of instructions associated with that computer. This set consists of a variety of instructions such as ADD WITH CARRY, ROTATE BITS LEFT, MOVE DATA, and JUMP TO LOCATION X. Each instruction is represented as a binary code that the instruction decoder of the CPU is designed to recognize and execute. These instructions are referred to as *machine language instructions*. The code of each machine language instruction is associated with an English-like mnemonic to make it easier for people to work with the codes. This set of mnemonics for the computer's basic instruction set is called its *assembly language*, which is specific to that particular computer. Thus, there is a one-to-one correspondence of each assembly language instruction to each machine language instruction. For example, in a simple 8bit instruction word computer, the binary code for the ADD WITH CARRY machine language instruction may be 10011101 and the corresponding mnemonic could be ADC. A programmer who is writing this code at the machine language level would write the code using mnemonics for each instruction. Then, the mnemonic code would be passed through another program called an *assembler* that would perform the one-to-one translation of the assembly language code to the machine language code. The code generated by the assembler running on the computer is called the *object code* and the original assembly code is called the *source code*. The assembler software can be resident on the computer being programmed and, thus is called a *resident assembler*. If the assembler is being run on another computer, the assembler is called a *cross assembler*. Cross assemblers can run on various types and models of computers. A *disassembler* reverses the function of an assembler by translating machine language into assembly language.

If a group of assembly language statements are used to perform a specific function, they can be defined to the assembler with a name called a *MACRO*. Then, instead of writing the list of statements, the MACRO can be called, causing the assembler to insert the appropriate statements.

Because it is desirable to write software in higher level, English-like statements, *high-level or high-order languages* are employed. In these languages, one statement usually requires a number of machine language instructions for its implementation. Therefore, unlike assembly language, there is a one-to-many relationship of high-level language instructions to machine language instructions. Pascal, FORTRAN, BASIC, and Java are examples of high-level languages. High-level languages are converted to the appropriate machine language instructions through either an *interpreter* or *compiler* programs. An interpreter operates on each high-level language source statement individually and performs the indicated operation by executing a predefined sequence of machine language instructions. Thus, the instructions are executed immediately. Java and BASIC are examples of interpreted languages. In contrast, a compiler translates the entire software program into its corresponding machine language instructions. These instructions are then loaded in the computer's memory and are executed as a program package. FORTRAN is an example of a compiled language. From a security standpoint, a compiled program is less desirable than an interpreted one because malicious code can be resident somewhere in the compiled code, and it is difficult to detect in a very large program.

High-level languages have been grouped into five generations, and they are labeled as a Generation Language (GL). The following is a list of these languages:

- 1 GL. A computer's machine language
- 2 GL. An assembly language
- 3 GL. FORTRAN, BASIC, PL/1, and C languages
- 4 GL. NATURAL, FOCUS, and database query languages
- 5 GL. Prolog, LISP, and other artificial intelligence languages that process symbols or implement predicate logic

The program or set of programs that control the resources and operations of the computer is/are called an *operating system (OS)*. Operating systems perform process management, memory management, system file management, and I/O management. Windows 2000, Linux, and Unix are some examples of these operating systems.

An OS communicates with I/O systems through a controller. A *controller* is a device, which serves as an interface to the peripheral, and runs specialized software to manage communications with another device. For example, a disk controller is used to manage the information exchange and operation of a disk drive.

Open and Closed Systems

Open systems are vendor-independent systems that have published specifications and interfaces in order to permit operations with the products of other suppliers. One advantage of an open system is that it is subject to review and evaluation by independent parties. Usually, this scrutiny will reveal any errors or vulnerabilities in that product.

A *closed system* uses vendor-dependent proprietary hardware and/or software that are usually not compatible with other systems or components. Closed systems are not subject to independent examination and may have vulnerabilities that are not known or recognized.

Distributed Architecture

The migration of computing from the centralized model to the client-server model has created a new set of issues for information system security professionals. In addition, this situation has also been compounded by the proliferation of desktop PCs and workstations. A PC on a user's desktop may contain documents, which are sensitive to the business of an organization, and that can be compromised. In most operations, a user also functions as the systems administrator, programmer, and operator of the desktop platform. The major concerns in this scenario are as follows:

- Desktop systems can contain sensitive information that may be at risk of being exposed.
- Users may generally lack security awareness.
- A desktop PC or workstation can provide an avenue of access into critical information systems of an organization.
- Modems that are attached to a desktop machine can make the corporate network vulnerable to dial-in attacks.
- Downloading data from the Internet increases the risk of infecting corporate systems with a malicious code or an unintentional modification of the databases.
- A desktop system and its associated disks may not be protected from physical intrusion or theft.
- A lack of proper backup may exist.

Security mechanisms can be put into place to counter these security vulnerabilities that can exist in a distributed environment. Such mechanisms are

- Email and download/upload policies

- Robust access control, which includes biometrics to restrict access to desktop systems
- Graphical user interface mechanisms to restrict access to critical information
- File encryption
- Separation of the processes that run in privileged or non-privileged processor states
- Protection domains
- Protection of the sensitive disks by locking them in non-movable containers and by physically securing the desktop system or laptop
- Distinct labeling of disks and materials according to their classification or an organization's sensitivity
- A centralized backup of desktop system files
- Regular security awareness training sessions
- Control of software installed on desktop systems
- Encryption and hash totals for use in sending and storing information
- Logging of transactions and transmissions
- Application of other appropriate physical, logical, and administrative access controls
- Database management systems restricting access to sensitive information
- Protection against environmental damage to computers and media
- Use of formal methods for software development and application, which includes libraries, change control, and configuration management
- Inclusion of desktop systems in disaster recovery and business continuity plans

Protection Mechanisms

In a computational system, multiple processes may be running concurrently. Each process has the ability to access certain memory locations and to execute a subset of the computer's instruction set. The execution and memory space assigned to each process is called a *protection domain*. This domain can be extended to virtual memory, which increases the apparent size of real memory by using disk storage. The purpose of establishing a protection domain is to protect programs from all unauthorized modification or executional interference.

Security professionals should also know that a *Trusted Computing Base (TCB)* is the total combination of protection mechanisms within a computer system, which includes the hardware, software, and firmware, that are trusted to enforce a security policy. The *security perimeter* is the boundary that separates the TCB from the remainder of the system. A *trusted path* must also exist so that a user can access the TCB without being compromised by other processes or users. A *trusted computer system* is one that employs the necessary hardware and software assurance measures to enable its use in processing multiple levels of classified or sensitive information. This system meets the specified requirements for reliability and security.

Resources can also be protected through the principle of *abstraction*. Abstraction involves viewing system components at a high level and ignoring or segregating its specific details. This approach enhances the system's ability to understand complex systems and to focus on critical, high-level issues. In object-oriented programming, for example, methods (programs) and data are *encapsulated* in an object that can be viewed as an abstraction. This concept is called *information hiding* because the object's functioning details are hidden. Communication with this object takes place through messages to which the object responds as defined by its internal method.

Rings

One scheme that supports multiple protection domains is the use of *protection rings*. These rings are organized with the most privileged domain located in the center of the ring and the least privileged domain in the outermost ring. This approach is shown in Figure 5.6.

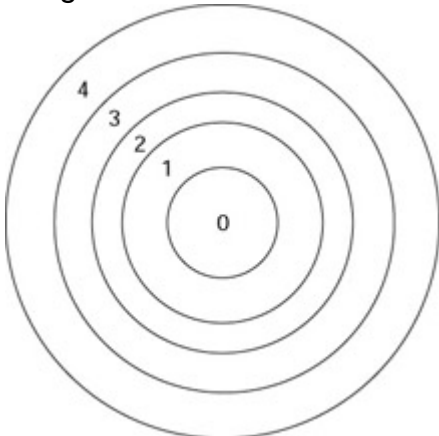


Figure 5.6: Protection rings.

The operating system security kernel is usually located at Ring 0 and has access rights to all domains in that system. A *security kernel* is defined as the hardware, firmware, and software elements of a trusted computing base that implement the reference monitor concept. A *reference monitor* is a system component that enforces access controls on an object. Therefore, the *reference monitor concept* is an abstract machine that mediates all access of subjects to objects. The security kernel must

- Mediate all accesses
- Be protected from modification
- Be verified as correct

In the ring concept, access rights decrease as the ring number increases. Thus, the most trusted processes reside in the center rings. System components are placed in the appropriate ring according to the principle of least privilege. Therefore, the processes only have the minimum privileges necessary to perform their functions.

The ring protection mechanism was implemented in MIT's MULTICS time-shared operating system that was enhanced for secure applications by the Honeywell Corporation. MULTICS was initially targeted for use on specific hardware platforms because some of its functions could be implemented through the hardware's customization. It was designed to support 64 rings, but, in practice, only eight rings were defined.

There are also other related kernel-based approaches to protection:

- Using a separate hardware device that validates all references in a system.
- Implementing a *virtual machine* monitor, which establishes a number of virtual machines isolated from each other that are running on the actual computer. The virtual machines mimic the architecture of a real machine, in addition to establishing a multilevel security environment — each virtual machine can run at a different security level.
- Using a software security kernel that operates in its own hardware protection domain.

Security Labels

A security label is assigned to a resource to denote a type of classification or designation. This label can then indicate special security handling, or it can be used for access control. Once labels are assigned they usually cannot be altered and are an effective access control mechanism. Because labels must be compared and evaluated in accordance with the security policy, they incur additional processing overhead when used.

Security Modes

An information system operates in different security modes that are determined by an information's classification level and the clearance of the users. A major distinction in its operation is between the system high mode and the multilevel security mode. In the *system high mode of operation*, a system operates at the highest level of information classification where all users must have clearances for the highest level. However, not all users may have a need to know for all the data. The *multilevel mode of operation* supports users with different clearances and data at multiple classification levels. Additional modes of operation are defined as follows:

Dedicated. All users have a clearance or an authorization and a need-to-know for all information that is processed by an information system; a system may handle multiple classification levels.

Compartmented. All users have a clearance for the highest level of information classification, but they do not necessarily have the authorization and a need-to-know for all the data handled by the computer system.

Controlled. It is a type of multilevel security where a limited amount of trust is placed in the system's hardware/software base along with the corresponding restrictions on the classification of the information levels that can be processed.

Limited access. It is a type of system access where the minimum user clearance is not cleared and the maximum data classification is unclassified but sensitive.

Additional Security Considerations

Vulnerabilities in the system security architecture can lead to violations of the system's security policy. Typical vulnerabilities that are architecturally-related vulnerabilities include the following:

Covert channel. An unintended communication path between two or more subjects sharing a common resource, which supports the transfer of information in a such a manner that violates the system's security policy. The transfer usually takes place through common storage areas or through access to a common path that can use a timing channel for the unintended communication.

Lack of parameter checking. The failure to check the size of input streams specified by parameters. Buffer overflow attacks exploit this vulnerability in certain operating systems and programs.

Maintenance hook. A hardware or software mechanism that was installed to permit system maintenance and to bypass the system's security protections. This vulnerability is sometimes referred to as a *trapdoor*.

Time of Check to Time of Use (TOC/TOU) attack. An attack that exploits the difference in the time that security controls were applied and the time the authorized service was used.

Recovery Procedures

Whenever a hardware or software component of a trusted system fails, it is important that the failure does not compromise the security policy requirements of that system. In addition, the recovery procedures should not also provide an opportunity for violation of

the system's security policy. If a system restart is required, the system must restart in a secure state. Start up should occur in the *maintenance mode* that permits access only by privileged users from privileged terminals. This mode supports the restoring the system state and the security state.

When a computer or network component fails and the computer or the network continues to function, it is called a *fault-tolerant* system. For fault-tolerance to operate, the system must be capable of detecting that a fault has occurred, and the system must then have the ability to correct the fault or operate around it. In a *fail safe* system, program execution is terminated, and the system is protected from being compromised when a hardware or software failure occurs and is detected. In a system that is *fail soft* or *resilient*, selected, non-critical processing is terminated when a hardware or software failure occurs and is detected. The computer or network then continues to function in a degraded mode. The term *failover* refers to switching to a duplicate "hot" backup component in real-time when a hardware or software failure occurs, which enables the system to continue processing.

A *cold start* occurs in a system when there is a TCB or media failure and the recovery procedures cannot return the system to a known, reliable, secure state. In this case, the TCB and portions of the software and data may be inconsistent and require external intervention. At that time, the maintenance mode of the system usually has to be employed.

Assurance

Assurance is simply defined as the degree of confidence in satisfaction of security needs. The following sections summarize guidelines and standards that have been developed to evaluate and accept the assurance aspects of a system.

Evaluation Criteria

In 1985, the Trusted Computer System Evaluation Criteria (TCSEC) was developed by the National Computer Security Center (NCSC) to provide guidelines for evaluating vendors' products for the specified security criteria. TCSEC provides the following:

- A basis for establishing security requirements in the acquisition specifications
- A standard of the security services that should be provided by vendors for the different classes of security requirements
- A means to measure the trustworthiness of an information system

The TCSEC document, called the Orange Book because of its color, is part of a series of guidelines with covers of different coloring called the Rainbow Series. The Rainbow Series is covered in detail in Appendix B. In the Orange book, the basic control objectives are security policy, assurance, and accountability. TCSEC addresses confidentiality, but does not cover integrity. Also, functionality (security controls applied) and assurance (confidence that security controls are functioning as expected) are not separated in TCSEC as they are in other evaluation criteria developed later. The Orange Book defines the major hierarchical classes of security by the letters D through A as follows:

- D. Minimal protection
- C. Discretionary protection (C1 and C2)
- B. Mandatory protection (B1, B2, and B3)
- A. Verified protection; formal methods (A1)

The DoD Trusted Network Interpretation (TNI) is analogous to the Orange Book. It addresses confidentiality and integrity in trusted computer/communications network

systems and is called the Red Book. The Trusted Data Base Management System Interpretation (TDI) addresses the trusted database management systems.

The European Information Technology Security Evaluation Criteria (ITSEC), address confidentiality, integrity, and availability. The product or system to be evaluated by ITSEC is defined as the *Target of Evaluation (TOE)*. The TOE must have a security target, which includes the security enforcing mechanisms and the system's security policy.

ITSEC separately evaluates functionality and assurance, and it includes ten functionality classes (F), eight assurance levels (Q), seven levels of correctness (E), and eight basic security functions in its criteria. It also defines two kinds of assurance. One assurance measure is of the correctness of the security functions' implementation, and the other is the effectiveness of the TOE while in operation.

The ITSEC ratings are in the form F-X,E where functionality and assurance are listed. The ITSEC ratings that are equivalent to TCSEC ratings are

F-C1, E1 = C1

F-C2, E2 = C2

F-B1, E3 = B1

F-B2, E4 = B2

F-B3, E5 = B3

F-B3, E6 = A1

The other classes of the ITSEC address high integrity and high availability.

TCSEC, ITSEC, and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) have evolved into one evaluation criteria, called the Common Criteria. The Common Criteria defines a *Protection Profile* that specifies the security requirements and protections of a product that is to be evaluated. The functional requirements of the Common Criteria are organized around TCB entities. These entities include physical and logical controls, start-up and recovery, reference mediation, and privileged states. The Common Criteria are discussed in Appendix G. As with TCSEC and ITSEC, the ratings of the Common Criteria are also hierarchical.

Certification and Accreditation

In many environments, formal methods must be applied to ensure that the appropriate information system security safeguards are in place and that they are functioning per the specifications. In addition, an authority must take responsibility for putting the system into operation. These actions are known as certification and accreditation.

Formally, the definitions are as follows:

Certification. The comprehensive evaluation of the technical and non-technical security features of an information system and the other safeguards, which are created in support of the accreditation process, to establish the extent in which a particular design and implementation meets the set of specified security requirements.

Accreditation. A formal declaration by a Designated Approving Authority (DAA) where an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

The certification and accreditation of a system must be checked after a defined period of time or when changes occur in the system and/or its environment. Then, recertification and re-accreditation are required.

DITSCAP and NIACAP

Two U.S. defense and government certification and accreditation standards have been developed for the evaluation of critical information systems. These standards are the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and the National Information Assurance Certification and Accreditation Process (NIACAP.)

DITSCAP

DITSCAP establishes a standard process, a set of activities, general task descriptions, and a management structure to certify and accredit the IT systems that will maintain the required security posture. This process is designed to certify that the IT system meets the accreditation requirements and that the system will maintain the accredited security posture throughout its life cycle. These are the four phases to the DITSCAP:

Phase 1, Definition. Phase 1 focuses on understanding the mission, the environment, and the architecture in order to determine the security requirements and level of effort necessary to achieve accreditation.

Phase 2, Verification. Phase 2 verifies the evolving or modified system's compliance with the information agreed on in the *System Security Authorization Agreement* (SSAA.) The objective is to use the SSAA to establish an evolving, yet binding agreement on the level of security required before system development begins or changes to a system are made. After accreditation, the SSAA becomes the baseline security configuration document.

Phase 3, Validation. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

Phase 4, Post Accreditation. Phase 4 includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment, and for addressing the changing threats a system faces through its life cycle.

NIACAP

The NIACAP establishes the minimum national standards for certifying and accrediting national security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that maintain the information assurance and the security posture of a system or site. The NIACAP is designed to certify that the information system meets the documented accreditation requirements and will continue to maintain the accredited security posture throughout the system's life cycle.

There are three types of NIACAP accreditation:

- *A site accreditation.* Evaluates the applications and systems at a specific, self-contained location
- *A type accreditation.* Evaluates an application or system that is distributed to a number of different locations
- *A system accreditation.* Evaluates a major application or general support system

The NIACAP is composed of four phases — Definition, Verification, Validation, and Post Accreditation — that are essentially identical to those of the DITSCAP.

Currently, the Commercial Information Security Analysis Process (CIAP) is being developed for the evaluation of critical commercial systems using the NIACAP methodology.

Information Security Models

Models are used in information security to formalize security policies. These models may be abstract or intuitive and will provide a framework for the understanding of fundamental concepts. In this section, three types of models are described — access control models, integrity models, and information flow models.

Access Control Models

Access control philosophies can be organized into models that define the major and different approaches to this issue. These models are the access matrix, the Take-Grant model, the Bell-LaPadula confidentiality model, and the state machine model.

The Access Matrix

The access matrix is a straightforward approach that provides access rights to subjects for objects. Access *rights* are of the type read, write, and execute. A *subject* is an active entity that is seeking rights to a resource or object. A subject can be a person, a program, or a process. An *object* is a passive entity such as a file or a storage resource. In some cases, an item can be a subject in one context and an object in another. A typical access control matrix is shown in Figure 5.7.

Subject Object	File Income	File Salaries	Process Deductions	Print Server A
Joe	Read	Read/Write	Execute	Write
Jane	Read/Write	Read	None	Write
Process Check	Read	Read	Execute	None
Program Tax	Read/Write	Read/Write	Call	Write

Figure 5.7: Example of an access matrix.

The columns of the access matrix are called *Access Control Lists (ACLs)* and the rows are called *capability lists*. The access matrix model supports discretionary access control because the entries in the matrix are at the discretion of the individual(s) who have the authorization authority over the table. In the access control matrix, a subject’s capability can be defined by the triple (object, rights, random #.) Thus, the triple defines the rights a subject has to an object along with a random number used to prevent a replay or spoofing of the triple’s source. This triple is similar to the Kerberos tickets previously discussed in Chapter 2, “Access Control Systems.”

Take-Grant Model

The Take-Grant model uses a directed graph to specify the rights that a subject can transfer to an object, or that a subject can take from another subject. For example, assume that Subject A has a set of rights (S) that includes Grant rights to Object B. This capability is represented in Figure 5.8a. Then, assume that Subject A can transfer Grant rights for Object B to Subject C, and that Subject A has another set of rights (Y), to Object D. In some cases, Object D acts as an object and, in other cases, it acts as a subject. Then, as shown by the heavy arrow in Figure 5.8b, Subject C can grant a subset of the Y rights to Subject/Object D because Subject A passed the Grant rights to Subject C.

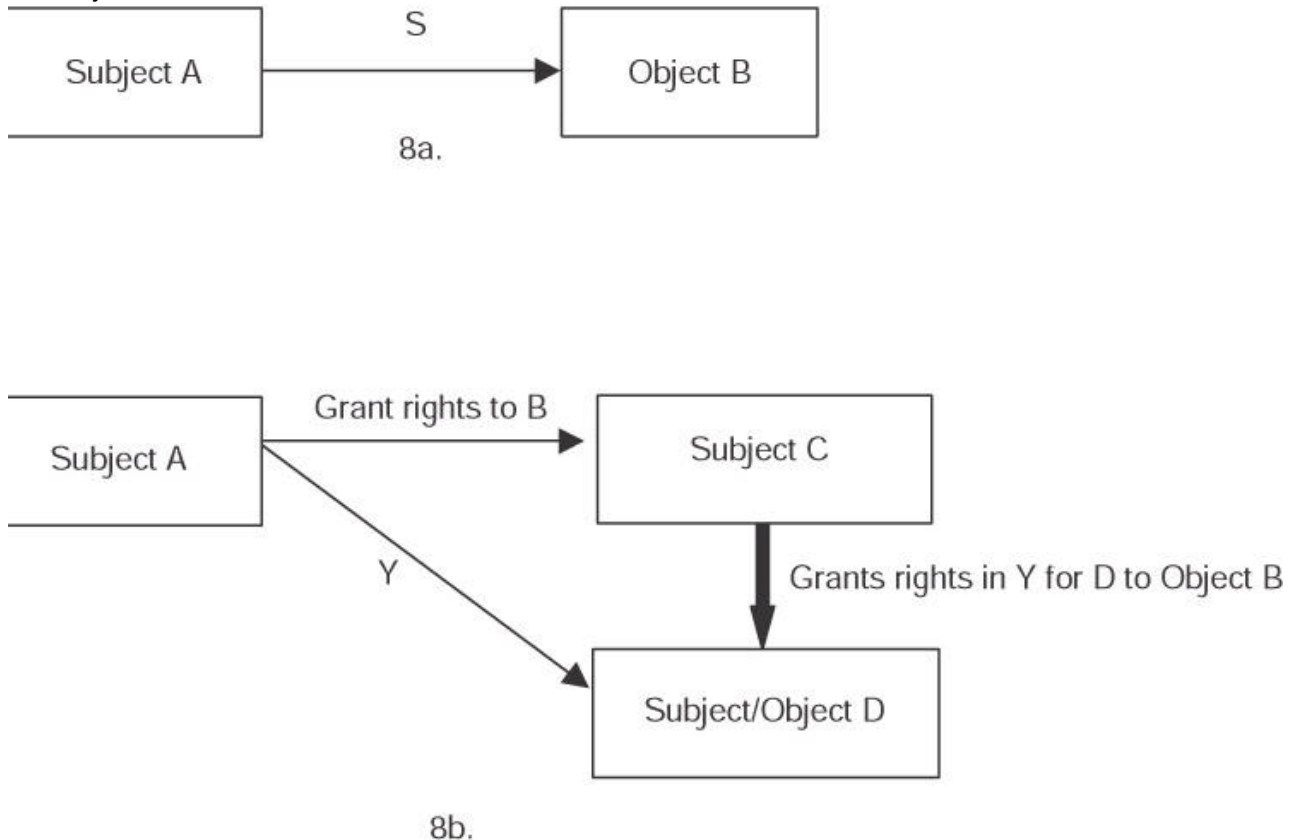


Figure 5.8: Take-Grant model illustration.

The Take capability operates in an identical fashion as the Grant illustration.

Bell-LaPadula Model

The Bell-LaPadula Model was developed to formalize the U.S. Department of Defense (DoD) multilevel security policy. The DoD labels materials at different levels of security classification. As previously discussed, these levels are Unclassified, Confidential, Secret, and Top Secret — from least sensitive to most sensitive. An individual who receives a clearance of Confidential, Secret, or Top Secret can access materials at that level of classification or below. An additional stipulation, however, is that the individual must have a *need-to-know* for that material. Thus, an individual cleared for Secret can only access the Secret-labeled documents that are necessary for that individual to perform an assigned job function. *The Bell-LaPadula model deals only with the confidentiality of classified material.* It does not address integrity or availability.

The Bell-LaPadula model is built on the state machine concept. This concept defines a set of allowable states (A_i), in a system. The transition from one state to another upon receipt of an input(s) (X_j) is defined by transition functions (f_k). The objective of this model is to ensure that the initial state is secure and that the transitions always result in a secure state. The transitions between two states are illustrated in Figure 5.9.

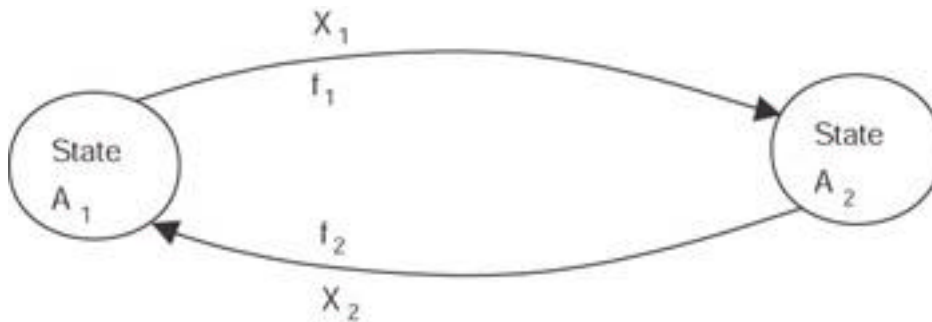


Figure 5.9: State transitions defined by the function f with an input X .

The Bell-LaPadula model defines a secure state through three multilevel properties. The first two properties implement mandatory access control, and the third one permits discretionary access control. These properties are defined as follows:

1. *The Simple Security Property (ss Property)*. States that reading of information by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up).
2. *The * (star) Security Property*. States that writing of information by a subject at a higher level of sensitivity to an object at a lower level of sensitivity is not permitted (no write down).
3. *The Discretionary Security Property*. Uses an access matrix to specify discretionary access control.

There are instances where the * (Star) property is too restrictive, and it interferes with required document changes. For instance, it may be desirable to move a low sensitivity paragraph in a higher sensitivity document to a lower sensitivity document. This transfer of information is permitted by the Bell-LaPadula model through a *Trusted Subject*. A Trusted Subject can violate the * property, yet it cannot violate its intent. These concepts are illustrated in Figure 5.10.

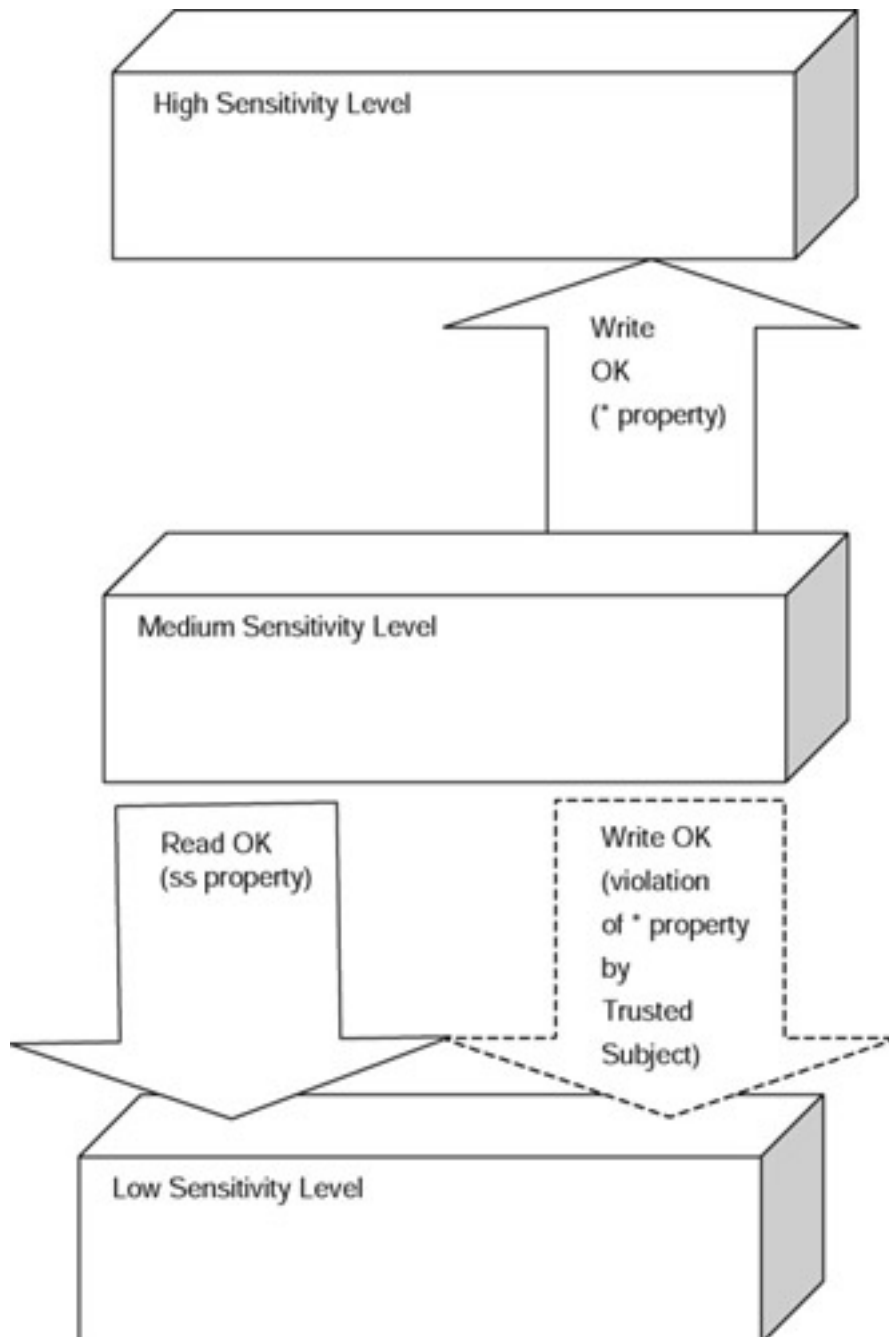


Figure 5.10: The Bell-LaPadula Simple Security and * properties.

In some instances, a property called the *Strong * Property* is cited. This property states that reading or writing is permitted at a particular level of sensitivity, but not to either higher or lower levels of sensitivity.

This model defines requests (R) to the system. A request is made while the system is in the state v_1 ; a decision (d) is made upon the request, and the system changes to the state v_2 . (R, d, v_1 , v_2) represents this tuple in the model. Again, the intent of this model is to ensure that there is a transition from one secure state to another secure state.

The discretionary portion of the Bell-LaPadula model is based on the access matrix. The system security policy defines who is authorized to have certain privileges to the system resources. *Authorization* is concerned with how access rights are defined and how they are evaluated. Some discretionary approaches are based on context-dependent and content-dependent access control. *Content-dependent* control makes access decisions based on the data contained in the object, whereas, *context-*

dependent control uses subject or object attributes or environmental characteristics to make these decisions. Examples of such characteristics include a job role, earlier accesses, and file creation dates and times.

As with any model, the Bell-LaPadula model has some weaknesses. These are the major ones:

- The model considers normal channels of the information exchange and does not address covert channels.
- The model does not deal with modern systems that use file sharing and servers.
- The model does not explicitly define what it means by a secure state transition.
- The model is based on multilevel security policy and does not address other policy types that may be used by an organization.

Integrity Models

In many organizations, both governmental and commercial, integrity of the data is as important or more important than confidentiality for certain applications. Thus, formal integrity models evolved. Initially, the integrity model was developed as an analog to the Bell-LaPadula confidentiality model and then became more sophisticated to address additional integrity requirements.

The Biba Integrity Model

Integrity is usually characterized by the three following goals:

1. The data is protected from modification by unauthorized users.
2. The data is protected from unauthorized modification by authorized users.
3. The data is internally and externally consistent — the data held in a database must balance internally and must correspond to the external, real-world situation.

To address the first integrity goal, the Biba model was developed in 1977 as an integrity analog to the Bell-LaPadula confidentiality model. The Biba model is lattice-based and uses the less than or equal to relation. A lattice structure is defined as a partially ordered set with a least upper bound (LUB) and a greatest lower bound (GLB.) The lattice represents a set of integrity classes (ICs) and an ordered relationship among those classes. A lattice can be represented as (IC, #, LUB, GUB.)

Similar to the Bell-LaPadula model's classification of different sensitivity levels, the Biba model classifies objects into different levels of integrity. The model specifies the three following integrity axioms:

1. *The Simple Integrity Axiom.* States that a subject at one level of integrity is not permitted to observe (read) an object of a lower integrity (no read down).
2. *The * (star) Integrity Axiom.* States that an object at one level of integrity is not permitted to modify (write to) an object of a higher level of integrity (no write up).
3. A subject at one level of integrity cannot invoke a subject at a higher level of integrity.

These axioms and their relationships are illustrated in Figure 5.11.

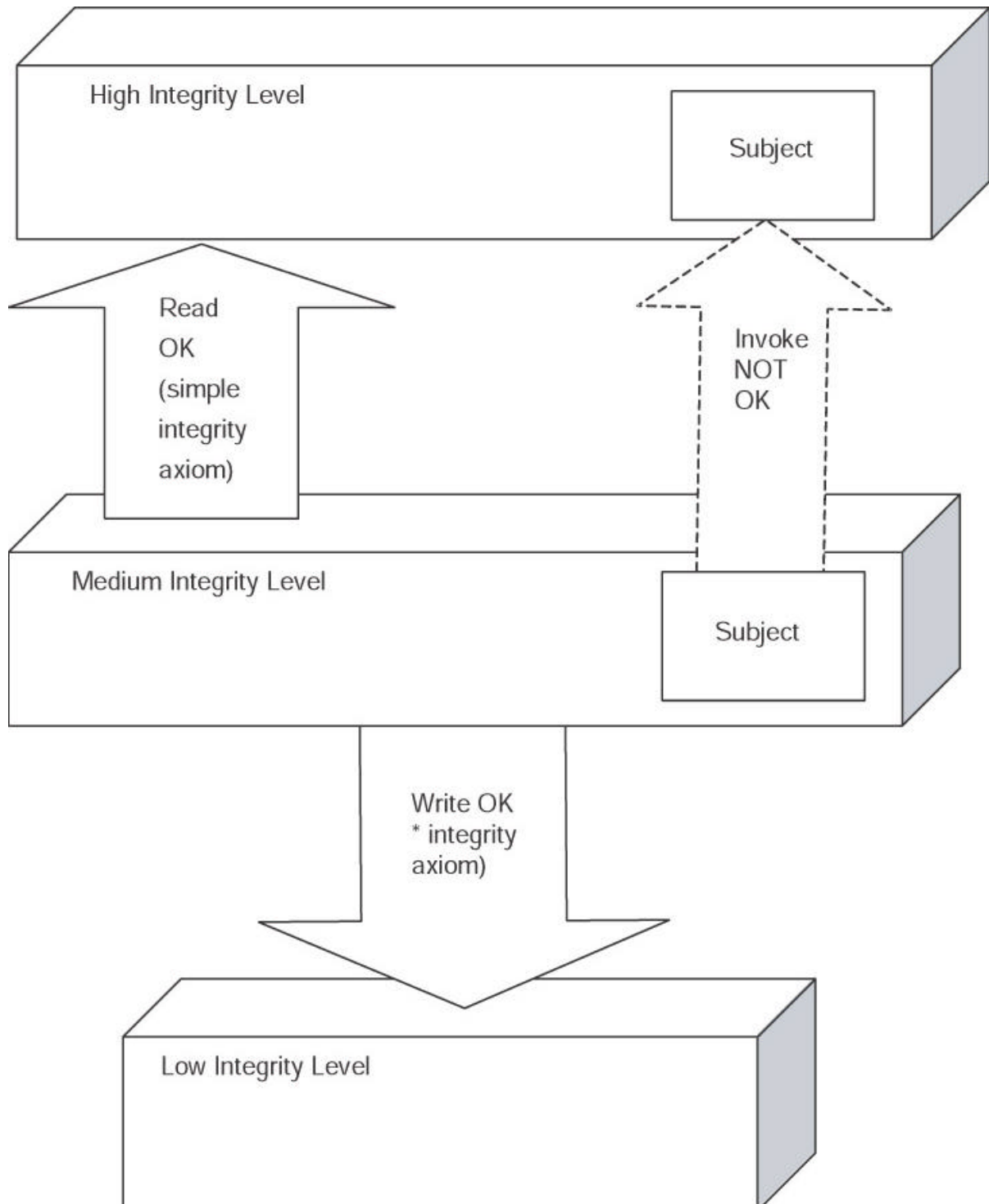


Figure 5.11: The Biba model axioms.

The Clark-Wilson Integrity Model

The approach of the Clark-Wilson model (1987) was to develop a framework for use in the real-world, commercial environment. This model addresses the three integrity goals and defines the following terms:

Constrained data item (CDI). A data item whose integrity is to be preserved

Integrity verification procedure (IVP). Confirms that all CDIs are in valid states of integrity

Transformation procedure (TP). Manipulates the CDIs through a well-formed transaction, which transforms a CDI from one valid integrity state to another valid integrity state

Unconstrained data item. Data items outside of the control area of the modeled environment such as input information

The Clark-Wilson model requires integrity labels to determine the integrity level of a data item and to verify that this integrity was maintained after an application of a TP. This model incorporates mechanisms to enforce internal and external consistency, a separation of duty, and a mandatory integrity policy.

Information Flow Models

An information flow model is based on a state machine, and it consists of objects, state transitions, and lattice (flow policy) states. In this context, objects can also represent users. Each object is assigned a security class and value, and information is constrained to flow in the directions that are permitted by the security policy. An example is shown in Figure 5.12.

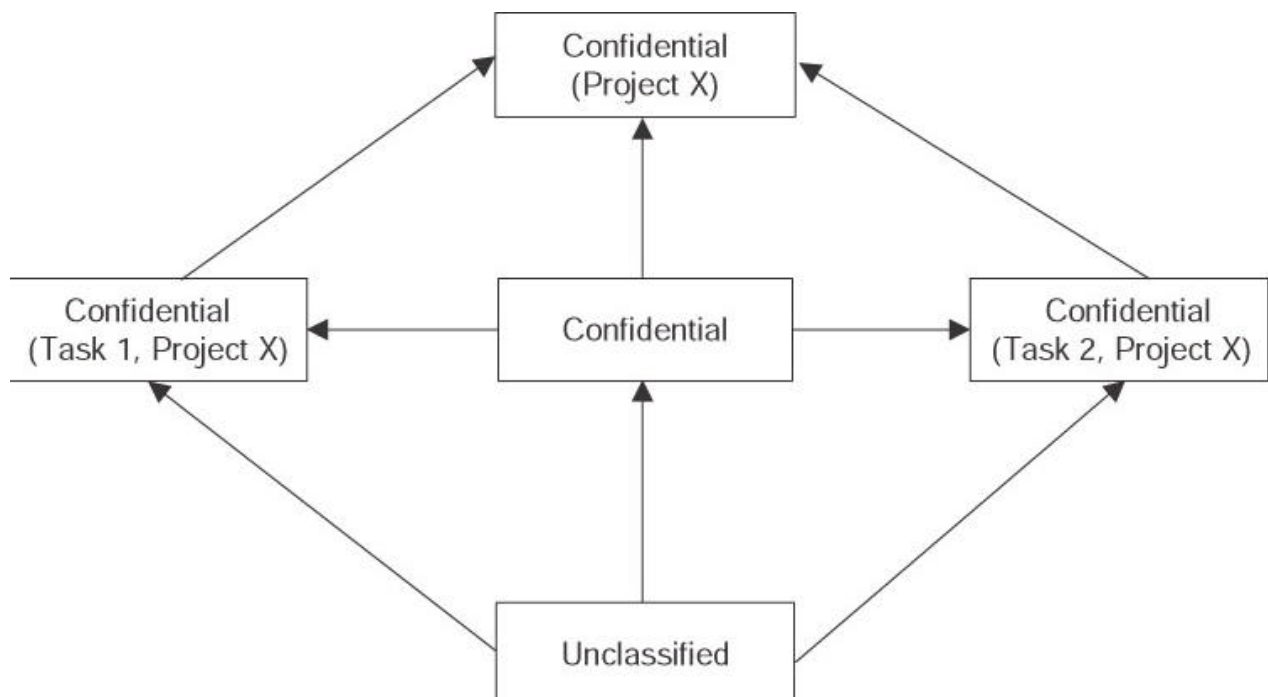


Figure 5.12: An Information Flow Model.

In Figure 5.12, information flows from Unclassified to Confidential in Tasks in Project X and to the combined tasks in Project X. This information can flow in only one direction.

Non-interference Model

This model is related to the information flow model with restrictions on the information flow. The basic principle of this model is that a group of users (A), who are using the commands (C), do not interfere with the user group (B), who are using commands (D). This concept is written as $A, C \mid B, D$. Restating this rule, the actions of Group A who are using commands C are not seen by users in Group B using commands D.

Composition Theories

In most applications, systems are built by combining smaller systems. An interesting situation to consider is whether the security properties of component systems are maintained when they are combined to form a larger entity.

John McClean studied this issue in 1994 (McLean, J. "A General Theory of Composition for Trace Sets Closed Under Selective Interleaving Functions," Proceedings of 1994 IEEE Symposium on Research in Security and Privacy, IEEE Press, 1994.)

He defined two compositional constructions — external and internal. The following are the types of external constructs:

Cascading. One system's input is obtained from the output of another system

Feedback. One system provides the input to a second system, which, in turn, feeds back to the input of the first system

Hookup. A system that communicates with another system as well as with external entities

The internal composition constructs are intersection, union, and difference.

The general conclusion of this study was that the security properties of the small systems were maintained under composition (in most instances) in the cascading construct, yet are also subject to other system variables for the other constructs.

Sample Questions

1. What does the Bell-LaPadula model NOT allow? ?
 - A. Subjects to read from a higher level of security relative to their level of security
 - B. Subjects to read from a lower level of security relative to their level of security
 - C. Subjects to write to a higher level of security relative to their level of security
 - D. Subjects to read at their same level of security

2. In the * (star) property of the Bell-LaPadula model, ?
 - A. Subjects cannot read from a higher level of security relative to their level of security
 - B. Subjects cannot read from a lower level of security relative to their level of security
 - C. Subjects cannot write to a lower level of security relative to their level of security
 - D. Subjects cannot read from their same level of security

3. The Clark-Wilson model focuses on data's ?
 - A. Integrity
 - B. Confidentiality
 - C. Availability
 - D. Format

4. The * (star) property of the Biba model states: ?
 - A. Subjects cannot write to a lower level of integrity relative to their level of integrity
 - B. Subjects cannot write to a higher level of integrity relative to their level of integrity
 - C. Subjects cannot read from a lower level of integrity relative to their level of integrity
 - D. Subjects cannot read from a higher level of integrity relative to their level of integrity

5. Which of the following does the Clark-Wilson model NOT involve? ?

- A. Constrained data items
 - B. Transformational procedures
 - C. Confidentiality items
 - D. Well-formed transactions
6. The Take-Grant model ?
- A. Focuses on confidentiality
 - B. Specifies the rights a subject can transfer to an object
 - C. Specifies the levels of integrity
 - D. Specifies the levels of availability
7. The Biba model addresses ?
- A. Data disclosure
 - B. Transformation procedures
 - C. Constrained data items
 - D. Unauthorized modification of data
8. Mandatory access controls first appear in the Trusted Computer System Evaluation Criteria (TCSEC) at the rating of ?
- A. D
 - B. C
 - C. B
 - D. A
9. In the access control matrix, the rows are ?
- A. Access Control Lists (ACLs)
 - B. Tuples
 - C. Domains
 - D. Capability lists
10. Superscalar computer architecture is characterized by a ?
- A. Computer using instructions that perform many operations per instruction
 - B. Computer using instructions that are simpler and require less clock cycles to execute
 - C. Processor that executes one instruction at a time
 - D. Processor that enables concurrent execution of multiple instructions in the same pipeline stage
11. A Trusted Computing Base (TCB) is defined as ?

- A. The total combination of protection mechanisms within a computer system that are trusted to enforce a security policy
 - B. The boundary separating the trusted mechanisms from the remainder of the system
 - C. A trusted path that permits a user to access resources
 - D. A system that employs the necessary hardware and software assurance measures to enable processing multiple levels of classified or sensitive information to occur
12. Memory space insulated from other running processes in a multiprocessing system is part of a ?
- A. Protection domain
 - B. Security perimeter
 - C. Least upper bound
 - D. Constrained data item
13. The boundary separating the TCB from the remainder of the system is called the ?
- A. Star property
 - B. Simple security property
 - C. Discretionary control boundary
 - D. Security Perimeter
14. The system component that enforces access controls on an object is the ?
- A. Security perimeter
 - B. Trusted domain
 - C. Reference monitor
 - D. Access control matrix
15. In the discretionary portion of the Bell-LaPadula mode that is based on the access matrix, how the access rights are defined and evaluated is called ?
- A. Authentication
 - B. Authorization
 - C. Identification
 - D. Validation
16. A computer system that employs the necessary hardware and software assurance measures to enable it to process multiple ?

levels of classified or sensitive information is called a

- A. Closed system
- B. Open system
- C. Trusted system
- D. Safe system

17. For fault-tolerance to operate, a system must be

?

- A. Capable of detecting and correcting the fault
- B. Capable of only detecting the fault
- C. Capable of terminating operations in a safe mode
- D. Capable of a cold start

18. Which of the following composes the four phases of the National Information Assurance Certification and Accreditation Process (NIACAP)?

?

- A. Definition, Verification, Validation, and Confirmation
- B. Definition, Verification, Validation, and Post Accreditation
- C. Verification, Validation, Authentication, and Post Accreditation
- D. Definition, Authentication, Verification, and Post Accreditation

19. What is a programmable logic device (PLD)?

?

- A. A volatile device
- B. Random Access Memory (RAM) that contains the software to perform specific tasks
- C. An integrated circuit with connections or internal logic gates that can be changed through a programming process
- D. A program resident on disk memory that executes a specific function

20. The termination of selected, non-critical processing when a hardware or software failure occurs and is detected is referred to as

?

- A. Fail safe
 - B. Fault tolerant
 - C. Fail soft
 - D. An Exception
21. Which of the following are the three types of NIACAP accreditation? ?
- A. Site, type, and location
 - B. Site, type, and system
 - C. Type, system, and location
 - D. Site, type, and general
22. Content-dependent control makes access decisions based on ?
- A. The object's data
 - B. The object's environment
 - C. The object's owner
 - D. The object's view
23. The term failover refers to ?
- A. Switching to a duplicate "hot" backup component
 - B. Terminating processing in a controlled fashion
 - C. Resiliency
 - D. A fail soft system
24. Primary storage is the ?
- A. Memory directly addressable by the CPU, which is for storage of instructions and data that are associated with the program being executed
 - B. Memory such as magnetic disks that provide non-volatile storage
 - C. Memory used in conjunction with real memory to present a CPU with a larger, apparent address space
 - D. Memory where information must be obtained by sequentially searching from the beginning of the memory space
25. In the Common Criteria, a Protection Profile ?
- A. Specifies the mandatory protection in the product to be evaluated

- B. Is also known as the Target of Evaluation (TOE)
- C. Is also known as the Orange Book
- D. Specifies the security requirements and protections of the products to be evaluated
26. Context-dependent control uses which of the following to make decisions? ?
- A. Subject or object attributes, or environmental characteristics
- B. Data
- C. Formal models
- D. Operating system characteristics
27. What is a computer bus? ?
- A. A message sent around a token ring network
- B. Secondary storage
- C. A group of conductors for the addressing of data and control
- D. A message in object-oriented programming
28. In a ring protection system, where is the security kernel usually located ? ?
- A. Highest ring number
- B. Arbitrarily placed
- C. Lowest ring number
- D. Middle ring number
29. Increasing performance in a computer by overlapping the steps of different instructions is called? ?
- A. A reduced instruction set computer
- B. A complex instruction set computer
- C. Vector processing
- D. Pipelining
30. Random access memory is ?
- A. Non-volatile
- B. Sequentially addressable
- C. Programmed by using fusible links
- D. Volatile

31. The addressing mode in which an instruction accesses a memory location whose contents are the address of the desired data is called ?
- A. Implied addressing
 - B. Indexed addressing
 - C. Direct addressing
 - D. Indirect addressing
32. Processes are placed in a ring structure according to ?
- A. Least privilege
 - B. Separation of duty
 - C. Owner classification
 - D. First in, first out
33. The MULTICS operating system is a classic example of ?
- A. An open system
 - B. Object orientation
 - C. Data base security
 - D. Ring protection system
34. What are the hardware, firmware, and software elements of a Trusted Computing Base (TCB) that implement the reference monitor concept called? ?
- A. The trusted path
 - B. A security kernel
 - C. An Operating System (OS)
 - D. A trusted computing system

Answers

1. *Answer: a).* The other options are not prohibited by the model.
2. *Answer: c).* By definition of the star property.
3. *Answer: a).* The Clark-Wilson model is an integrity model.
4. *Answer: b).*
5. *Answer: c.* Answers a, b, and d are parts of the Clark-Wilson model
6. *Answer: b).*
7. *Answer: d).* The Biba model is an integrity model. Answer a) is associated with confidentiality. Answers b) and c) are specific to the Clark-Wilson model.
8. *Answer: c).*
9. *Answer: d).* Answer a) is incorrect because the access control list is not a row in the access control matrix. Answer b) is incorrect since a tuple is a row in the table of a relational database. Answer c) is incorrect since a domain is the set of allowable values a column or attribute can take in a relational database.

10. *Answer: d).* Answer a) is the definition of a complex instruction set computer. Answer b) is the definition of a reduced instruction set computer. Answer c) is the definition of a scalar processor.
11. *Answer: a).* Answer b is the security perimeter. Answer c is the definition of a trusted path. Answer d is the definition of a trusted computer system.
12. *Answer: a).*
13. *Answer: d).* Answers a) and b) deal with security models and answer c) is a distractor.
14. *Answer: c).*
15. *Answer: b).* Since authorization is concerned with how access rights are defined and how they are evaluated.
16. *Answer: c).* By definition of a trusted system. Answers a) and b) refer to open, standard information on a product as opposed to a closed or proprietary product. Answer d) is a distractor.
17. *Answer: a).* The two conditions required for a fault-tolerant system. Answer b) is a distractor. Answer c) is the definition of fail safe and answer d) refers to starting after a system shutdown.
18. *Answer: b).*
19. *Answer: c).* Answer a) is incorrect since a PLD is non-volatile. Answer b) is incorrect since random access memory is volatile memory that is not a non-volatile logic device. Answer c) is a distractor.
20. *Answer: c).*
21. *Answer: b).*
22. *Answer: a).* Answer b) is context-dependent control. Answers c) and d) are distractors.
23. *Answer: a).* Failover means switching to a hot backup system that maintains duplicate states with the primary system. Answer b) refers to fail safe and answers c) and d) refer to fail soft.
24. *Answer: a).* Answer b) refers to secondary storage. Answer c) refers to virtual memory answer d) refers to sequential memory.
25. *Answer: d).* Answer a) is a distractor. Answer b) is the product to be evaluated. Answer c) refers to TCSEC.
26. *Answer: a).* Answer b) refers to content-dependent and answers c) and d) are distractors.
27. *Answer: c).* Answer a) is a token. Answer b) refers to disk storage. Answer d) is a distractor.
28. *Answer: c).*
29. *Answer: d).*
30. *Answer: d).* RAM is volatile. The other answers are incorrect since RAM is volatile, random accessible and not programmed by fusible links.
31. *Answer: d).*
32. *Answer: a).* A process is placed in the ring that gives it the minimum privileges necessary to perform its functions.
33. *Answer: d).* Multics is based on the ring protection architecture.

34.

Answer: b).

Chapter 6: Operations Security

Overview

The Operations Security Domain of Information Systems Security contains many elements that are important for a CISSP candidate to remember. In this domain, we will describe the controls that a computing operating environment needs to ensure the three pillars of information security: Confidentiality, Integrity, and Availability. Examples of these elements of control are controlling the separation of job functions, controlling the hardware and media that are used, and controlling the exploitation of common I/O errors.

This domain somewhat overlaps the Physical Security domain. In fact, there has been discussion as to whether the Physical domain should be removed altogether and merged with the Operations domain. We will point out the areas that overlap in this chapter.

Operations Security can be described as the controls over the hardware in a computing facility, the data media used in a facility, and the operators using these resources in a facility.

From the published (ISC)² goals for the Certified Information Systems Security Professional candidate:

A CISSP candidate will be expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms that are available, the potential for access abuse, the appropriate controls, and the principles of good practice.

Our Goals

We will approach this material from the three following directions:

1. *Controls and Protections.* We will describe the categories of operational controls needed to ensure C.I.A.
2. *Monitoring and Auditing.* We will describe the need for monitoring and auditing these controls.
3. *Threats and Vulnerabilities.* We will discuss threats and violations that are applicable to the Operations domain.

Domain Definition

Operations Security refers to the act of understanding the threats to and vulnerabilities of computer operations in order to routinely support operational activities that enable computer systems to function correctly. It also refers to the implementation of security controls for normal transaction processing, system administration tasks, and critical external support operations. These controls can include resolving software or hardware problems along with the proper maintenance of auditing and monitoring processes.

Triples

Like the other domains, the Operations Security domain is concerned with triples — threats, vulnerabilities, and assets. We will now look at what constitutes a triple in the Operations Security domain:

- *Threat.* A *threat* in the Operations Security domain can be defined as an event that could cause harm by violating the security. An example of an

operations threat would be an operator's abuse of privileges, thereby violating confidentiality.

- *Vulnerability.* A *vulnerability* is defined as a weakness in a system that enables security to be violated. An example of an operations vulnerability would be a weak implementation of the separation of duties.
- *Asset.* An *asset* is considered anything that is a computing resource or ability, such as hardware, software, data, and personnel.

C.I.A.

The following are the effects of operations controls on C.I.A:

- *Confidentiality.* Operations controls affect the sensitivity and secrecy of the information.
- *Integrity.* How well the operations controls are implemented directly affects the data's accuracy and authenticity.
- *Availability.* Like the Physical Security domain, these controls affect the organization's level of fault tolerance and its ability to recover from failure.

Controls and Protections

The Operations Security domain is concerned with the controls that are used to protect hardware, software, and media resources from the following:

- Threats in an operating environment
- Internal or external intruders
- Operators who are inappropriately accessing resources

A CISSP candidate should know the resources to protect, how privileges should be restricted, and the controls to implement.

In addition, we will also discuss the following two critical aspects of operations controls:

1. Resource protection, which includes hardware control.
2. Privileged-entity control.

Categories of Controls

The following are the major categories of operations security controls:

- *Preventative Controls.* In the Operations Security domain, preventative controls are designed to achieve two things — to lower the amount and impact of unintentional errors that are entering the system, and to prevent unauthorized intruders from internally or externally accessing the system. An example of these controls might be pre-numbered forms, or a data validation and review procedure to prevent duplications.
- *Detective Controls.* Detective controls are used to detect an error once it has occurred. Unlike preventative controls, these controls operate after the fact and can be used to track an unauthorized transaction for prosecution, or to lessen an error's impact on the system by identifying it quickly. An example of this type of control is an audit trail.
- *Corrective (or Recovery) Controls.* Corrective controls are implemented to help mitigate the impact of a loss event through data recovery procedures. They can be used to recover after damage, such as restoring data that was inadvertently erased from floppy diskettes.

The following are additional control categories:

- *Deterrent Controls.* Deterrent controls are used to encourage compliance with external controls, such as regulatory compliance. These controls are

meant to complement other controls, such as preventative and detective controls. Deterrent controls are also known as *directive* controls.

- *Application Controls.* Application controls are the controls that are designed into a software application to minimize and detect the software's operational irregularities. In addition, the following controls are also examples of the various types of application controls.
- *Transaction Controls.* Transaction controls are used to provide control over the various stages of a transaction — from initiation, to output, through testing and change control. There are several types of transaction controls:
 - *Input Controls.* Input controls are used to ensure that transactions are properly input into the system only once. Elements of input controls may include counting the data and timestamping it with the date it was entered or edited.
 - *Processing Controls.* Processing controls are used to guarantee that transactions are valid and accurate and that wrong entries are reprocessed correctly and promptly.
 - *Output Controls.* Output controls are used for two things — for protecting the confidentiality of an output, and for verifying the integrity of an output by comparing the input transaction with the output data. Elements of proper output controls would involve ensuring the output reaches the proper users, restricting access to the printed output storage areas, printing heading and trailing banners, requiring signed receipts before releasing sensitive output, and printing “no output” banners when a report is empty.
 - *Change Controls.* Change controls are implemented to preserve data integrity in a system while changes are made to the configuration. Procedures and standards have been created to manage these changes and modifications to the system and its configuration. Change control and configuration management control is thoroughly described later in this chapter.
 - *Test Controls.* Test controls are put into place during the testing of a system to prevent violations of confidentiality and to ensure a transaction's integrity. An example of this type of control is the proper use of sanitized test data. Test controls are often part of the change control process.

Orange Book Controls

The Trusted Computer Security Evaluation Criteria (TCSEC, the Orange Book) defines several levels of assurance requirements for secure computer operations. Assurance is a level of confidence that ensures a TCB's security policy has been correctly implemented and that the system's security features have accurately implemented that policy.

The Orange Book defines two types of assurance — *operational assurance* and *life cycle assurance*. Operational assurance focuses on the basic features and architecture of a system, while life cycle assurance focuses on the controls and standards that are necessary for building and maintaining a system. An example of an operational

assurance would be a feature that separates a security-sensitive code from a user code in a system's memory.

The operational assurance requirements specified in the Orange Book (found in Appendix B) are as follows:

- System architecture
- System integrity
- Covert channel analysis
- Trusted facility management
- Trusted recovery

Life cycle assurance ensures that a TCB is designed, developed, and maintained with formally controlled standards that enforces protection at each stage in the system's life cycle. *Configuration management*, which carefully monitors and protects all changes to a system's resources, is a type of life cycle assurance.

The life cycle assurance requirements specified in the Orange Book are as follows:

- Security testing
- Design specification and testing
- Configuration management
- Trusted distribution

In the Operations Security domain, the operations assurance areas of covert channel analysis, trusted facility management and trusted recovery, and the life cycle assurance area of configuration management are covered.

Covert Channel Analysis

A *covert channel* is an information path that is not normally used for communication within a system, therefore it is not protected by the system's normal security mechanisms. Covert channels are a secret way to convey information to another person or program.

There are two types of covert channels — *covert storage channels* and *covert timing channels*. Covert storage channels convey information by changing a system's stored data. For example, a program can convey information to a less secure program by changing the amount or the patterns of free space on a hard disk. Changing the characteristics of a file is also another example of creating a covert channel.

Covert timing channels convey information by altering the performance of or modifying the timing of a system resource in some measurable way. Timing channels often work by taking advantage of some kind of system clock or timing device in a system. Information is conveyed by using elements such as the elapsed time required to perform an operation, the amount of CPU time expended, or the time occurring between two events.

Noise and traffic generation are effective ways to combat the use of covert channels. Table 6.1 describes the primary covert channel classes.

Class	Description
B2	The system must protect against covert storage channels. It must perform covert channel analysis for all covert storage channels.
B3 and A1	The system must protect against both covert storage and covert timing channels. It must perform a covert channel analysis for both types.

Trusted Facility Management

Trusted facility management is defined as the assignment of a specific individual to administer the security-related functions of a system. Although trusted facility management is an assurance requirement only for highly secure systems (B2, B3, and A1), many systems evaluated at lower security levels are structured to try to meet this requirement (see Table 6.2).

Class	Requirements
B2	Systems must support separate operator and system administrator roles.
B3 and A1	Systems must clearly identify the functions of the security administrator to perform the security-related functions.

Trusted facility management is closely related to the concept of *least privilege*, and it is also related to the administrative concept of *separation of duties* and *need to know*.

Separation of Duties

Separation of duties (also called *segregation of duties*) assigns parts of tasks to different personnel. Thus, if no single person has total control of the system's security mechanisms, the theory is that no single person can completely compromise the system. This concept is related to the principle of *least privilege*. In this context, least privilege means that a system's users should have the lowest level of rights and privileges necessary to perform their work, and should only have them for the shortest length of time.

In many systems, a system administrator has total control of the system's administration and security functions. This consolidation of power is not allowed in a secure system because security tasks and functions should not automatically be assigned to the role of the system administrator. In highly secure systems, three distinct administrative roles may be required — a system administrator, a security administrator who is usually an Information System Security Officer (ISSO), and an enhanced operator function.

The security administrator, system administrator, and operator may not necessarily be different personnel, which is often the case. However, whenever a system administrator assumes the role of the security administrator, this role change must be controlled and audited. Because the security administrator's job is to perform security functions, the performance of non-security tasks must be strictly limited. This separation of duties reduces the likelihood of loss that results from users abusing their authority by taking actions outside of their assigned functional responsibilities. While it may be cumbersome for the person to switch from one role to another, the roles are functionally different and must be executed as such.

In the concept of *two-man control*, two operators review and approve the work of each other. The purpose of two-man control is to provide accountability and to minimize fraud in highly sensitive or high-risk transactions. The concept of *dual control* means that both operators are needed to complete a sensitive task.

Typical system administrator or enhanced operator functions may include the following:

- Installing system software

- Starting up (booting) and shutting down a system
- Adding and removing system users
- Performing backups and recovery
- Handling printers and managing print queues

Typical security administrator functions may include the following:

- Setting user clearances, initial passwords, and other security characteristics for new users
- Changing security profiles for existing users
- Setting or changing file sensitivity labels
- Setting the security characteristics of devices and communications channels
- Reviewing audit data

An operator may perform some system administrator roles, such as backups. This may happen in facilities where personnel resources are constrained.

The System Administrator's Many Hats

It's not just small organizations anymore that require a system administrator to function as a security administrator. The LAN/Internet Network administrator role creates security risks due to the inherent lack of the separation of duties. With the current pull-back in the Internet economy, a network administrator has to wear many hats and performing security-related tasks is almost always one of them (along with various operator functions). The sometimes cumbersome, yet very important, concept of separation of duties is vital to preserve operations controls.

Rotation of Duties

Another variation on separation of duties is called *rotation of duties*. It is defined as the process of limiting the amount of time an operator is assigned to perform a security-related task before being moved to a different task with a different security classification. This control lessens the opportunity for collusion between operators for fraudulent purposes. Like separation of duties, rotation of duties may be difficult to implement in small organizations, but can be an effective security control procedure.

Trusted Recovery

Trusted recovery ensures that security is not breached when a system crash or other system failure (sometimes called a "discontinuity") occurs. It must ensure that the system is restarted without compromising its required protection scheme, and that it can recover and rollback without being compromised after the failure. Trusted recovery is required only for B3 and A1 level systems. A system failure represents a serious security risk because the security controls may be bypassed when the system is not functioning normally.

For example, if a system crashes while sensitive data is being written to a disk (where it would normally be protected by controls), the data may be left unprotected in memory and may be accessible by unauthorized personnel.

Trusted recovery has two primary activities — preparing for a system failure and recovering the system.

Failure Preparation

Under trusted recovery, preparing for a system failure consists of backing up all critical files on a regular basis. This preparation must enable the data recovery in a protected

and orderly manner while ensuring the continued security of the system. These procedures may also be required if a system problem, such as a missing resource, an inconsistent database, or any kind of compromise, is detected, or the system needs to be halted and rebooted.

System Recovery

While specific trusted recovery procedures depend upon a system's requirements, general secure system recovery procedures include the following:

- Rebooting the system into a *single user mode* — an operating system loaded without the security front end activated — so no other user access is enabled at this time
- Recovering all file systems that were active at the time of the system failure
- Restoring any missing or damaged files and databases from the most recent backups
- Recovering the required security characteristics, such as file security labels
- Checking security-critical files, such as the system password file

After all of these steps have been performed, and the system's data cannot be compromised, operators may then access the system.

In addition, the Common Criteria also describes three hierarchical recovery types:

1. *Manual Recovery*. System administrator intervention is required to return the system to a secure state after a crash.
2. *Automated Recovery*. Recovery to a secure state is automatic (without system administrator intervention) when resolving a single failure; however, manual intervention is required to resolve any additional failures.
3. *Automated Recovery without Undue Loss*. Similar to automated recovery, this type of recovery is considered a higher level of recovery defining prevention against the undue loss of protected objects.

Configuration/Change Management Control

Configuration management is the process of tracking and approving changes to a system. It involves identifying, controlling, and auditing all changes made to the system. It can address hardware and software changes, networking changes, or any other change affecting security. Configuration management can also be used to protect a trusted system while it is being designed and developed.

The primary security goal of configuration management is to ensure that changes to the system do not unintentionally diminish security. For example, configuration management may prevent an older version of a system from being activated as the production system. Configuration management also makes it possible to accurately roll back to a previous version of a system, in case a new system is found to be faulty. Another goal of configuration management is to ensure that system changes are reflected in current documentation to help mitigate the impact that a change may have on the security of other systems, while either in the production or planning stages.

Although configuration management is a requirement only for B2, B3, and A1 systems, it is recommended for systems that are evaluated at lower levels. Most developers use some type of configuration management because it is common sense.

The following are the primary functions of configuration or change control:

- To ensure that the change is implemented in a orderly manner through formalized testing
- To ensure that the user base is informed of the impending change
- To analyze the effect of the change on the system after implementation
- To reduce the negative impact the change may have had on the computing services and resources

Five generally accepted procedures exist to implement and support the change control process:

1. Applying to introduce a change.
2. Cataloging the intended change.
3. Scheduling the change.
4. Implementing the change.
5. Reporting the change to the appropriate parties.

Table 6.3 shows the two primary configuration management classes.

Class	Requirement
B2 and B3	Configuration management procedures must be enforced during development and maintenance of a system.
A1	Configuration management procedures must be enforced during the entire system's life cycle.

Administrative Controls

Administrative controls can be defined as the controls that are installed and maintained by administrative management to help reduce the threat or impact of violations on computer security. We separate them from the operations controls because these controls have more to do with human resources personnel administration and policy than they do with hardware or software controls.

The following are some examples of administrative controls:

- *Personnel Security*. These controls are administrative human resources controls that are used to support the guarantees on the quality levels of the personnel performing the computer operations. These are also explained in the Physical Security domain. Elements of these include the following:
 - *Employment Screening or Background Checks*. Pre-employment screening for sensitive positions should be implemented. For less sensitive positions, post-employment background checks may be suitable.
 - *Mandatory Taking of Vacation in One Week Increments*. This practice is common in financial institutions or other organizations where an operator has access to sensitive financial transactions. Some

institutions require a two week vacation, during which the operator's accounts, processes, and procedures are audited carefully to uncover any evidence of fraud.

- *Job Action Warnings or Termination.* These are the actions taken when employees violate the published computer behavior standards.
- *Separation of Duties and Responsibilities.* Separation (or Segregation) of Duties and Responsibilities is the concept of assigning parts of security-sensitive tasks to several individuals. This was described earlier in this chapter.
- *Least Privilege.* Least privilege requires that each subject be granted the most restricted set of privileges needed for the performance of their task. This concept is described later in more detail.
- *Need to Know.* Need to know refers to the access to, knowledge of, or possession of specific information that is required to carry out a job function. It requires that the subject is given only the amount of information required to perform an assigned task. This concept is also described later in more detail.
- *Change/Configuration Management Controls.* The function of Change Control or Configuration Control is to protect a system from problems and errors that may result from improperly executed or tested changes to a system. This concept was described earlier in this chapter.
- *Record Retention and Documentation.* The administration of security controls on documentation and the procedures implemented for record retention have an impact on operational security. These are described later in more detail.

Least Privilege

It may be necessary to separate the levels of access based on the operator's job function. A very effective approach is *least privilege*. An example of least privilege is the concept of computer operators who are not allowed access to computer resources at a level beyond what is absolutely needed for their specific job tasks. Operators are organized into privilege-level groups. Each group is then assigned the most restrictive level that is applicable.

The three basic levels of privilege are defined as follows:

Read Only. This is the lowest level of privilege and the one to which most operators should be assigned. Operators are allowed to view data, but are not allowed to add, delete, or make changes to the original or copies of the data.

Read/Write. The next higher privilege level is read/write access. This level enables operators to read, add to, or write over any data for which they have authority. Operators usually only have read/write access to data copied from an original location—they cannot access the original data.

Access Change. The third and highest level is access change. This level enables operators the right to modify data directly in its original location, in addition to data copied from the original location. Operators may also have the right to change file and operator access permissions in the system (a supervisor right).

These privilege levels are commonly much more granular than we have stated them here. Privilege levels in a large organization can, in fact, be very complicated.

Operations Job Function Overview

In a large shop, job functions and duties may be divided amongst a very large base of IT personnel. In many IT departments, the following roles are combined into fewer positions. The following listing, however, gives a nice overview of the various task components of the operational functions.

Computer Operator. Responsible for backups, running the system console, mounting and unmounting reel tapes and cartridges, recording and reporting operational problems with hardware devices and software products, and maintaining environmental controls.

Operations Analyst. Responsible for working with application software developers, maintenance programmers, and computer operators.

Job Control Analyst. Responsible for the overall quality of the production job control language and conformance to standards.

Production Scheduler. Responsible for planning, creating, and coordinating computer processing schedules for all production and job streams in conjunction with the established processing periods and calendars.

Production Control Analyst. Responsible for the printing and distribution of computer reports and microfiche/microfilm records.

Tape Librarian. Responsible for collecting input tapes and scratch tapes, sending tapes to and receiving returns from off-site storage and third parties, and for maintaining tapes.

Record Retention

Record retention refers to how long transactions and other types of records (legal, audit trails, email, and so forth) should be retained according to management, legal, audit, or tax compliance requirements. In the Operations Security domain, record retention deals with retaining computer files, directories, and libraries. The retention of data media (tapes, diskettes, and backup media) can be based on one or more criteria, such as number of days elapsed, number of days since creation, hold time, or other factors. An example of record retention issues could be the mandated retention periods for trial documentation or financial records.

Data Remanence

Data remanence refers to the data left on the media after the media has been erased. After erasure, there may be some physical traces left, which could enable the data to be reconstructed that could contain sensitive material.

Systems administrators and security administrators should be informed of the risks involving the issues of object reuse, declassification, destruction, and disposition of storage media. Data remanence, object reuse, and the proper disposal of data media are discussed thoroughly in Chapter 10, "Physical Security."

Due Care and Due Diligence

The concepts of *due care* and *due diligence* require that an organization engage in good business practices relative to the organization's industry. Training employees in security awareness could be an example of due care, unlike simply creating a policy with no implementation plan or follow up. Mandating statements from the employees stating that they have read and understood appropriate computer behavior is also an example of due care.

Due diligence may be mandated by various legal requirements in the organization's industry or compliance with governmental regulatory standards. Due care and due diligence are described in more detail in Chapter 9, "Law, Investigation, and Ethics."

Due Care and the Internet Community

Due care and due diligence are becoming serious issues in computer operations today. In fact, the legal system has begun to hold major partners liable for the lack of due care in the event of a major security breach. Violations of security and privacy are hot-button issues that are confronting the Internet community, and standards covering the best practices of due care are necessary for an organization's protection.

Documentation

A security system needs documentation controls. Documentation can include several things — security plans, contingency plans, risk analyses, and security policies and procedures. Most of this documentation must be protected from unauthorized disclosure, and it must also be available in the event of a disaster.

Operations Controls

Operations Controls embody the day-to-day procedures used to protect computer operations. The concepts of resource protection, hardware/software control, and privileged entity must be understood by a CISSP candidate.

The following are the most important aspects of operations controls:

- Resource protection
- Hardware controls
- Software controls
- Privileged-entity controls
- Media controls
- Physical access controls

Resource Protection

Resource protection is just what it sounds like — it is the concept of protecting an organization's computing resources and assets from loss or compromise. Computing resources are defined as any hardware, software, or data that is owned and used by the organization. Resource protection is designed to help reduce the possibility of damage, which can result from the unauthorized disclosure and/or alteration of data, by limiting the opportunities for its misuse.

Resources that Require Protection

These are various examples of resources that require protection.

Hardware Resources

- Communications, which includes routers, firewalls, gateways, switches, modems, and access servers
- Storage media, which includes floppies, removable drives, external hard drives, tapes, and cartridges
- Processing systems, which includes file servers, mail servers, Internet servers, backup servers, and tape drives
- Standalone computers, which includes workstations, modems, disks, and tapes
- Printers and fax machines

Software Resources

- Program libraries and source code
- Vendor software or proprietary packages
- Operating system software and systems utilities

Data Resources

- Backup data
- User data files
- Password files
- Operating Data Directories
- System logs and audit trails

Transparency of Controls

One important aspect of controls is the need for their transparency. Operators need to feel that security protections are reasonably flexible and that the security protections do not get in the way of doing their job. Ideally, the controls should not require users to perform extra steps, although realistically this is hard to achieve. Transparency also aids in preventing users from learning too much about the security controls.

Hardware Controls

Hardware Maintenance. System maintenance requires physical or logical access to a system by support and operations staff, vendors, or service providers. Maintenance may be performed on site, or it may be transported to a repair site. It may also be remotely performed. Furthermore, background investigations of the service personnel may be necessary. Supervising and escorting the maintenance personnel when they are on-site is also necessary.

Maintenance Accounts. Many computer systems provide *maintenance accounts*. These supervisor-level accounts are created at the factory with preset and widely known passwords. It is critical to change these passwords or at least disable the accounts until these accounts are needed. If an account is used remotely, authentication of the maintenance provider can be performed by using call-back or encryption.

Diagnostic Port Control. Many systems have diagnostic ports through which troubleshooters can directly access the hardware. These ports should only be used by authorized personnel and should not enable either internal or external unauthorized access. *Diagnostic port attacks* is the term that describes this type of abuse.

Hardware Physical Control. Many data processing areas that contain hardware may require locks and alarms. The following are some examples:

- Sensitive operator terminals and keyboards
- Media storage cabinets or rooms
- Server or communications equipment data centers
- Modem pools or telecommunication circuit rooms

Locks and alarms are described in Chapter 10, "Physical Security."

Software Controls

An important element of operations controls is software support — controlling what software is used in a system. Elements of controls on software are as follows:

Anti-Virus Management. If personnel can load or execute any software on a system, the system is more vulnerable to viruses, unexpected software interactions, and to the subversion of security controls.

Software Testing. A rigid and formal software testing process is required to determine compatibility with custom applications or to identify other unforeseen interactions. This procedure should also apply to software upgrades.

Software Utilities. Powerful systems utilities can compromise the integrity of operations systems and logical access controls. Their use must be controlled by security policy.

Safe Software Storage. A combination of logical and physical access controls should be implemented to ensure that the software and copies of backups have not been modified without proper authorization.

Backup Controls. Not only do support and operations personnel backup software and data, in a distributed environment, users may backup their own data. It is very important to routinely test the restore accuracy of a backup system. A backup should also be stored securely to protect from theft, damage, or environmental problems. A description of the types of backups is in Chapter 3, “Telecommunications and Network Security.”

Privileged Entity Controls

Privileged entity access, which is also known as *privileged operations functions*, is defined as an extended or special access to computing resources given to operators and system administrators. Many job duties and functions require privileged access.

Privileged entity access is most often divided into classes. Operators should be assigned to a class based on their job title.

The following are some examples of privileged entity operator functions:

- Special access to system commands
- Access to special parameters
- Access to the system control program

Restricting Hardware Instructions

A *system control program* restricts the execution of certain computing functions, and permits them only when a processor is in a particular functional state, known as *privileged or supervisor state*. Applications can run in different states, during which different commands are permitted. To be authorized to execute privileged instructions, a program should be running in a restrictive state that enables these commands.

Media Resource Protection

Media resource protection can be classified into two areas — media security controls and media viability controls. Media security controls are implemented to prevent any threat to C.I.A. by the intentional or unintentional exposure of sensitive data. Media viability controls are implemented to preserve the proper working state of the media, particularly to facilitate the timely and accurate restoration of the system after a failure.

Media Security Controls

Media security controls should be designed to prevent the loss of sensitive information when the media is stored outside the system.

A CISSP candidate needs to know several of the following elements of media security controls:

Logging. Logging the use of data media provides accountability. Logging also assists in physical inventory control, by preventing tapes from walking away and facilitating their recovery process.

Access Control. Physical access control to the media is used to prevent unauthorized personnel from accessing the media. This is also a part of physical inventory control.

Proper Disposal. Proper disposal of the media after use is required to prevent data remanence. The process of removing information from used data media is called *sanitization*. Three techniques are commonly used for sanitization — overwriting, degaussing, and destruction. These are described in Chapter 10.

Media Viability Controls

Many physical controls should be used to protect the viability of the data storage media. The goal is to protect the media from damage during handling and transportation, or during short-term or long-term storage. Proper marking and labeling of the media is required in the event of a system recovery process:

Marking. All data storage media should be accurately marked or labeled. The labels can be used to identify media with special handling instructions, or to log serial numbers or bar codes for retrieval during a system recovery.

There is a difference between this kind of physical storage media marking for inventory control and the logical data labeling of sensitivity classification for mandatory access control, which is described in other chapters, so please do not get them confused.

Handling. Proper handling of the media is important. Some issues with the handling of media include cleanliness of the media and the protection from physical damage to the media during transportation to the archive sites.

Storage. Storage of the media is very important for both security and environmental reasons. A proper heat- and humidity-free, clean storage environment should be provided for the media. Data media is sensitive to temperature, liquids, magnetism, smoke, and dust.

Media Librarian

It is the job of a media librarian to control access to the media library and to regulate the media library environment. All media must be labeled in a human and machine-readable form that should contain information such as the date and by whom the media was created, the retention period, a volume name and version, and security classification.

Physical Access Controls

The control of physical access to the resources is the major tenet of the Physical Security domain. Obviously, the Operations Security domain requires physical access control, and the following list contains examples of some of the elements of the operations resources that need physical access control.

Hardware

- Control of communications and the computing equipment
- Control of the storage media
- Control of the printed logs and reports

Software

- Control of the backup files
- Control of the system logs
- Control of the production applications
- Control of the sensitive/critical data

Obviously all personnel require some sort of control and accountability when accessing physical resources, yet some personnel will require special physical access to perform their job functions. The following are examples of this type of personnel:

- IT department personnel
- Cleaning staff
- Heating Ventilation and Air Conditioning (HVAC) maintenance personnel
- Third-party service contract personnel
- Consultants, contractors, and temporary staff

Special arrangements for supervision must be made when external support providers are entering a data center.

Note Physical piggybacking describes when an unauthorized person goes through a door behind an authorized person. The concept of a “man trap” (described in Chapter 10) is designed to prevent physical piggybacking.

Monitoring and Auditing

Problem identification and problem resolution are the primary goals of monitoring. The concept of monitoring is integral to almost all of the domains of information security. In Chapter 3, “Telecommunications and Network Security,” we described the technical aspects of monitoring and intrusion detection. Chapter 10, “Physical Security,” will also describe intrusion detection and monitoring from a physical access perspective. In this chapter, we are more concerned with monitoring the controls implemented in an operational facility in order to identify abnormal computer usage, such as inappropriate use or intentional fraud. Failure recognition and response, which includes reporting mechanisms, is an important part of monitoring.

Monitoring

Monitoring contains the mechanisms, tools, and techniques which permit the identification of security events that could impact the operation of a computer facility. It also includes the actions to identify the important elements of an event and to report that information appropriately.

The concept of monitoring includes monitoring for illegal software installation, monitoring the hardware for faults and error states, and monitoring operational events for anomalies.

Monitoring Techniques

To perform this type of monitoring, an information security professional has several tools at his disposal:

- Intrusion detection
- Penetration testing
- Violation processing using clipping levels

Intrusion Detection (ID)

Intrusion Detection (ID) is a useful tool that can assist in the detective analysis of intrusion attempts. ID can be used not only for the identification of intruders, but it can also be used to create a sampling of traffic patterns. By analyzing the activities occurring outside of normal clipping levels, a security practitioner can find evidence of events such as in-band signaling or other system abuses. A more in-depth description about the types of common intrusion detection is provided in Chapter 3 and Chapter 10.

Penetration Testing

Penetration testing is the process of testing a network’s defenses by attempting to access the system from the outside using the same techniques an external intruder (for example, a cracker) would use. This testing gives a security professional a better snapshot of the organization’s security posture.

Among the techniques used to perform a penetration test are:

- *Scanning and Probing.* Various scanners, like a port scanner, can reveal information about a network's infrastructure and enable an intruder to access the network's unsecured ports.
- *Demon Dialing.* Demon (or "war") dialers automatically test every phone line in an exchange to try to locate modems that are attached to the network. Information about these modems can then be used to attempt external unauthorized access.
- *Sniffing.* A protocol analyzer can be used to capture data packets that are later decoded to collect information such as passwords or infrastructure configurations.

Other techniques that are not solely technology-based may be used to complement the penetration test. The following are examples of such techniques:

- *Dumpster Diving.* Searching paper disposal areas for unshredded or otherwise improperly disposed of reports.
- *Social Engineering.* The most commonly used technique of all — getting information (like passwords) just by asking for them.

Violation Analysis

One of the most used techniques to track anomalies in user activity is *violation tracking, processing, and analysis*. To make violation tracking effective, *clipping levels* must be established. A clipping level is a baseline of user activity that is considered routine level of user errors. A clipping level is used to enable a system to ignore normal user errors. When the clipping level is exceeded, a violation record is then produced. Clipping levels are also used for *variance detection*.

Using clipping levels and *profile-based anomaly detection*, the following are the types of violations that should be tracked, processed, and analyzed:

- Repetitive mistakes that exceed the clipping level number
- Individuals who exceed their authority
- Too many people with unrestricted access
- Patterns indicating serious intrusion attempts

Note

Profile-based anomaly detection uses profiles to look for abnormalities in user behavior. A *profile* is a pattern that characterizes the behavior of users. Patterns of usage are established according to the various types of activity the users engage in, such as processing exceptions, resource utilization, and patterns in actions performed, for example. The ways in which the various types of activity are recorded in the profile are referred to as *profile metrics*.

Auditing

The implementation of regular system audits is the foundation of operational security controls monitoring. In addition to enabling internal and external compliance checking, regular auditing of audit (transaction) trails and logs can assist the monitoring function by helping to recognize patterns of abnormal user behavior.

Independent Testing

It is important to note that, in most cases, external penetration testing should be performed by a reputable, experienced firm that is independent of an organization's IT or Audit departments. This independence guarantees an objective, non-political report on the state of the company's defenses.

Security Auditing

Information Technology (IT) auditors are often divided into two types — internal and external. Internal auditors typically work for a given organization, while external auditors do not. External auditors are often Certified Public Accountants (CPAs) or other audit professionals who are hired to perform an independent audit of an organization's financial statements. Internal auditors, on the other hand, usually have a much broader mandate — checking for compliance and standards of due care, auditing operational cost-efficiencies, and recommending the appropriate controls.

IT auditors typically audit the following functions:

- Backup controls
- System and transaction controls
- Data library procedures
- Systems development standards
- Data center security
- Contingency plans

In addition, IT auditors may also recommend improvement to controls, and they often participate in a system's development process to help an organization to avoid costly re-engineering after the system's implementation.

Audit Trails

An audit (or transaction) trail enables a security practitioner to trace a transaction's history. This transaction trail provides information about additions, deletions, or modifications to the data within a system. Audit trails enable the enforcement of individual accountability by creating a reconstruction of events. Like monitoring, one purpose of an audit trail is to assist in a problem's identification that leads to a problem's resolution. An effectively implemented audit trail also lets the data be retrieved and easily certified by an auditor. Any unusual activity and variations from the established procedures should be identified and investigated.

The audit logs should record the following:

- The transaction's date and time
- Who processed the transaction
- At which terminal the transaction was processed
- Various security events relating to the transaction

In addition, an auditor should also examine the audit logs for the following:

- Amendments to production jobs
- Production job reruns
- Computer operator practices

Other important security issues regarding the use of audit logs are as follows:

- Retention and protection of the audit media and reports when their storage is off site
- Protection against the alteration of audit or transaction logs
- Protection against the unavailability of an audit media during an event

Problem Management Concepts

Effective auditing embraces the concepts of problem management. Problem management is a way to control the process of problem isolation and problem resolution. An auditor may use problem management to resolve the issues arising from an IT security audit, for example.

The goal of problem management is threefold:

1. To reduce failures to a manageable level.
2. To prevent the occurrence or re-occurrence of a problem.
3. To mitigate the negative impact of problems on computing services and resources.

The first step in implementing problem management is to define the potential problem areas and the abnormal events that should be investigated. Some examples of potential problem areas are

- The performance and availability of computing resources and services
- The system and networking infrastructure
- Procedures and transactions
- The safety and security of personnel

Some examples of abnormal events which could be discovered during an audit are:

- Degraded hardware or software resource availability
- Deviations from the standard transaction procedures
- Unexplained occurrences in a processing chain

Of course, the final objective of problem management is resolution of the problem.

Electronic Audit Trails

Maintaining a proper audit trail is more difficult now because more transactions are not recorded to paper media, and thus they will always stay in an electronic form. In the old paper system, a physical purchase order may be prepared with multiple copies, initiating a physical, permanent paper trail. An auditor's job is now more complicated because digital media is more transient and a paper trail may not exist.

Threats and Vulnerabilities

A *threat* is simply any event that, if realized, can cause damage to a system, and create a loss of confidentiality, availability, or integrity. Threats can be malicious — such as the intentional modification of sensitive information — or they can be accidental — such as an error in a transaction calculation or the accidental deletion of a file.

A *vulnerability* is a weakness in a system that can be exploited by a threat. Reducing the vulnerable aspects of a system can reduce the risk and the impact of threats on the system.

For example, a password generation tool, which helps users choose robust passwords, reduces the chance users will select poor passwords (the vulnerability) and makes the password more difficult to crack (the threat of external attack).

Threats

We have grouped the threats into several categories, and we will describe some of the elements of each category.

Accidental Loss

Accidental loss is a loss that is incurred unintentionally, though either the lack of operator training or proficiency, or by the malfunctioning of an application processing procedure. The following are some examples of the types of accidental loss:

- *Operator input errors and omissions.* Manual input transaction errors, entry or data deletion, and faulty data modification.

- *Transaction processing errors.* Errors that are introduced into the data through faulty application programming or processing procedures.

Inappropriate Activities

Inappropriate activity is computer behavior that, while not rising to the level of criminal activity, may be grounds for job action or dismissal.

- *Inappropriate Content.* Using the company systems to store pornography, entertainment, political, or violent content.
- *Waste of Corporate Resources.* Personal use of hardware or software, such as conducting a private business with a company's computer system.
- *Sexual or Racial Harassment.* Using email or other computer resources to distribute inappropriate material.
- *Abuse of Privileges or Rights.* Using unauthorized access levels to violate the confidentiality of sensitive company information.

Illegal Computer Operations and Intentional Attacks

Under this heading, we have grouped the areas of computer activities that are considered as intentional and illegal computer activity for personal financial gain or destruction.

- *Eavesdropping.* Data scavenging, traffic or trend analysis, social engineering, economic or political espionage, sniffing, dumpster diving, keystroke monitoring, or shoulder surfing are all types of eavesdropping to gain information or to create a foundation for a later attack. Eavesdropping is a primary cause of the failure of confidentiality.
- *Fraud.* Examples of the types of fraud are collusion, falsified transactions, data manipulation, and other altering of data integrity for gain.
- *Theft.* Examples of the types of theft are the theft of information or trade secrets for profit or unauthorized disclosure, and hardware or software physical theft.
- *Sabotage.* Sabotage includes Denial of Service (DoS), production delays, and data integrity sabotage.
- *External Attack.* Examples of external attacks are malicious cracking, scanning, and probing to gain infrastructure information, demon dialing to locate an unsecured modem line, and the insertion of a malicious code or virus.

Vulnerabilities

Traffic/Trend Analysis. *Traffic analysis*, which is sometimes called *trend analysis*, is a technique employed by an intruder that involves analyzing data characteristics (message length, message frequency, and so forth) and the patterns of transmissions (rather than any knowledge of the actual information transmitted) to infer information that is useful to an intruder.

Countermeasures to traffic analysis are similar to the countermeasures to crypto-attacks:

- *Padding messages.* Creating all messages to be a uniform data size by filling empty space in the data.
- *Sending noise.* Transmitting non-informational data elements mixed in with real information to disguise the real message.
- *Covert channel analysis.* Previously described in the "Orange Book Controls" section of this chapter.

Maintenance Accounts. See Hardware Controls. It is a method used to break into computer systems by using maintenance accounts that still have factory-set or easily guessed passwords. Physical access to the hardware by maintenance personnel can also constitute a security violation.

Data Scavenging Attacks. Data scavenging is the technique of piecing together information from found bits of data. There are two common types of data scavenging attacks:

1. *Keyboard Attacks.* Data scavenging through the resources that are available to normal system users — sitting at the keyboard and using normal utilities and tools to glean information.
2. *Laboratory Attacks.* Data scavenging by using very precise electronic equipment — it is a planned, orchestrated attack.

IPL Vulnerabilities. The start of a system, the *Initial Program Load (IPL)*, presents very specific system vulnerabilities whether the system is a centralized mainframe type or a distributed LAN type. During the IPL, the operator brings up the facility's system. This operator has the ability to put a system into a single user mode, without full security features, which is a very powerful ability. In this state, an operator could load unauthorized programs or data, reset passwords, rename various resources, or reset the system's time and date. The operator could also reassign the data ports or communications lines to transmit information to a confederate outside of the data center.

In a Local Area Network (LAN), a system administrator could start the bootup sequence from a tape, CD-ROM, or floppy disk, bypassing the operating system's security on the hard drive.

Network Address Hijacking. It may be possible for an intruder to re-route data traffic from a server or network device to a personal machine, either by device address modification, or network address "hijacking." This diversion enables the intruder to capture traffic to and from the devices for data analysis or modification, or to steal the password file from the server and gain access to user accounts. By rerouting the data output, the intruder can obtain supervisory terminal functions and bypass the system logs.

Sample Questions

1. What does IPL stand for? ?
 - A. Initial Program Life cycle
 - B. Initial Program Load
 - C. Initial Post-transaction Logging
 - D. Internet Police League

2. Which of the following is NOT a use of an audit trail? ?
 - A. Provides information about additions, deletions, or modifications to the data
 - B. Collects information such as passwords or infrastructure configurations
 - C. Assists the monitoring function by helping to recognize patterns of abnormal user behavior
 - D. Allows the security practitioner to trace a transaction's history

3. Why is security an issue when a system is booted into "Single-user mode"? ?
 - A. The operating system is started without the security front-end loaded.
 - B. The users cannot login to the system and they will complain.
 - C. Proper forensics cannot be executed while in the single-user mode.
 - D. Backup tapes cannot be restored while in the single-user mode.

4. Which of the following examples is the best definition of Fail Secure? ?
 - A. Access personnel have security clearance, but they do not have a "need-to-know."
 - B. The operating system is started without the security front-end loaded.
 - C. The system fails to preserve a secure state during and after a system crash.
 - D. The system preserves a secure state during and after a system crash.

5. Which of the following would NOT be an example of compensating controls being implemented? ?
- A. Sensitive information requiring two authorized signatures to release
 - B. A safety deposit box needing two keys to open
 - C. Modifying the timing of a system resource in some measurable way to covertly transmit information
 - D. Signing in or out of a traffic log and using a magnetic card to access to an operations center
6. "Separation of duties" embodies what principle? ?
- A. An operator does not know more about the system than the minimum required to do the job.
 - B. Two operators are required to work in tandem to perform a task.
 - C. The operators' duties are frequently rotated.
 - D. The operators have different duties to prevent one person from compromising the system.
7. Which is NOT true about Covert Channel Analysis? ?
- A. It is an operational assurance requirement that is specified in the Orange book.
 - B. It is required for B2 class systems in order to protect against covert storage channels.
 - C. It is required for B2 class systems to protect against covert timing channels.
 - D. It is required for B3 class systems to protect against both covert storage and covert timing channels.
8. An audit trail is an example of what type of control? ?

- A. Deterrent control
B. Preventative control
C. Detective control
D. Application control
9. Using pre-numbered forms to initiate a transaction is an example of what type of control? ?
- A. Deterrent control
B. Preventative control
C. Detective control
D. Application control
10. Which of the following is a reason to institute output controls? ?
- A. To preserve the integrity of the data in the system while changes are being made to the configuration
B. To protect the output's confidentiality
C. To detect irregularities in the software's operation
D. To recover damage after an identified system failure
11. Convert Channel Analysis, Trusted Facility Management, and Trusted Recovery are parts of which book in the TCSEC Rainbow series? ?
- A. Red Book
B. Orange Book
C. Green Book
D. Dark Green Book
12. How do covert timing channels convey information? ?
- A. By changing a system's stored data characteristics
B. By generating noise and traffic with the data
C. By performing a covert channel analysis
D. By modifying the timing of a system resource in some measurable way
13. Which of the following is the best example of "need-to-know"? ?
- A. An operator does not know more about the system than

the minimum required to do the job.

- B. Two operators are required to work together to perform a task.
- C. The operators' duties are frequently rotated.
- D. An operator cannot generate and verify transactions alone.

14. Which of the following is an example of "least privilege"?

?

- A. An operator does not know more about the system than the minimum required to do the job.
- B. An operator does not have more system rights than the minimum required to do the job.
- C. The operators' duties are frequently rotated.
- D. An operator cannot generate and verify transactions alone.

15. Which of the following would be the BEST description of clipping levels?

?

- A. A baseline of user errors above which violations will be recorded
- B. A listing of every error made by users to initiate violation processing
- C. Variance detection of too many people with unrestricted access
- D. Changes a system's stored data characteristics

16. Which of the following is NOT a proper media control?

?

- A. The data media should be logged to provide a physical inventory control.
- B. All data storage media should be accurately marked.
- C. A proper storage environment should be provided for the media.
- D. The media that is re-used in a sensitive environment does not

- need sanitization.
17. Configuration management control best refers to ?
- A. The concept of “least control” in operations
 - B. Ensuring that changes to the system do not unintentionally diminish security
 - C. The use of privileged-entity controls for system administrator functions
 - D. Implementing resource protection schemes for hardware control
18. Which of the following would NOT be considered a penetration testing technique? ?
- A. War dialing
 - B. Sniffing
 - C. Data manipulation
 - D. Scanning
19. Inappropriate computer activities could be described as ?
- A. Computer behavior that may be grounds for a job action or dismissal
 - B. Loss incurred unintentionally though the lack of operator training
 - C. Theft of information or trade secrets for profit or unauthorized disclosure
 - D. Data scavenging through the resources available to normal system users
20. Why are maintenance accounts a threat to operations controls? ?
- A. Maintenance personnel could slip and fall and sue the organization.
 - B. Maintenance accounts are commonly used by hackers to access network devices.
 - C. Maintenance account information could be compromised if printed reports are left out in the open.
 - D. Maintenance may require

physical access to the system
by vendors or service
providers.

Answers

1. *Answer:* b). The IPL is a task performed by the operator to boot up the system. The other terms do not exist.
2. *Answer:* b). Auditing should not be used to collect user's passwords. It is used for the other three examples, however.
3. *Answer:* a). When the operator boots the system in "single-user mode," the user front-end security controls are not loaded. This mode should be used for recovery and maintenance procedures only, and all operations should be logged and audited.
4. *Answer:* d). Based on the Common Criteria, a system can be evaluated as Fail Secure if it "preserves a secure state during and after identified failures occur."
5. *Answer:* c). This is the definition for a covert timing channel. The other three are examples of compensating controls, which are a combination of technical, administrative or physical controls to enhance security.
6. *Answer:* d). "Separation of duties" means that the operators are prevented from generating and verifying transactions alone, for example. A task might be divided into different smaller tasks to accomplish this, or in the case of an operator with multiple duties, the operator makes a logical, functional job change when performing such conflicting duties. Answer a) is "need-to-know," answer b) is "dual-control", and c) is "job rotation."
7. *Answer:* c). Covert channel analysis is required to be performed for B2 level class systems to protect against covert storage channels by the Orange book. B3 systems need to be protected against both covert storage channels and covert timing channels.
8. *Answer:* c). An audit trail is a record of events to piece together what has happened and allow enforcement of individual accountability by creating a reconstruction of events. They can be used to assist in the proper implementation of the other controls, however.
9. *Answer:* b). Pre-numbered forms are an example of the general category of preventative controls. They can also be considered a type of transaction controls, and input control.
10. *Answer:* b). In addition to being used as a transaction control verification mechanism, output controls are used to ensure output, such as printed reports, are distributed securely. a), is an example of Configuration or Change control, c) is an example of Application controls, and d) is an example of Recovery controls.
11. *Answer:* b). a), the Red Book is the Trusted Network Interpretation (TNI) summary of network requirements (described in the Telecommunications and Network Security domain), c) the Green Book is the Department of Defense

(DoD) *Password Management Guideline*, and d), the Dark Green Book is *The Guide to Understanding Data Remanence in Automated Information Systems*.

12. *Answer: d)* A covert timing channel alters the timing of parts of the system to enable it to be used to communicate information covertly (outside of the normal security function). Answer a), is the description of the use of a covert storage channel, b) is a technique to combat the use of covert channels, and c), is the Orange Book requirement for B3, B2, and A1 evaluated systems.
13. *Answer: a).* "Need-to-know" means the operators are working in an environment which limits their knowledge of the system, applications or data to the minimum elements that they require to perform their job. Answer b) is "dual-control," c) is "job rotation," and answer d) is "separation of duties."
14. *Answer: b).* "Least Privilege" embodies the concept that users or operators should be granted the lowest level of system access or system rights that allows them to perform their job. Answer a) is "need-to-know," c) is "job rotation," and d) is "separation of duties."
15. *Answer: a).* This is the best description of a clipping level. It's not b), as the reason for creating a clipping level is to prevent auditors from having to examine every error. The answer c), is a common use for clipping levels, but is not a definition. D) is meaningless.
16. *Answer: d).* Sanitization is the process of removing information from used data media to prevent data remanence. Different media require different types of sanitation. All the others are examples of proper media controls.
17. *Answer: b).* Configuration Management Control (and Change Control) are processes to ensure that any changes to the system are managed properly and do not inordinately affect either the availability or security of the system.
18. *Answer: c).* Data manipulation describes the corruption of data integrity to perform fraud for personal gain or other reasons. External penetration testing should not alter the data in any way. The other three are common penetration techniques.
19. *Answer: a).* While all of the activities described above are considered in the broad category of inappropriate activities, this description is used to define a narrower category of inappropriate activities. Answer b), is commonly defined as accidental loss, answer c), is considered intentionally illegal computer activity and d), is a "keyboard attack." A type of data scavenging attack using common tools or utilities available to the user.
20. *Answer: b)* Maintenance accounts are login accounts to systems resources, primarily networked devices. They often have the factory-set passwords which are frequently distributed through the hacker community.

Chapter 7: Applications and Systems Development

Overview

There are information system security issues associated with applications software whether the software is developed internally or acquired from an external source. This chapter addresses these security issues from the viewpoint of the developer, user, and information system security specialist. Thus, a CISSP professional should understand the following areas:

- The software life cycle development process
- The software process capability maturity model
- Object-oriented systems
- Artificial intelligence systems
- Database systems
 - Database security issues
 - Data warehousing
 - Data mining
 - Data dictionaries
- Application controls

The Software Life Cycle Development Process

Quality software is difficult to obtain without a development process. As with any project, two principal goals of software development are to produce a quality product that meets the customer's requirements and to stay within the budget and time schedule. A succession of models has emerged over time incorporating improvements in the development process. An early model defined succeeding stages taking into account the different staffing and planning that was required for each stage. The model was simplistic in that it assumed that each step could be completed and finalized without any effect from the later stages that may require rework. This model is shown in Figure 7.1 .

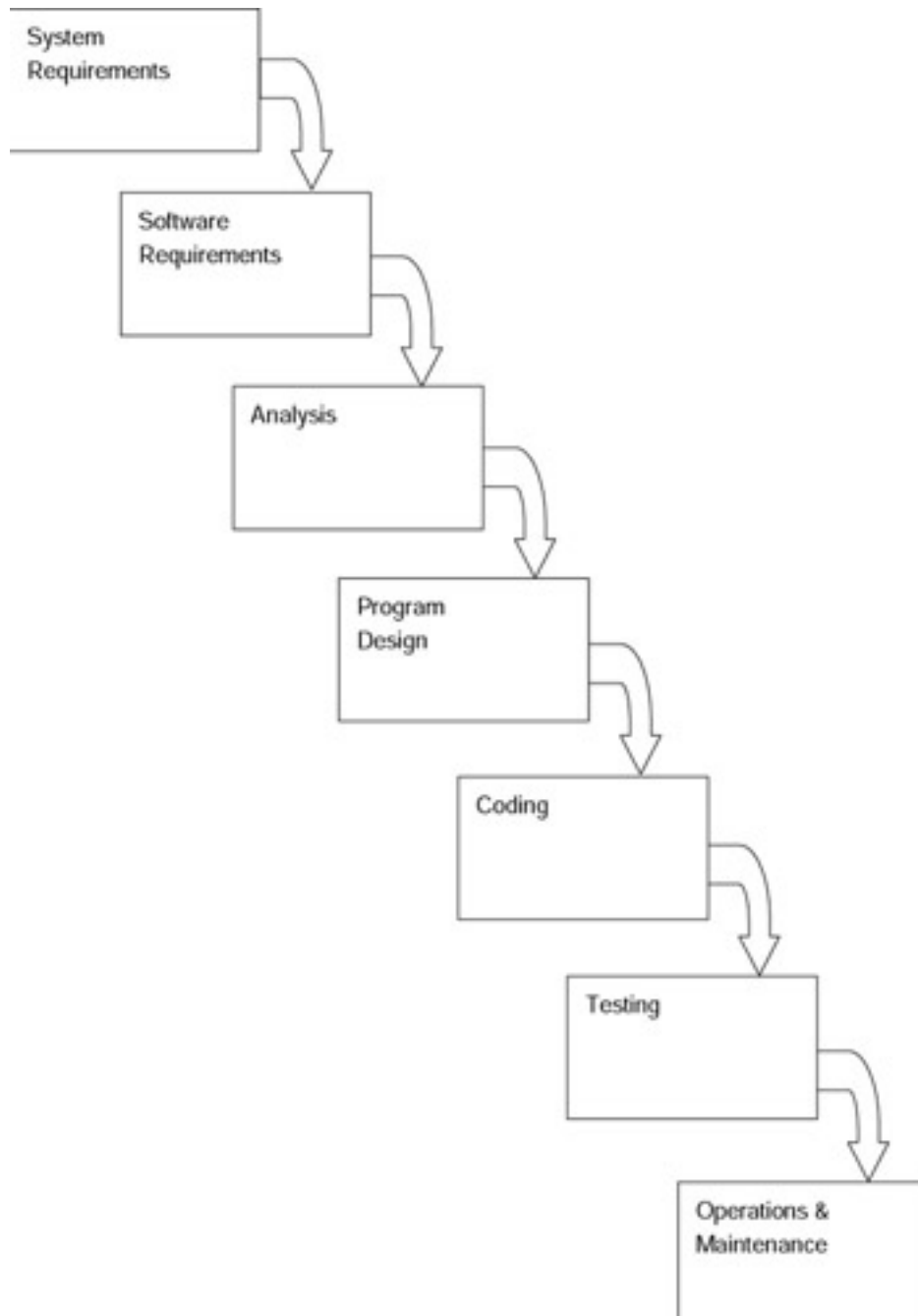


Figure 7.1: Simplistic software development model.

The Waterfall Model

Because subsequent stages such as design, coding, and testing in the development process may require modifying earlier stages in the model, the *Waterfall* model emerged. Under this model, software development can be managed if the developers are limited to going back only one stage to rework. If this limitation is not imposed (particularly on a large project with several team members), then any developer can be working on any phase at any time and the required rework may be accomplished several times. Obviously, this approach results in a lack of project control, and it is difficult to manage. The Waterfall model is shown in Figure 7.2.

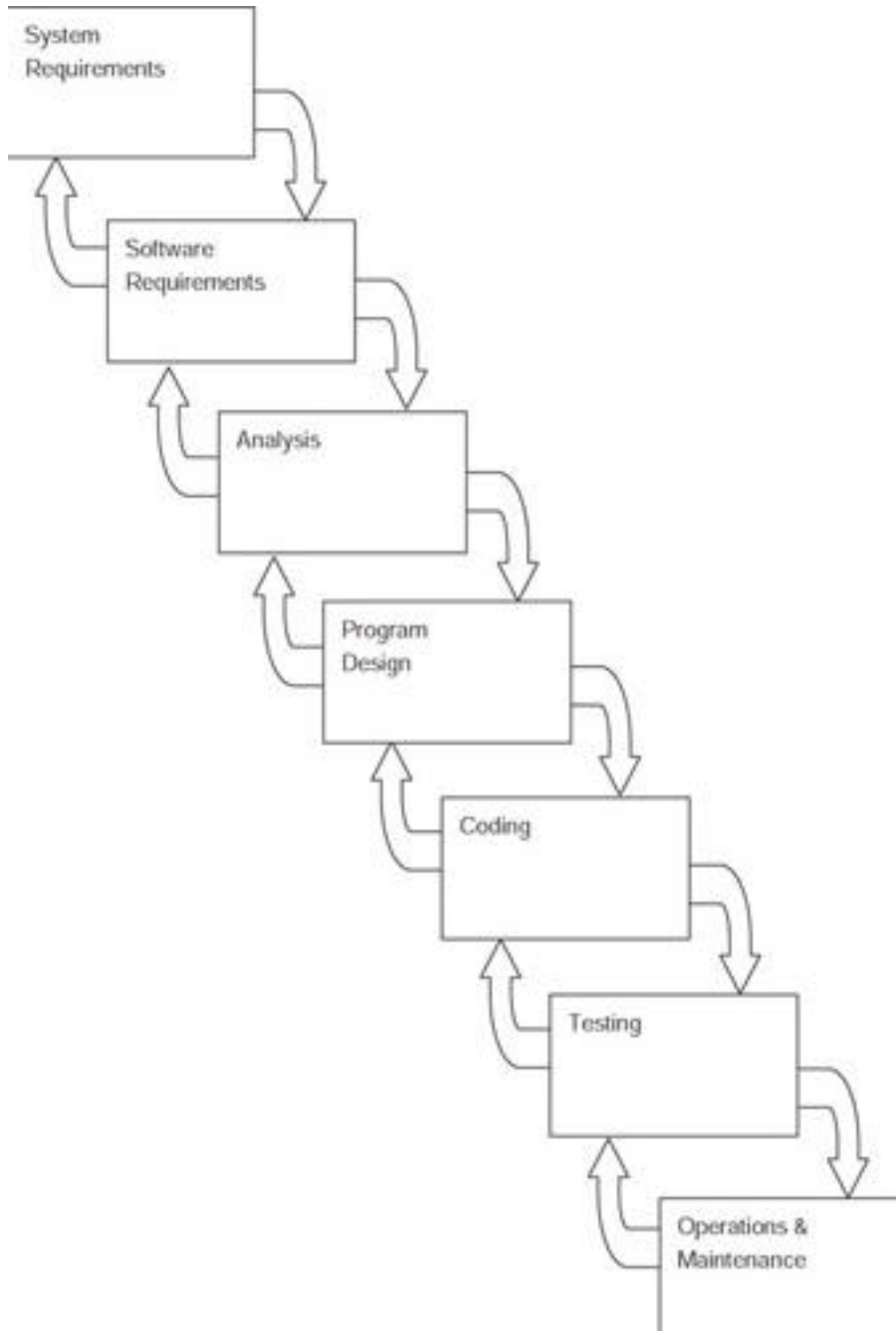


Figure 7.2: The Waterfall model.

One fundamental problem with these models is that they assume that a phase or stage ends at a specific time, however, this is not usually the case in real world applications. If an ending phase is forcibly tied to a project milestone, the situation can be improved. If rework is required in this mode, the phase is not officially pronounced as ending. The rework must then be accomplished and the project milestone met before the phase is officially recognized as completed. In 1976, Barry Boehm reinterpreted the Waterfall model to have phases end at project milestones and to have the backward arrows represent back references for verification and validation (V&V) against defined baselines. Verification evaluates the product during development against the specification, and validation refers to the work product satisfying the real-world requirements and concepts. In simpler terms, Barry Boehm states, "Verification is doing the job right and validation is doing the right job." These concepts are illustrated in Figure 7.3.

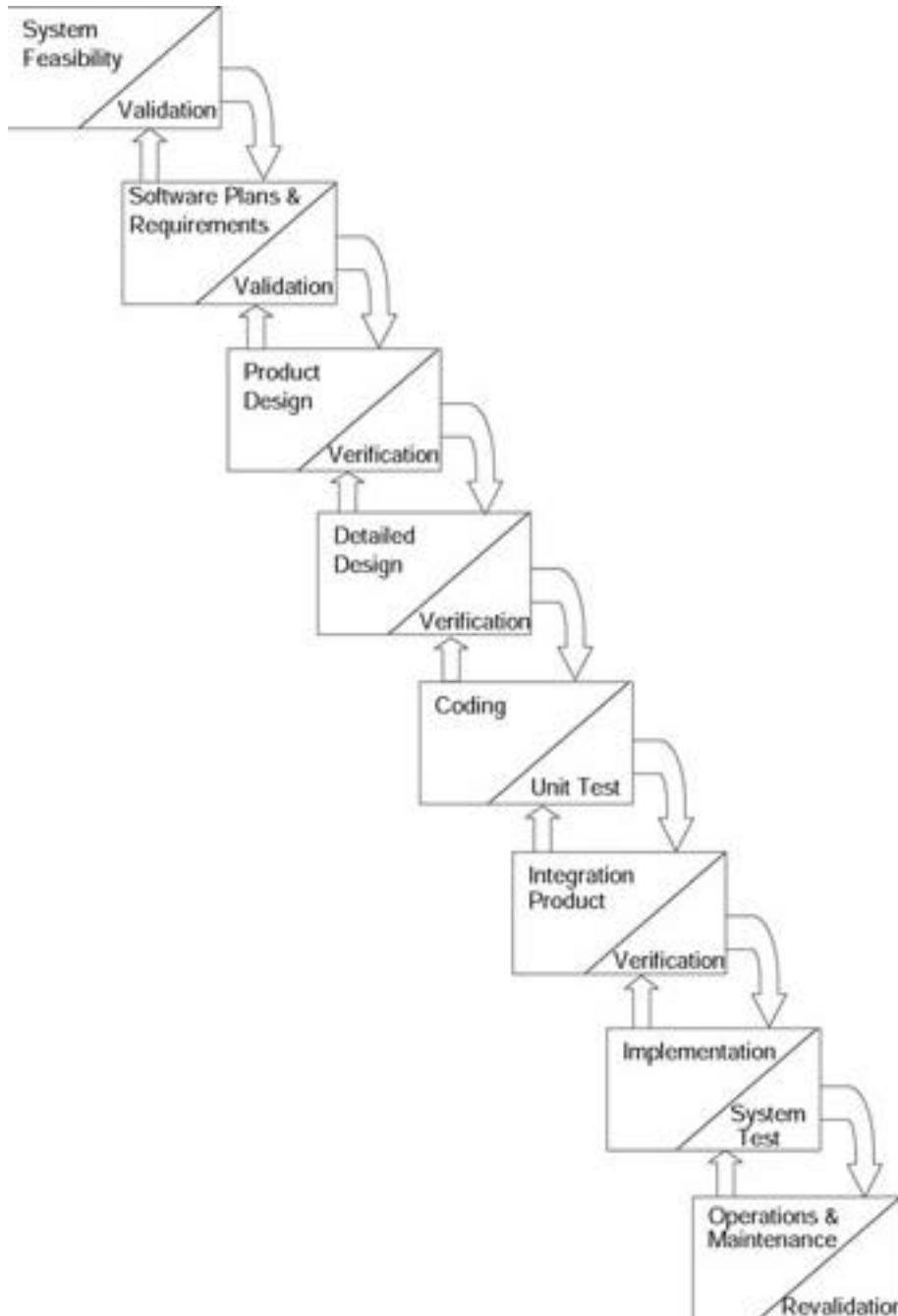


Figure 7.3: A modified Waterfall model incorporating V&V.

In this modified version of the Waterfall model, the end of each phase is a point in time for which no iteration of phases is provided. Rework can be accomplished within a phase when the phase end review shows that it is required.

The Spiral Model

In 1988 at TRW, Barry Boehm developed the *Spiral* model, which is actually a meta-model, that incorporates a number of the software development models. This model depicts a spiral that incorporates the various phases of software development. As shown in Figure 7.4, the angular dimension represents the progress made in completing the phases, and the radial dimension represents cumulative project cost. The model states that each cycle of the spiral involves the same series of steps for each part of the project.

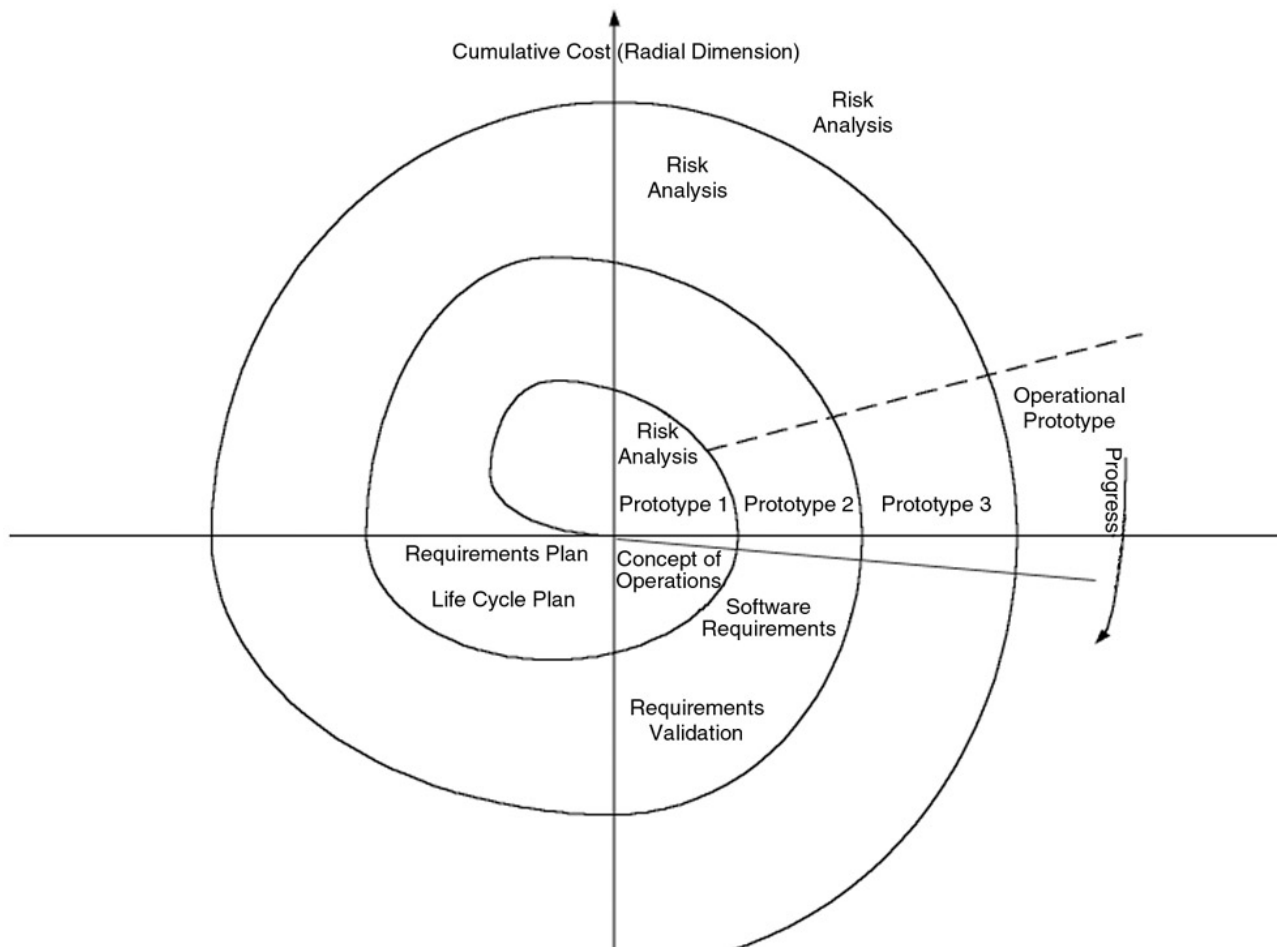


Figure 7.4: The Spiral Model.

The lower-left quadrant focuses on developing plans that will be reviewed in the upper quadrants of the diagram prior to finalization of the plans. Then, after a decision to proceed with the project is made, the spiral is initiated in the upper-left quadrant. This particular quadrant defines the objectives of the part of the project being addressed, alternative means of accomplishing this part of the project, and the constraints associated with these alternatives.

The next step involves assessing the alternatives in regard to the project objectives and constraints. This assessment can include prototyping, modeling, and simulation. The purpose of this step is to identify and evaluate the risks involved, and it is shown in the upper-right quadrant of the model. Once these issues are resolved, the next step in this procedure follows the traditional life cycle model approach. The lower-right quadrant of the spiral depicts the final developmental phase for each part of the product. An important concept of the Spiral model is that the left horizontal axis depicts the major review that is required to complete each full cycle.

Information Security and the Life Cycle Model

As is the case with most engineering and software development practices, the earlier in the process a component is introduced, the better chance there is for success, lower development costs, and reduced rework. Information security is no exception. Information security controls conception, development, implementation, testing, and maintenance should be conducted concurrently with the system software life cycle phases. This approach is conceptually shown in Figure 7.5.

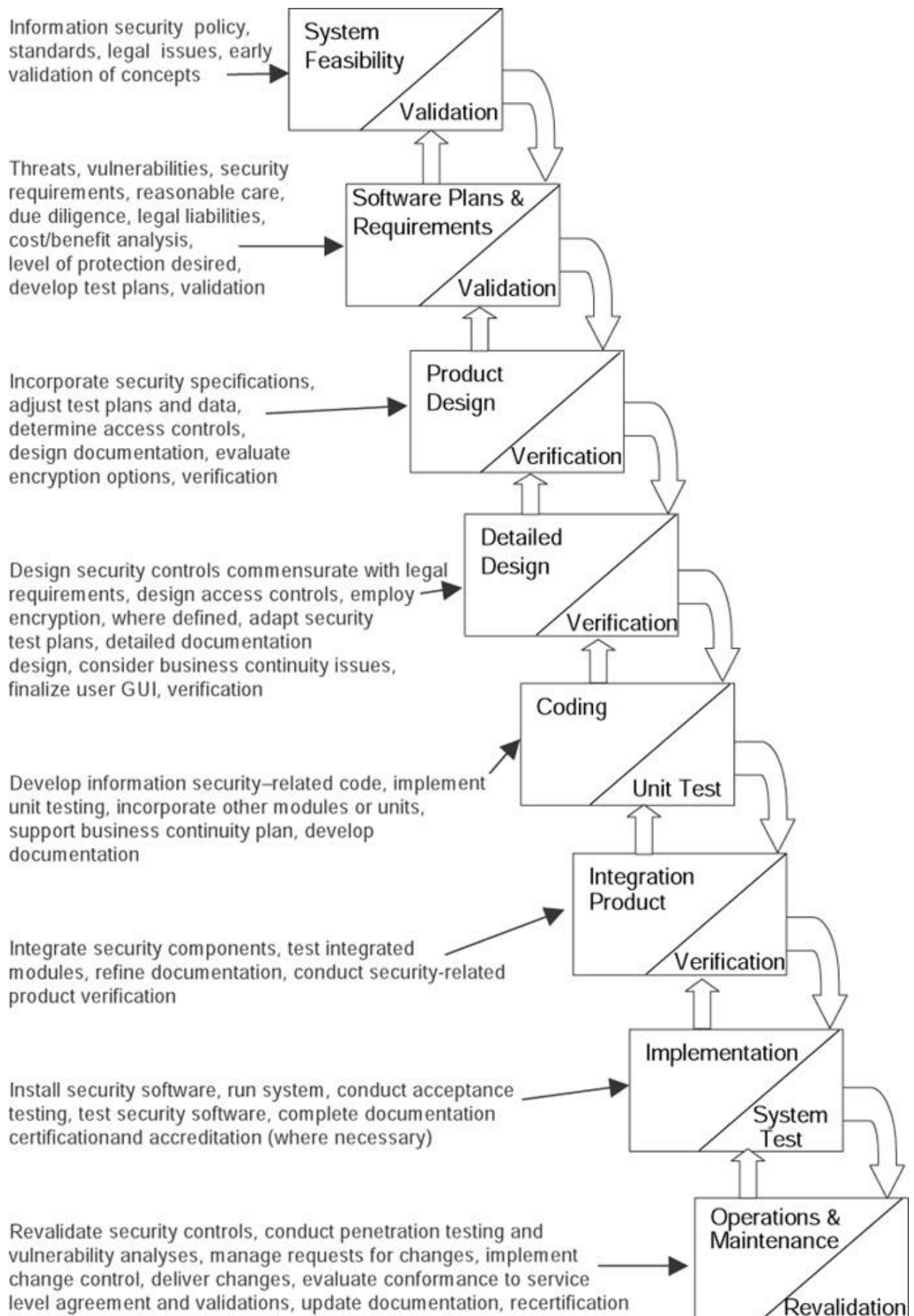


Figure 7.5: Security life cycle components.

Testing Issues

Testing of the software modules or unit testing should be addressed when the modules are being designed. Personnel separate from the programmers should conduct this testing. The test data is part of the specifications. Testing should not only check the modules using normal and valid input data, but it should also check for incorrect types, out of range values, and other bounds and/or conditions. Live or actual field data is not recommended for use in the testing procedures because both data types may not cover out of range situations and the correct outputs of the test are unknown. Special test suites of data that exercise all paths of the software to the fullest extent possible and whose correct resulting outputs are known beforehand should be used.

The Software Maintenance Phase and the Change Control Process

In the life cycle models we have presented, the maintenance phase is listed at the end of the cycle with operations. One way of looking at the maintenance phase is to divide it into the following three sub-phases:

1. Request control.
2. Change control.
3. Release control.

The request control activity manages the users' requests for changes to the software product and gathers information that can be used for managing this activity. The following steps are included in this activity:

- Establishing the priorities of requests
- Estimating the cost of the changes requested
- Determining the interface that is presented to the user

The change control process is the principal step in the maintenance phase. Issues that are addressed by change control include the following:

- Recreating and analyzing the problem
- Developing the changes and corresponding tests
- Performing quality control

In addition, there are also other considerations such as the following :

- The tool types to be used in implementing the changes
- The documentation of the changes
- The restriction of the changes' effects on other parts of the code
- Recertification and accreditation, if necessary

Release control is associated with issuing the latest release of the software. This step involves deciding which requests will be included in the new release, archiving of the release, configuration management, quality control, distribution, and acceptance testing.

Configuration Management

In order to manage evolving changes to software products and to formally track and issue new versions of software products, configuration management is employed. According to the British Standards Institution (British Standards Institute, U.K.; "Information Security Management, British Standard 7799," 1998), configuration management is "the discipline of identifying the components of a continually evolving system for the purposes of controlling changes to those components and maintaining integrity and traceability throughout the life cycle." The following definitions are associated with configuration management:

Configuration Item. A component whose state is to be recorded and against which changes are to be progressed.

Version. A recorded state of the configuration item.

Configuration. A collection of component configuration items that comprise a configuration item in some stage of its evolution (recursive).

Building. The process of assembling a version of a configuration item from versions of its component configuration items.

Build List. The set of the versions of the component configuration items that is used to build a version of a configuration item.

Software Library. A controlled area that is accessible only to approved users who are restricted to the use of approved procedures.

The following procedures are associated with configuration management:

1. Identify and document the functional and physical characteristics of each configuration item (*configuration identification*).
2. Control changes to the configuration items and issue versions of configuration items from the software library (*configuration control*).
3. Record the processing of changes (*configuration status accounting*).
4. Control the quality of the configuration management procedures (*configuration audit*).

The Software Capability Maturity Model (CMM)

The Software CMM is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes. A process is defined by the Carnegie Mellon University Software Engineering Institute (SEI) as “a set of activities, methods, practices, and transformations that people use to develop and maintain systems and associated products”(SEI, “The Capability Maturity Model: Guidelines for Improving the Software Process,” Addison Wesley, 1995.)

The Software CMM was first developed by the SEI in 1986 with support from the Mitre Corporation. The SEI defines five maturity levels that serve as a foundation for conducting continuous process improvement and as an ordinal scale for measuring the maturity of the organization involved in the software processes. The following are the five maturity levels and their corresponding focuses and characteristics:

Level 1 — Initiating. Competent people and heroics; processes are informal and ad hoc.

Level 2 — Repeatable. Project management processes; project management practices are institutionalized.

Level 3 — Defined. Engineering processes and organizational support; technical practices are integrated with management practices institutionalized.

Level 4 — Managed. Product and process improvement; product and process are quantitatively controlled.

Level 5 — Optimizing. Continuous process improvement; process improvement is institutionalized.

The Software CMM is a component that supports the concept of continuous process improvement. This concept is embodied in the SEI Process Improvement IDEAL Model and is shown in Figure 7.6.

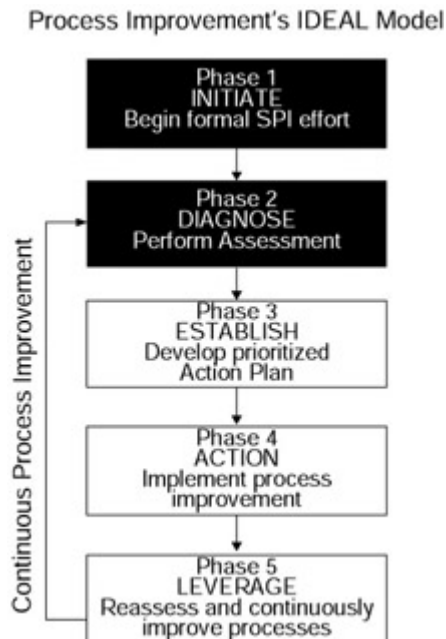


Figure 7.6: The IDEAL model.

Phase 1 of the IDEAL Model is the initiation phase in which management support is obtained for process improvement, the objectives and constraints of the process improvement effort are defined, and the resources and plans for the next phase are obtained.

Phase 2 identifies the appropriate appraisal method (such as CMM-based), identifies the project(s) to be appraised, trains the appraisal team, conducts the appraisal, and briefs management and the organization on the appraisal results.

In Phase 3, an action plan is developed based on the results of Phase 2, management is briefed on the action plan, and the resources and group(s) are coordinated to implement the action plan.

Phase 4 is the action phase where resources are recruited for implementation of the action plan, the action plan is implemented, the improvement effort is measured, and the plan and implementation are modified based on measurements and feedback.

Phase 5 is the review phase, which ensures that all success criteria have been achieved, all feedback is evaluated, the lessons learned are analyzed, the business plan and process improvement are compared for the desired outcome, and the next stage of the process improvement effort is planned.

The benefits of a long-term, formal software process improvement plan are as follows:

- Improved software quality
- Reduced life cycle time
- More accurate scheduling and meeting of milestones
- Management visibility
- Proactive planning and tracking

Object-Oriented Systems

An object-oriented system has the potential characteristics of being more reliable and capable of reducing the propagation of program change errors, in addition to supporting

modeling of the “real world.” An object-oriented system can be thought of as a group of independent *objects* that can be requested to perform certain operations or exhibit specific behaviors. These objects cooperate to provide the system’s required functionality. The objects have an *identity* and can be created as the program executes (*dynamic lifetime*.) To provide the desired characteristics of object-oriented systems, the objects are *encapsulated* — they can only be accessed through messages sent to them to request performance of their defined operations. The object can be viewed as a “black box” whose internal details are hidden from outside observation and cannot normally be modified. Grady Booch defines encapsulation as “The process of compartmentalizing the elements of an abstraction that constitute its structure and behavior; . . . [it] serves to separate the contractual interface of an abstraction and its implementation.” Objects also exhibit the *substitution* property, which means that objects providing compatible operations can be substituted for each other. According to Booch, “An object has a state, behavior, and identity” (Grady Booch. “Object- Oriented Development”. *IEEE Transactions on Software Engineering*, Vol. SE-12, No. 2, February 1986, pp. 211-221.)

The following definitions are fundamental to object-oriented systems:

Message. A message is the communication to an object to carry out some operation.

Method. A method is the code that defines the actions an object performs in response to a message.

Behavior. Behavior refers to the results exhibited by an object upon receipt of a message.

Class. A class is a collection of the common methods of a set of objects that defines the behavior of those objects. Booch defines a class as “a set of objects that share a common structure and a common behavior.”

Instance. Objects are instances of classes that contain their methods.

Inheritance. Methods from a class are inherited by another subclass. Thus, the subclass inherits the behavior of the larger class or, as it is sometimes called, a *superclass*.

Multiple Inheritance. Multiple inheritance is the situation where a class inherits the behavioral characteristics of more than one parent class.

Delegation. Delegation is the forwarding of a request by an object to another object or *delegate*. This forwarding is necessitated by the fact that the object receiving the request does not have a method to service the request.

Polymorphism. According to Booch, “A name may denote objects of many different classes that are related by some common superclass; thus, any object denoted by this name is able to respond to some common set of operations in a different way.”

Polyinstantiation. Polyinstantiation is the development of a detailed version of an object from another object using different values in the new object. In database information security, this term is concerned with the same primary key for different relations at different classification levels being stored in the same database. For example, in a relational database, the name of a military unit may be classified Secret in the database and may have an identification number as the primary key. If another user at a lower classification level attempts to create a confidential entry for another military unit using the same identification number as a primary key, a rejection of this attempt would infer to the lower level user that the same identification number existed at a higher level of classification. To avoid this inference channel of information, the lower level user would be issued the same identification number for their unit and the database management system would manage this situation where the same primary key was used for two different units.

Relative to the software development life cycle phases, object-orientation is applied in different phases as follows:

1. *Object-Oriented Requirements Analysis (OORA)*. Defines classes of objects and their interactions.
2. *Object-Oriented Analysis (OOA)*. In terms of object-oriented concepts, understanding and modeling a particular problem within a problem domain.
3. *Domain Analysis (DA)*. According to Booch, "Whereas OOA typically focuses upon one specific problem at a time, domain analysis seeks to identify the classes and objects that are common to all applications within a given domain."
4. *Object-Oriented Design (OOD)*. Object is the basic unit of modularity; objects are instantiations of a class.
5. *Object-Oriented Programming (OOP)*. Emphasizes the employment of objects and methods rather than types or transformations as in other programming approaches.

A simple example of a class is the class Airplane. From this class, the object called fighter plane can be created. Other objects called passenger plane, cargo plane, and trainer can also be defined as objects in the class Airplane. The method associated with this class would be carried out when the object received a message. The messages to the object could be Climb, Roll, or Descend.

By reusing tested and reliable objects, applications can be developed in less time and at less cost. These objects can be controlled through an object program library that controls and manages the deposit and issuance of tested objects to users. To provide protection from disclosure and violations of the integrity of objects, security controls must be implemented for the program library. In addition, objects can be made available to users through *Object Request Brokers (ORBs)*. ORBs act as the locators and distributors of objects across networks. ORBs are considered *middleware* because they reside between two other entities. ORBs can also provide security features, or the objects can call security services.

The Object Management Group (OMG) has developed a *Common Object Request Broker Architecture (CORBA)*, which defines an industry standard that enables programs written in different languages and using different platforms and operating systems to interface and communicate. To implement this compatible interchange, a user develops a small amount of initial code and an Interface Definition Language (IDL) file. The IDL file then identifies the methods, classes, and objects that are the interface targets. For example, CORBA can enable a Java code to access and use code written in C++.

Another standard, the *Common Object Model (COM)*, supports the exchange of objects among programs. This capability was formerly known as *Object Linking and Embedding (OLE)*. The *Distributed Common Object Model (DCOM)* defines the standard for sharing objects in a networked environment.

Some examples of object-oriented systems are Simula 67, C++, and Smalltalk. Simula 67 was the first system to support object-oriented programming, but was not widely adopted. However, its constructs influenced other object-oriented languages, including C++. C++ supports classes, multiple inheritance, strict type checking, and user controlled management of storage. Smalltalk was developed at the Xerox Palo Alto Research Center (PARC) as a complete system. It supports incremental development of programs and run-time type checking.

Object orientation, thus, provides an improved paradigm that represents application domains through basic component definition and interfacing. It supports the reuse of software (objects), reduces the development risks for complex systems, and is natural in its representation of real world entities.

Artificial Intelligence Systems

An alternative approach for using software and/or hardware to solve problems is through the use of artificial intelligence systems. These systems attempt to mimic the workings of the human mind. Two types of artificial intelligence systems are covered in this section:

- Expert systems
- Neural networks

Expert Systems

An expert system exhibits reasoning similar to that of a human expert to solve a problem. It accomplishes this reasoning by building a knowledge base of the domain to be addressed in the form of rules and an inferencing mechanism to determine if the rules have been satisfied by the system input.

Computer programs are usually defined as

algorithm + data structures = program

In an expert system, the relationship is

inference engine + knowledge base = expert system

The knowledge base contains facts and the rules concerning the domain of the problem in the form of *If-Then* statements. The inference engine compares information it has acquired in memory to the *If* portion of the rules in the knowledge base to see if there is a match. If there is a match, the rule is ready to “fire” and is placed in a list for execution. Certain rules may have a higher priority or *salience*, and the system will fire these rules before others that have a lower salience.

The expert system operates in either a forward chaining or backward chaining mode. In a forward chaining mode, the expert system acquires information and comes to a conclusion based on that information. In a backward chaining mode, the expert system backtracks to determine if a given hypothesis is valid.

As with human reasoning, there is a degree of uncertainty in the conclusions of the expert system. This uncertainty can be handled through a number of approaches such as Bayesian networks, certainty factors, or fuzzy logic.

Bayesian networks are based on Bayes theorem

$$P\{H|E\} = P\{E|H\} * P(H) / P(E)$$

that gives the probability of an event (H) given that an event (E) has occurred.

Certainty factors are easy to develop and use. These factors are the probability that a belief is true. For example, a probability of 85 percent can be assigned to Object A occurring under certain conditions.

Fuzzy logic is used to address situations where there are degrees of uncertainty concerning whether something is true or false. This situation is often the case in real world situations. A fuzzy expert system incorporates fuzzy functions to develop conclusions. The inference engine steps in fuzzy logic are as follows:

- *Fuzzification.* The membership functions defined on the input variables are applied to their actual values, to determine the degree of truth for each rule premise.
- *Inference.* The truth value for the premise of each rule is computed, and applied to the conclusion part of each rule. This results in one fuzzy subset to be assigned to each output variable for each rule.
- *Composition.* All of the fuzzy subsets assigned to each output variable are combined together to form a single fuzzy subset for each output variable.
- *Defuzzification.* Used when it is useful to convert the fuzzy output set to a quantitative number.

The Spiral model can be used to build an expert system. The following are the common steps when building a Spiral model:

- Analysis
- Specification
- Development
- Deployment

A key element in this process is the acquisition of knowledge. This activity involves interviewing experts in the domain field and obtaining data from other expert sources. Knowledge acquisition begins in the specification phase and runs into the development phase.

Verification and validation of an expert system are concerned with inconsistencies inherent in conflicting rules, redundant rules, circular chains of rules, and unreferenced values along with incompleteness resulting from unreferenced or unallowable data values.

Neural Networks

A neural network is based on the functioning of biological neurons. In biological neurons, signals are exchanged among neurons through electrical pulses traveling along an *axon*. The electrical pulses arrive at a neuron at points called *synapses*. When a pulse arrives at the synapse, it causes the release of a chemical neurotransmitter that travels across the synaptic cleft to the post-synaptic receptor sites on the dendrite side of the synapse. The neurotransmitter then causes a change in the dendrite membrane post-synaptic-potential (PSP). These PSPs are integrated by the neuron over time. If the integrated PSPs exceed a threshold, the neuron fires and generates an electrical pulse that travels to other neurons.

An analog of the biological neuron system is provided in Figure 7.7. Inputs \downarrow to the neuron are modified by weights, W_i , and then summed in unit S. If the weighted sum exceeds a threshold, unit S will produce an output, Z. The functioning of this artificial neural network is shown in the following equation

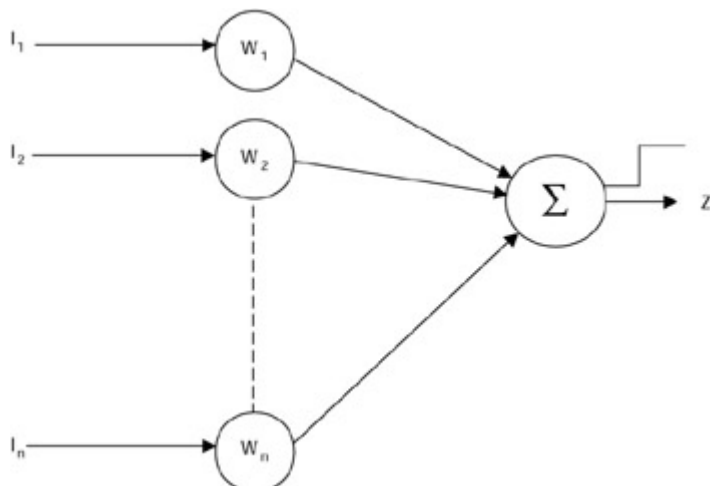


Figure 7.7: A single layer artificial neural network.

$$z = W_1 I_1 + W_2 I_2 + \dots + W_n I_n$$

If the sum of the weighted inputs then exceeds the threshold, the neuron will “fire” and there will be an output from that neuron. An alternative approach would be to have the output of the neuron be a linear function of the sum of the artificial neuron inputs.

Because there is only one summing node in Figure 7.7, this network is called a single-layer network. Networks with more than one level of summing nodes are called multi-layer networks. The value of a neural network is its ability to dynamically adjust its weights in order to associate the given input vectors with corresponding output vectors. A “training” period for the neural network has the input vectors repeatedly presented and the weights dynamically adjusted according to the learning paradigm. The delta rule is an example of a learning rule. In the delta rule, the change in weight, $\Delta w_{ij} = R * I_j * (T_j - Z_j)$ where R is the learning rate, I_j is the input vector, T_j is the target output vector, and Z_j is the actual output of node S . For example, if a specific output vector was required for a specific input where the relationship between input and output was non-linear, the neural network would be trained by applying a set of input vectors. Using the delta rule, the neural network would repetitively adjust the weights until it produced the correct output vector for each given input vector. The neural network would then be said to have learned to provide the correct response for each input vector.

Database Systems

A database system can be used as a general mechanism for defining, storing, and manipulating data without writing specific programs to perform these functions. A Database Management System (DBMS) provides high-level commands to operate on the data in the database. Some of the different types of databases are as follows:

- Hierarchical
- Mesh
- Object-oriented
- Relational

Much research on information security has been done with relational databases. The information security applications of relational databases are discussed in Chapter 2, “Access Control Systems.”

Database Security Issues

In a relational database, security can be provided through the use of *views*. A view is a virtual relation that combines information from other relations. A view can be used to restrict the data made available to users based on their privileges and need to know. A database information security vulnerability may be exploited through the DBMS.

Designed to facilitate queries to the database, the DBMS, can be a possible source of data compromise by circumventing the normal security controls. The *granularity* of the access to objects in a database refers to the “fineness” in which this access can be controlled or limited. Other database security issues are *aggregation* and *inference*. Aggregation is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity. Inference is the ability of users to infer or deduce information about data at sensitivity levels for which they do not have access privileges. A link that enables inference to occur is called an *inference channel*.

Open Database Connectivity (ODBC) is a Microsoft-developed standard for supporting access to databases through different applications. This access must be controlled to avoid compromising the database.

Data Warehouse and Data Mining

A data warehouse is a repository of information from heterogeneous databases that is available to users for making queries. Data in the data warehouse is *normalized* — redundant data is removed. Thus, data in the warehouse is extracted and refined, and it is available for access and analysis. The objective is to find relationships that were unknown up until now among the data in the warehouse. This searching for data correlations in the data warehouse is called *data mining*. The correlations or “data about data” are referred to as *metadata*. Normally, the extracted metadata is not stored in the warehouse. It is stored in another system with high levels of protection called a *data mart*. The information obtained from the metadata should, however, be sent back for incorporation into the data warehouse to be available for future queries and metadata analyses.

Data mining can be applied to information system security as an intrusion detection tool to discover abnormal system characteristics, in order to determine if there are aggregation or inference problems and for analyzing audit information.

Data Dictionaries

A data dictionary is a database for system developers. It records all the data structures used by an application. Advanced data dictionaries incorporate application generators that use the data stored in the dictionary to automate some of the program production tasks. The data dictionary interacts with the DBMS, the program library, applications, and the information security system. In some instances, the data dictionary system is organized into a primary data dictionary and one or more secondary data dictionaries. The primary data dictionary provides a baseline of data definitions and central control while the secondary data dictionaries are assigned to separate development projects, to provide backup to the primary dictionary, and to serve as a partition between the development and test databases.

Application Controls

The goal of application controls is to enforce the organization’s security policy and procedures and to maintain the confidentiality, integrity, and availability of the computer-based information. Application security involves the input to the system, the data being processed, and the output of the system. The controls can be classified into preventive, detective, and corrective measures that apply to different security categories. These controls and categories are listed in Table 7.1.

Table 7.1: Application Control Types

Application Control Type	Accuracy	Security	Consistency
Preventive	Data checks, forms, custom screens, validity checks, contingency planning, and backups.	Firewalls, reference monitors, sensitivity labels, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments	Data dictionary, programming standards, and database management system.
Detective	Cyclic redundancy checks, structured walk-throughs, hash totals, and reasonableness checks.	Intrusion detection systems and audit trails.	Comparison controls, relationship tests, and reconciliation controls.
Corrective	Backups, control reports, before/after imaging reporting, and checkpoint restarts.	Emergency response and reference monitor controls.	Program comments and database

Users running applications require the availability of the system. A *service level agreement* guarantees the quality of a service to a subscriber by a network service provider. Defined service levels provide a basis for measuring the delivered services and are useful in anticipating, identifying, and correcting problems. Some of the metrics in service level agreements are

- Turn-around times

- Average response times
- Number of on-line users
- System utilization rates
- System up-times
- Volume of transactions
- Production problems

Distributed Systems

Distributed systems are commonplace and pose special challenges to information systems security implementation. Security in distributed systems should include access control mechanisms, identification, authentication, some type of intrusion detection capability, emergency response plans, logs, and audit trails.

The client/server model implements a type of distributed system. In this model, the client requests services and the server provides the requested service. The client provides the interface to the user, supports the entry of information, and provides the reports. The server provides access to data, holds the databases, provides data to the client, performs backups, and provides security services.

Distributed environments support agents. An *agent* is a surrogate program or process performing services in one environment on behalf of a principal in another environment. This behavior differs from that of a *proxy* in that a proxy acts on behalf of a principal, but it may hide the characteristics of that principal. Similarly, *applets* are small applications that may be written in various languages, which include C++ and Java. Both of these languages are object-oriented. C++ was developed at Bell Laboratories and is an extension of C. Java is a multithreaded, interpreted language that was developed at Sun Microsystems. A *thread* is considered a “lightweight” process and has a lower overhead for maintaining state and switching contexts. *Multiple threads* run in the protection domain of a task or process, and they share a single address space. An *interpreted* language executes each instruction in real-time. This action is referred to as *run-time binding*. A *compiled* language has all the high-level instructions translated into machine code (object code) by a compiler. Then, the computer executes the code. With a compiler, *the binding occurs at compile time*. Compiled code poses more of a security risk than interpreted code because malicious code can be embedded in the compiled code and can be difficult to detect.

Applets can be accessed and downloaded from the World Wide Web (WWW) into a web browser such as Netscape. This applet can execute in the network browser and may contain malicious code. These types of downloadable programs are also known as *mobile code*. Java code is designed to run in a constrained space in the client web browser called a *sandbox* for protection of the system. The Microsoft ActiveX environment also supports the downloading of mobile code written in a language such as Visual BASIC or C++ to web browsers and, thus, has the potential for causing harm to a system. ActiveX, however, establishes a trust relationship between the client and the server through the use of digital certificates guaranteeing that the server is trusted. Some security controls that can be applied to mitigate the effects of malicious mobile code are as follows:

- Configure firewalls to screen applets
- Configure web browsers to restrict or prevent the downloading of applets
- Configure web browsers to only permit the receipt of applets from trusted servers
- Provide training to users to make them aware of mobile code threats

Centralized Architecture

A centralized system architecture is less difficult to protect than a distributed system architecture because, in the latter, the components are interconnected through a network. Centralized systems provide for implementation of the local security and application system controls, whereas distributed systems have to deal with geographically separate entities communicating via a network or through many networks.

Real-Time Systems

Another system classification that is based on temporal considerations rather than on architectural characteristics is real-time systems. Real-time systems operate by acquiring data from transducers or sensors in real time, and then making computations and control decisions in a fixed time window. An example of such a system would be a “fly by wire” control of supersonic aircraft where adjustment of the planes’ control surfaces is time-critical. Availability of such systems is crucial, and, as such, can be addressed through *Redundant Array of Independent Disks (RAID)* technology, disk mirroring, disk duplexing, fault-tolerant systems, and recovery mechanisms to cope with system failures. In *disk mirroring*, a duplicate of the disk is used and in *disk duplexing*, the disk controller is backed up with a redundant controller. A *fault-tolerant* system has to detect a fault and then take action to recover from that fault.

Sample Questions

1. What is a data warehouse? ?
 - A. A remote facility used for storing backup tapes
 - B. A repository of information from heterogeneous databases
 - C. A table in a relational database system
 - D. A hot backup building
2. What does normalizing data in a data warehouse mean? ?
 - A. Redundant data is removed.
 - B. Numerical data is divided by a common factor.
 - C. Data is converted to a symbolic representation.
 - D. Data is restricted to a range of values.
3. What is a neural network? ?
 - A. A hardware or software system that emulates the reasoning of a human expert
 - B. A collection of computers that are focused on medical applications
 - C. A series of networked PCs

- performing artificial intelligence tasks
- D. A hardware or software system that emulates the functioning of biological neurons
4. A neural network learns by using various algorithms to ?
- A. Adjust the weights applied to the data
- B. Fire the rules in knowledge base
- C. Emulate an inference engine
- D. Emulate the thinking of an expert
5. The SEI Software Capability Maturity Model is based on the premise that ?
- A. Good software development is a function of the number of expert programmers in the organization.
- B. The maturity of an organization's software processes cannot be measured.
- C. The quality of a software product is a direct function of the quality of its associated software development and maintenance processes.
- D. Software development is an art that cannot be measured by conventional means.
6. In configuration management, a configuration item is ?
- A. The version of the operating system, which is operating on the work station, that provides information security services
- B. A component whose state is to be recorded and against which changes are to be progressed
- C. The network architecture used by the organization
- D. A series of files that contain sensitive information
7. In an object-oriented system, polymorphism denotes ?
- A. Objects of many different

classes that are related by some common superclass; thus, any object denoted by this name is able to respond to some common set of operations in a different way

- B. Objects of many different classes that are related by some common superclass; thus, all objects denoted by this name are able to respond to some common set of operations in identical fashion
- C. Objects of the same class; thus, any object denoted by this name is able to respond to some common set of operations in the same way
- D. Objects of many different classes that are unrelated, but respond to some common set of operations in the same way

8. The simplistic model of software life cycle development assumes that

?

- A. Iteration will be required among the steps in the process.
- B. Each step can be completed and finalized without any effect from the later stages that may require rework.
- C. Each phase is identical to a completed milestone.
- D. Software development requires reworking and repeating some of the phases.

9. What is a method in an object-oriented system?

?

- A. The means of communication among objects
- B. A guide to programming of objects
- C. The code defining the actions that the object performs in response to a message
- D. The situation where a class inherits the behavioral characteristics of more than one parent class

10. What does the Spiral Model depict? ?
- A. A spiral that incorporates various phases of software development
 - B. A spiral that models the behavior of biological neurons
 - C. The operation of expert systems
 - D. Information security checklists
11. In the software life cycle, verification ?
- A. Evaluates the product in development against real world requirements
 - B. Evaluates the product in development against similar products
 - C. Evaluates the product in development against general baselines
 - D. Evaluates the product in development against the specification
12. In the software life cycle, validation ?
- A. Refers to the work product satisfying the real-world requirements and concepts
 - B. Refers to the work product satisfying derived specifications
 - C. Refers to the work product satisfying software maturity levels
 - D. Refers to the work product satisfying generally accepted principles
13. In the modified Waterfall Model ?
- A. Unlimited backward iteration is permitted.
 - B. The model was reinterpreted to have phases end at project milestones.
 - C. The model was reinterpreted to have phases begin at project milestones.
 - D. Product verification and validation are not included.
14. Cyclic redundancy checks, structured walk- ?

throughs, and hash totals are examples of what type of application controls?

- A. Preventive security controls
- B. Preventive consistency controls
- C. Detective accuracy controls
- D. Corrective consistency controls

15. In a system life cycle, information security controls should be ?
- A. Designed during the product implementation phase
 - B. Implemented prior to validation
 - C. Part of the feasibility phase
 - D. Specified after the coding phase
16. The software maintenance phase controls consist of ?
- A. Request control, change control, and release control
 - B. Request control, configuration control, and change control
 - C. Change control, security control, and access control
 - D. Request control, release control, and access control
17. In configuration management, what is a software library? ?
- A. A set of versions of the component configuration items
 - B. A controlled area accessible only to approved users who are restricted to the use of an approved procedure
 - C. A repository of backup tapes
 - D. A collection of software build lists
18. What is configuration control? ?
- A. Identifying and documenting the functional and physical characteristics of each configuration item
 - B. Controlling changes to the configuration items and issuing versions of configuration items from the software library

- C. Recording the processing of changes
- D. Controlling the quality of the configuration management procedures
19. What is searching for data correlations in the data warehouse called? ?
- A. Data warehousing
- B. Data mining
- C. A data dictionary
- D. Configuration management
20. The security term that is concerned with the same primary key existing at different classification levels in the same database is ?
- A. Polymorphism
- B. Normalization
- C. Inheritance
- D. Polyinstantiation
21. What is a data dictionary? ?
- A. A database for system developers
- B. A database of security terms
- C. A library of objects
- D. A validation reference source
22. Which of the following is an example of mobile code? ?
- A. Embedded code in control systems
- B. Embedded code in PCs
- C. Java and ActiveX code downloaded into a web browser from the World Wide Web (WWW)
- D. Code derived following the spiral model
23. Which of the following is NOT true regarding software unit testing? ?
- A. The test data is part of the specifications.
- B. Correct test output results should be developed and known beforehand.
- C. Live or actual field data is recommended for use in the testing procedures.

D. Testing should check for out-of-range values and other bounds conditions.

Answers

1. *Answer:* b). A repository of information from heterogeneous databases. Answers a and d describe physical facilities for backup and recovery of information systems and answer c describes a relation in a relational database.
2. *Answer:* a). Removing redundant data.
3. *Answer:* d). A neural network is a hardware or software system that emulates the functioning of biological neurons. Answer a) refers to an expert system and answers b) and c) are distractors.
4. *Answer:* a). A neural network learns by using various algorithms to adjust the weights applied to the data. Answers b), c) and d) are terminology referenced in expert systems.
5. *Answer:* c). The quality of a software product is a direct function of the quality of its associated software development and maintenance processes. Answer a) is false since the SEI Software CMM relates the production of good software to having the proper processes in place in an organization and not to expert programs or heroes. Answer b) is false since the Software CMM provides means to measure the maturity of an organization's software processes. Answer d) is false for the same reason as answer b).
6. *Answer:* b). A component whose state is to be recorded and against which changes are to be progressed. Answers a), c), and d) are incorrect by the definition of a configuration item.
7. *Answer:* a). Objects of many different classes that are related by some common superclass that are able to respond to some common set of operations in a different way. Answers b), c), and d) are incorrect by the definition of polymorphism.
8. *Answer:* b). Each step can be completed and finalized without any affect from the later stages that might require rework. Answer a) is incorrect since no iteration is allowed for in the model. Answer c is incorrect since it applies to the modified Waterfall model. Answer d) is incorrect since no iteration or reworking is considered in the model.
9. *Answer:* c). A method in an object-oriented system is the code that defines the actions that the object performs in response to a message. Answer a) is incorrect since it defines a message. Answer b) is a distractor and answer d) refers to multiple inheritance.
10. *Answer:* a). A spiral that incorporates various phases of software development. The other answers are distractors.
11. *Answer:* d). In the software life cycle, verification evaluates the product in development against the specification. Answer a) defines validation. Answers b) and c) are distractors.
12. *Answer:* a) In the software life cycle, validation is the work product satisfying the real-world requirements and concepts.

- The other answers are distractors.
- 13.** *Answer:* b). The modified Waterfall model was reinterpreted to have phases end at project milestones. Answer a) is false since unlimited backward iteration is not permitted in the modified Waterfall model. Answer c) is a distractor and answer d) is false since verification and validation are included.
- 14.** *Answer:* c). Cyclic redundancy checks, structured walk-throughs and hash totals are examples of detective accuracy controls. The other answers do not apply by the definition of the types of controls.
- 15.** *Answer:* c). In the system life cycle, information security controls should be part of the feasibility phase. The other answers are incorrect since the basic premise of information system security is that controls should be included in the earliest phases of the software life cycle and not added later in the cycle or as an afterthought.
- 16.** *Answer:* a). The software maintenance phase controls consist of request control, change control and release control by definition. The other answers are, therefore, incorrect.
- 17.** *Answer:* b). In configuration management, a software library is a controlled area accessible only to approved users who are restricted to the use of approved procedure. Answer a) is incorrect since it defines a build list. Answer c) is incorrect since it defines a backup storage facility. Answer d) is a distractor.
- 18.** *Answer:* b). Configuration control is controlling changes to the configuration items and issuing versions of configuration items from the software library. Answer a is the definition of configuration identification. Answer c is the definition of configuration status accounting and answer d is the definition of configuration audit.
- 19.** *Answer:* b). Searching for data correlations in the data warehouse is called data mining. Answer a) is incorrect since data warehousing is creating a repository of information from heterogeneous databases that is available to users for making queries. Answer c) is incorrect since a data dictionary is a database for system developers. Answer d) is incorrect since configuration management is the discipline of identifying the components of a continually evolving system for the purposes of controlling changes to those components and maintaining integrity and traceability throughout the life cycle.
- 20.** *Answer:* d). The security term that is concerned with the same primary key existing at different classification levels in the same database is polyinstantiation. Answer a) is incorrect since polymorphism is defined as objects of many different classes that are related by some common superclass; thus, any object denoted by this name is able to respond to some common set of operations in a different way. Answer b) is incorrect since normalization refers to removing redundant or incorrect data from a database. Answer c is incorrect since inheritance refers to methods from a class inherited by another subclass.

- 21.** *Answer:* a). A data dictionary is a database for system developers. Answers b), c), and d) are distractors.
- 22.** *Answer:* c). An example of mobile code is Java and ActiveX code downloaded into a web browser from the World Wide Web. Answers a), b), and d) are incorrect since they are types of code that are not related to mobile code.
- 23.** *Answer:* c), live or actual field data are NOT recommended for use in testing since they do not thoroughly test all normal and abnormal situations and the test results are not known beforehand. Answers a), b), and d), are true of testing.

Chapter 8: Business Continuity Planning and Disaster Recovery Planning

Overview

The Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) domain is all about business. We're not talking about infringements of security policy or unauthorized access; this is about making contingency plans for a business-threatening emergency and continuing the business in the event of a disaster. While the other domains are concerned with preventing risks and protecting the infrastructure against attack, this domain assumes the worst has happened. It is really two domains in one: BCP is about making the plans and creating the framework to ensure that the business can continue in an emergency; DRP is about quickly recovering from an emergency with the minimum of impact to the organization.

From the published (ISC)² goals for the Certified Information Systems Security Professional candidate:

“The candidate will be expected to know the difference between business continuity planning and disaster recovery; business planning in terms of project scope and planning, business impact analysis, recovery strategies, recovery plan development, and implementation. The candidate should understand disaster recovery in terms of recovery plan development, implementation and restoration.”

Our Goals

The CISSP candidate should know the following:

- The basic difference between BCP and DRP
- The difference between natural and man-made disasters
- The four prime elements of BCP
- The reasons for and steps in conducting a Business Impact Assessment (BIA)
- The steps in creating a disaster recovery plan
- The five types of disaster recovery plan tests
- The various types of backup services

We have divided the chapter into two sections, BCP and DRP. Many elements of BCP are also applicable to DRP; we will try to not be too redundant.

Domain Definition

The BCP and DRP domain addresses the preservation of business in the face of major disruptions to normal operations. Business Continuity Planning and Disaster Recovery Planning involve the preparation, testing, and updating of the actions required to protect critical business processes from the effects of major system and network failures. The CISSP candidate must have an understanding of the preparation of specific actions required to preserve the business in the event of a major disruption to normal business operations.

The BCP process includes the following:

- Scope and plan initiation
- Business Impact Assessment (BIA)
- Business continuity plan development

The DRP process includes the following:

- Disaster Recovery Planning (DRP) processes
- Testing the disaster recovery plan
- Disaster recovery procedures

So What Is the Difference?

Obviously, these two concepts are so close as to allow combining them into one domain. There are some differences, however. Basically, business continuity planning is the process of making the plans that will ensure that critical business functions can withstand a variety of emergencies. Disaster recovery planning involves making preparations for a disaster, but also addresses the procedures to be followed during and after a loss.

Business Continuity Planning

Simply put, business continuity plans are created to prevent interruptions to normal business activity. They are designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes. Business continuity planning is a strategy to minimize the effect of disturbances and to allow for resumption of business processes.

A disruptive event is any intentional or unintentional security violation that suspends normal operations. The aim of BCP is to minimize the effects of a disruptive event on a company. The primary purpose of business continuity plans are to reduce the risk of financial loss and enhance a company's ability to recover from a disruptive event promptly. The business continuity plan should also help minimize the cost associated with the disruptive event and mitigate the risk associated with it.

Business continuity plans should look at all critical information processing areas of the company, including but not limited to:

- Local and wide area networks and servers
- Telecommunications and data communication links
- Workstations and workspaces
- Applications, software, and data
- Media and records storage
- Staff duties and production processes

Note The Number-One Priority of Disaster Planning

The number-one priority of all business continuity and disaster planning is always this: people first. While we talk about preservation of capital, resumption of normal business processing activities, and other business continuity issues, the main overriding concern of all plans is to get the personnel out of harm's way. If there is at any time a conflict between preserving hardware or data and the threat of physical danger to personnel, the protection of the people always comes first. Personnel evacuation and safety must be the first element of a disaster response plan.

Continuity Disruptive Events

The events that can affect business continuity and require disaster recovery are well documented in the Physical Security domain. Here we are concerned with those events, either natural or man-made, that are of such a substantial nature as to pose a threat to the continuing existence of the organization. All of the plans and processes in this section are “after the fact,” that is, no preventative controls similar to the controls discussed in the Operations Security domain will be demonstrated here. Business continuity plans are designed to minimize the damage done by the event, and facilitate rapid restoration of the organization to its full operational capability.

We can make a simple list of these events, categorized as to whether their origination was natural or human. Examples of natural events that can affect business continuity are as follows:

- Fires, explosions, or hazardous material spills of environmental toxins
- Earthquakes, storms, floods, and fires due to acts of nature
- Power outages or other utility failures

Examples of man-made events that can affect business continuity are as follows:

- Bombings, sabotage, or other intentional attacks
- Strikes and job actions
- Employee or operator unavailability due to emergency evacuation or other issues (these could be either man-made or naturally caused)
- Communications infrastructure failures or testing-related outages (including a massive failure of configuration management controls)

The Four Prime Elements of BCP

There are four major elements of the BCP process:

- *Scope and Plan Initiation.* This phase marks the beginning of the BCP process. It entails creating the scope and the other elements needed to define the parameters of the plan.
- *Business Impact Assessment.* A BIA is a process used to help business units understand the impact of a disruptive event. This phase includes the execution of a vulnerability assessment.
- *Business Continuity Plan Development.* This refers to using the information collected in the BIA to develop the actual business continuity plan. This includes the areas of plan implementation, plan testing, and ongoing plan maintenance.
- *Plan Approval and Implementation.* This involves getting the final senior management sign-off, creating enterprise-wide awareness of the plan, and implementing a maintenance procedure for updating the plan as needed.

Scope and Plan Initiation

The Scope and Plan Initiation phase is the first step to creating a business continuity plan. This phase marks the beginning of the BCP process. It entails creating the scope for the plan and the other elements needed to define the parameters of the plan. This phase embodies an examination of the company’s operations and support services. Scope activities could include: creating a detailed account of the work required, listing the resources to be used, and defining the management practices to be employed.

Note Distributed Processing Issues

With the advent of the personal computer in the workplace, distributed processing introduces special problems into the BCP process. It's important that the centralized planning effort encompass all distributed processes and systems.

Roles and Responsibilities

The BCP process involves many personnel from various parts of the enterprise. Creation of a BCP committee will represent the first enterprise-wide involvement of the major critical functional business units. All other business units will be involved in some way later, especially during the implementation and awareness phases.

The BCP Committee. A BCP committee should be formed and given the responsibility to create, implement, and test the plan. The committee is made up of representatives from senior management, all functional business units, information systems, and security administration. The committee initially defines the scope of the plan, which should deal with how to recover promptly from a disruptive event and mitigate the financial and resource loss due to a disruptive event.

Senior Management's Role. Senior management has the ultimate responsibility for all phases of the plan. This includes not only initiation of the plan process, but also monitoring and management of the plan during testing, and supervision and execution of the plan during a disruptive event. This support is essential, and without management being willing to commit adequate tangible and intangible resources, the plan will not be successful.

Because of the concept of due diligence, stockholders may hold senior managers as well as the board of directors personally responsible if a disruptive event causes losses that adherence to base industry standards of due care could have prevented. For this and other reasons, it is in the senior managers' best interest to be fully involved in the BCP process.

Also, many elements of the BCP will address senior management, such as the statement of importance and priorities, the statement of organizational responsibility, and the statement of urgency and timing. Table 8.1 shows the roles and responsibilities in the BCP process.

Who	Does What
Executive management staff	Initiates the project, gives final approval, and gives ongoing support.
Senior business unit management	Identifies and prioritizes time-critical systems.
BCP committee	Directs the planning, implementation, and test processes.
Functional business units	Participate in implementation and testing.

Note Senior corporate executives are increasingly being held liable for failure of “due care” in disasters. They can also face civil suits from shareholders and clients for compensatory damages. The definition of “due care” is being updated to include computer functionality outages, as more and more people around the world depend upon data information to do their jobs.

Business Impact Assessment

The purpose of a BIA is to create a document to be used to help understand what impact a disruptive event would have on the business. The impact may be financial (quantitative), or operational (qualitative, such as the inability to respond to customer complaints). A *vulnerability assessment* is often part of the BIA process.

BIA has three primary goals:

- *Criticality Prioritization.* Every critical business unit process must be identified and prioritized, and the impact of a disruptive event must be evaluated. Obviously, non-time-critical business processes will require a lower priority rating for recovery than time-critical business processes.
- *Downtime Estimation.* The BIA is used to help estimate the Maximum Tolerable Downtime (MTD) that the business can tolerate and still remain a viable company; that is, what is the longest period of time a critical process can remain interrupted before the company can never recover. It is often found during the BIA process that this time period is much shorter than expected, that is, the company can only tolerate a much briefer period of interruption than was previously thought.
- *Resource Requirements.* The resource requirements for the critical processes are also identified at this time, with the most time-sensitive processes receiving the most resource allocation.

A BIA generally takes the form of these four steps:

- Gathering the needed assessment materials
- Performing the vulnerability assessment
- Analyzing the information compiled
- Documenting the results and presenting recommendations

The FCPA

The Foreign Corrupt Practices Act of 1977 imposes civil and criminal penalties if publicly held organizations fail to maintain adequate controls over their information systems. Organizations must take reasonable steps to ensure not only the integrity of their data, but also the system controls the organization put in place.

Gathering Assessment Materials

The initial step of the BIA is identifying which business units are critical to continuing an acceptable level of operations. Often the starting point is a simple organizational chart that shows the business units' relationships to each other. Other documents may also be collected at this stage in an effort to define the functional interrelationships of the organization.

As the materials are collected and the functional operations of the business are identified, the BIA will examine these business function interdependencies with an eye

toward several factors, such as the business success factors involved, establishing a set of priorities between the units, and what alternate processing procedures can be utilized.

The Vulnerability Assessment

The vulnerability assessment is often part of a BIA. It is similar to a Risk Assessment in that there is a quantitative (financial) section and a qualitative (operational) section. It differs in that it is smaller than a full risk assessment and is focused on providing information that is used solely for the business continuity plan or disaster recovery plan.

A function of a vulnerability assessment is to conduct a loss impact analysis. Because there will be two parts to the assessment, a financial assessment and an operational assessment, it will be necessary to define loss criteria both quantitatively and qualitatively.

Quantitative loss criteria may be defined as follows:

- Incurring financial losses from loss of revenue, capital expenditure, or personal liability resolution
- The additional operational expenses incurred due to the disruptive event
- Incurring financial loss from resolution of violation of contract agreements
- Incurring financial loss from resolution of violation of regulatory or compliance requirements

Qualitative loss criteria may consist of the following:

- The loss of competitive advantage or market share
- The loss of public confidence or credibility, or incurring public embarrassment

During the vulnerability assessment, *critical support areas* must be defined in order to assess the impact of a disruptive event. A critical support area is defined as a business unit or function that must be present to sustain continuity of the business processes, maintain life safety, or avoid public relations embarrassment.

Critical support areas could include the following:

- Telecommunications, data communications, or information technology areas
- Physical infrastructure or plant facilities, transportation services
- Accounting, payroll, transaction processing, customer service, purchasing

The granular elements of these critical support areas will also need to be identified. By granular elements we mean the personnel, resources, and services the critical support areas need to maintain business continuity.

Analyzing the Information

During the analysis phase of the BIA, several activities take place, such as documenting required processes, identifying interdependencies, and determining what an acceptable interruption period would be.

The goal of this section is to clearly describe what support the defined critical areas will require to preserve the revenue stream and maintain pre-defined processes, such as transaction processing levels and customer service levels. Therefore, elements of the analysis will have to come from many areas of the enterprise.

Documentation and Recommendation

The last step of the BIA entails a full documentation of all of the processes, procedures, analysis, and results, and the presentation of recommendations to the appropriate senior management.

The report will contain the previously gathered material, list the identified critical support areas, summarize the quantitative and qualitative impact statements, and provide the recommended recovery priorities generated from the analysis.

Business Continuity Plan Development

Business Continuity Plan development refers to using the information collected in the BIA to create the recovery strategy plan to support these critical business functions. Here we take the information gathered from the BIA and begin to map out a strategy for creating a continuity plan.

This phase consists of two main steps:

- Defining the continuity strategy
- Documenting the continuity strategy

The Criticality Survey

A criticality survey is another term for a standardized questionnaire or survey methodology, such as the InfoSec Assessment Method (IAM) promoted by the federal government's National Security Agency (NSA), or it could be a subset of the Security Systems Engineering Capability Maturity Model (SSE-CMM; see Appendix D). Its purpose is to help identify the most critical business functions by gathering input from management personnel in the various business units. Also, it's very important to obtain senior executive management buy-in and support for the survey, as it requires full disclosure from the business units and a high-level organizational view.

The Information Technology Department

The Information Technology (IT) department plays a very important role in identifying and protecting the company's internal and external information dependencies. Also, the information technology elements of the BCP should address several vital issues, including:

- Ensuring that the organization employs an adequate data backup and restoration process, including off-site media storage
- Ensuring that the company employs sufficient physical security mechanisms to preserve vital network and hardware components, including file and print servers
- Ensuring that the organization uses sufficient logical security methodologies (authentication, authorization, etc.) for sensitive data
- Ensuring that the department implements adequate system administration, including up-to-date inventories of hardware, software, and media storage

Defining the Continuity Strategy

To define the BCP strategy, the information collected from the BIA is used to create a continuity strategy for the enterprise. This is a large task, and many elements of the enterprise must be included in defining the continuity strategy, such as:

- *Computing.* A strategy needs to be defined to preserve the elements of hardware, software, communication lines, applications, and data.
- *Facilities.* The strategy needs to address the use of the main buildings or campus and any remote facilities.
- *People.* Operators, management, and technical support personnel will have defined roles in implementing the continuity strategy.
- *Supplies and equipment.* Paper, forms, HVAC, or specialized security equipment must be defined as they apply to the continuity plan.

Documenting the Continuity Strategy

Documenting the continuity strategy simply refers to the creation of documentation of the results of the continuity strategy definition phase. You will see “documentation” a lot in this chapter. Documentation is required in almost all sections, and it is the nature of BCP/DRP to require a lot of paper.

Plan Approval and Implementation

As the last step, the Business continuity plan is implemented. The plan itself must contain a roadmap for implementation. Implementation here doesn’t mean executing a disaster scenario and testing the plan, but rather it refers to the following steps:

1. Approval by senior management.
2. Creating an awareness of the plan enterprise-wide.
3. Maintenance of the plan, including updating when needed.

Senior Management Approval. As previously mentioned, senior management has the ultimate responsibility for all phases of the plan. Because they have the responsibility for supervision and execution of the plan during a disruptive event, they must have final approval. When a disaster strikes, senior management must be able to make informed decisions quickly during the recovery effort.

Plan Awareness. Enterprise-wide awareness of the plan is important. There are several reasons for this, including the fact that the capability of the organization to recover from an event will most likely depend on the efforts of many individuals. Also, employee awareness of the plan will emphasize the organization’s commitment to its employees. Specific training may be required for certain personnel to carry out their tasks, and quality training is perceived as a benefit that increases the interest and the commitment of personnel in the BCP process.

Plan Maintenance. Business continuity plans often get out of date: a major similarity among recovery plans is how quickly they become obsolete, for many different reasons. The company may reorganize and the critical business units may be different than when the plan was first created. Most commonly, the network or computing infrastructure changes, including the hardware, software, and other components. The reasons may be administrative: cumbersome plans are not easily updated, personnel lose interest or forget, or employee turnover may affect involvement.

Whatever the reason, plan maintenance techniques must be employed from the outset to ensure that the plan remains fresh and usable. It’s important to build maintenance procedures into the organization by using job descriptions that centralize responsibility for updates. Also, create audit procedures that can report regularly on the state of the plan. It’s also important to ensure that multiple versions of the plan do not exist, because it could create confusion during an emergency. Always replace older versions of the text with updated versions throughout the enterprise when a plan is changed or replaced.

Disaster Recovery Planning

A *disaster recovery plan* is a comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss of information systems resources. Disaster Recovery Plans are the procedures for responding to an emergency, providing extended backup operations during the interruption, and managing recovery and salvage processes afterwards, should an organization experience a substantial loss of processing capability.

The primary objective of the disaster recovery plan is to provide the capability to implement critical processes at an alternate site and return to the primary site and normal processing within a time frame that minimizes the loss to the organization, by executing rapid recovery procedures.

Note It's possible that an organization may not need a disaster recovery plan. While every company may have business units that can withstand lengthy interruptions, perhaps it has been determined that the organization does not have any critical processing areas that require any sort of disaster recovery. In that case, a disaster recovery plan may not need to be implemented; however, we have yet to see a company that doesn't need some type of a contingency plan.

Goals and Objectives of DRP

A major goal of DRP is to provide an organized way to make decisions if a disruptive event occurs. The purpose of the disaster recovery plan is to reduce confusion and enhance the ability of the organization to deal with the crisis.

Obviously, when a disruptive event occurs, the organization will not have the luxury to create and execute a recovery plan on the spot. Therefore, the amount of planning and testing that can be done beforehand will determine the ability of the organization to withstand a disaster.

The objectives of the DRP are multiple but each is important. They can include the following:

- Protecting an organization from major computer services failure
- Minimizing the risk to the organization from delays in providing services
- Guaranteeing the reliability of standby systems through testing and simulation
- Minimizing the decision-making required by personnel during a disaster

In this section, we will examine the following areas of DRP:

- The DRP process
- Testing the disaster recovery plan
- Disaster recovery procedures

The Disaster Recovery Planning Process

This phase involves the development and creation of the recovery plans, which are similar to the BCP process. However, in BCP we were involved in BIA and loss criteria for identifying the critical areas of the enterprise that the business requires to sustain continuity and financial viability; here, we're assuming that those identifications have been made and the rationale has been created. Now we're defining the steps we will need to perform to protect the business in the event of an actual disaster.

The steps in the disaster planning process phase are as follows:

- *Data Processing Continuity Planning*. Planning for the disaster and creating the plans to cope with it.
- *Data Recovery Plan Maintenance*. Keeping the plans up-to-date and relevant.

Disaster Recovery Plan Software Tools

There are several vendors that distribute automated tools to create disaster recovery plans. These tools can improve productivity by providing formatted templates customized to the particular organization's needs. Some vendors also offer specialized recovery software focused on a particular type of business or vertical market. Links to these vendors can be found at www.isc2.org.

Data Processing Continuity Planning

The various means of processing backup services are all important elements to the disaster recovery plan. Here we look at the most common alternate processing types:

- Mutual aid agreements
- Subscription services
- Multiple centers
- Service bureaus
- Other data center backup alternatives
- Mutual Aid Agreements

A *mutual aid agreement* (sometimes called a *reciprocal* agreement) is an arrangement with another company that may have similar computing needs. The other company may have similar hardware or software configurations, or may require the same network data communications or Internet access as your organization.

In this type of agreement, both parties agree to support each other in the case of a disruptive event. This arrangement is made on the assumption that each organization's operations area will have the capacity to support the other's in time of need. This is a big assumption.

There are clear advantages to this type of arrangement. It allows an organization to obtain a disaster processing site at very little or no cost, thereby creating an alternate processing site even though a company may have very few financial resources to create one. Also, if the company has very similar processing needs, that is, the same network operating system, the same data communications needs, or the same transaction processing procedures, this type of agreement may be workable.

This type of agreement has serious disadvantages, however, and really should be considered only if the organization has the perfect partner (a subsidiary, perhaps) and has no other alternative to disaster recovery (i.e., a solution would not exist otherwise). One disadvantage is that it is highly unlikely that each organization's infrastructure will have the extra unused capacity to enable full operational processing during the event. Also, as opposed to a hot or warm site, this type of arrangement severely limits the responsiveness and support available to the organization during an event, and can be used only for short-term outage support.

The biggest flaw in this type of plan is obvious if we ask what happens when the disaster is large enough to affect both organizations. A major outage can easily disrupt both companies, thereby canceling any advantage this agreement may provide. The capacity and logistical elements of this type of plan make it seriously limited.

Subscription Services

Another type of alternate processing scenario is presented by *subscription services*. In this scenario, third-party, commercial services provide alternate backup and processing facilities. Subscription services are probably the most common of the alternate processing site implementations. They have very specific advantages and disadvantages, as we shall see below.

There are three basic forms of subscription services, with some variations:

- Hot site
- Warm site
- Cold site

Hot Site

This is the Cadillac of disaster recovery alternate backup sites. A hot site is a fully configured computer facility with electrical power, heating, ventilation, and air conditioning (HVAC), and functioning file/print servers and workstations. The applications that are needed to sustain remote transaction processing are installed on the servers and workstations and are kept up-to-date to mirror the production system. Theoretically, personnel and/or operators should be able to walk in and, with a data restoration of modified files from the last backup, begin full operations in a very short time. If the site participates in remote journaling, that is, mirroring transaction processing with a high-speed data line to the hot site, even the backup time may be reduced or eliminated.

This type of site requires constant maintenance of the hardware, software, data, and applications to be sure the site accurately mirrors the state of the production site. This adds administrative overhead and can be a strain on resources, especially if a dedicated disaster recovery maintenance team does not exist.

The advantages to a hot site are numerous. The primary advantage is that 24/7 availability as well as exclusivity of use are assured. The site is immediately (or within the allowable time tolerances) available after the disruptive event occurs. The site can support an outage for a short time as well as a long-term outage.

Some of the drawbacks of a hot site are as follows:

- It is seriously the most expensive of any alternative. Full redundancy of all processing components (e.g., hardware, software, communications lines, and applications) is expensive, and the services provided to support this function will not be cheap.
- It is common for the service provider to oversell its processing capabilities, betting that not all of its clients would need the facilities simultaneously. This could create serious contention for the site's resources if a disaster were large enough to affect a major geographic region.
- There also exists a security issue at the hot site, as the applications may contain mirrored copies of live production data. Therefore, all of the security controls and mechanisms that are required at the primary site must be duplicated at the hot site. Access must be controlled and the organization must be aware of the security methodology implemented by the service organization.
- Also, a hot site may be administratively resource intensive, as controls must be implemented to keep the data up-to-date and the software patched.

Warm Site

A warm site could best be described as a cross between a hot site and cold site. Like a hot site, the warm site is a computer facility readily available with electrical power and HVAC and computers, but the applications may not be installed or configured. It may have file/print servers, but not a full complement of workstations. External communication links and other data elements that commonly take a long time to order and install will be present, however.

To enable remote processing at this type of site, workstations will have to be delivered quickly and applications and their data will need to be restored from backup media.

The advantages to this type of site, as opposed to the hot site, are primarily as follows:

- *Cost.* This type of configuration will be considerably less expensive than a hot site.
- *Location.* Because this type of site requires less extensive control and configuration, more flexibility exists in the choice of site.
- *Resources.* Administrative resource drain is lower than with the maintenance of a hot site.

The primary disadvantage of a warm site, compared to a hot site, is the difference in the amount of time and effort it will take to start production processing at the new site. If extremely urgent critical transaction processing is not needed, this may be an acceptable alternative.

Cold Site

A cold site is the least ready of any of the three choices, but is probably the most common of the three. A cold site differs from the other two in that it is ready for equipment to be brought in during an emergency, but no computer hardware (servers or workstations) resides at the site. The cold site is a room with electrical power and HVAC, but computers must be brought on-site if needed, and communications links may be ready or not. File and print servers have to be brought in, as well as all workstations, and applications will need to be installed and current data restored from backups.

A cold site is not considered an adequate resource for disaster recovery, because of the length of time required to get it going and all of the variables that will not be resolved before the disruptive event. In reality, using a cold site will most likely make effective recovery impossible. It will be next to impossible to perform an in-depth disaster recovery test or to do parallel transaction processing, making it very hard to predict the success of a disaster recovery effort.

There are some advantages to a cold site, however, the primary one being cost. If an organization has very little budget for an alternative backup processing site, the cold site may be better than nothing. Also, resource contention with other organizations will not be a problem, and neither will geographic location likely be an issue.

The big problem with this type of site is that a false sense of security could be engendered by having the cold site. But until a disaster strikes, there's really no way to tell if it works or not, and by then it will be too late.

Multiple Centers

A variation on the previously listed alternative sites is called *multiple centers*, or dual sites. In a multiple-center concept, the processing is spread over several operations centers, creating a distributed approach to redundancy and sharing of available

resources. These multiple centers could be owned and managed by the same organization (in-house sites) or used in conjunction with some sort of reciprocal agreement.

The advantages are primarily financial, because the cost is contained. Also, this type of site will often allow for resource and support sharing among the multiple sites. The main disadvantage is the same as for mutual aid: a major disaster could easily overtake the processing capability of the sites. Also, multiple configurations could be difficult to administer.

Service Bureaus

In rare cases, an organization may contract with a service bureau to fully provide all alternate backup processing services. The big advantage to this type of arrangement is the quick response and availability of the service bureau, testing is possible, and the service bureau may be available for more than backup. The disadvantages of this type of setup are primarily the expense and resource contention during a large emergency.

Other Data Center Backup Alternatives

There are a few other alternatives to the ones we have previously mentioned. Quite often an organization may use some combination of these alternatives in addition to one of the preceding scenarios.

- *Rolling/mobile backup sites.* Contracting with a vendor to provide mobile backup services. This may take the form of mobile homes or flatbed trucks with power and HVAC sufficient to stage the alternate processing required. This is considered a cold site variation.
- *In-house or external supply of hardware replacements.* Vendor re-supply of needed hardware, or internal stockpiling of critical components inventory. The organization may have a subscription service with a vendor to send identified critical components overnight. May be acceptable for a warm site but is not acceptable for a hot site.
- *Prefabricated buildings.* It's not unusual for a company to employ a service organization to construct prefabricated buildings to house the alternate processing functions if a disaster should occur. Not too different from a mobile backup site: a very cold site.

Transaction Redundancy Implementations

The CISSP candidate should understand the three concepts used to create a level of fault tolerance and redundancy in transaction processing. While these processes are not used solely for disaster recovery, they are often elements of a larger disaster recovery plan. If one or more of these processes are employed, the ability of a company to get back on-line is greatly enhanced.

- *Electronic vaulting.* Electronic vaulting refers to the transfer of backup data to an off-site location. This is primarily a batch process of dumping the data through communications lines to a server at an alternate location.
- *Remote journaling.* Remote journaling refers to the parallel processing of transactions to an alternate site, as opposed to a batch dump process like electronic vaulting. A communications line is used to transmit live data as it occurs. This allows the alternate site to be fully operational at all times and introduces a very high level of fault tolerance.

- *Database shadowing.* Database shadowing uses the live processing of remote journaling, but creates even more redundancy by duplicating the database sets to multiple servers. See *server redundancy* in the Telecomm section.

Disaster Recovery Plan Maintenance

Disaster recovery plans often get out of date. A similarity common to all recovery plans is how quickly they become obsolete, for many different reasons. The company may reorganize and the critical business units may be different than when the plan was first created. Most commonly, changes in the network or computing infrastructure may change the location or configuration of hardware, software, and other components. The reasons may be administrative: complex disaster recovery plans are not easily updated, personnel lose interest in the process, or employee turnover may affect involvement.

Whatever the reason, plan maintenance techniques must be employed from the outset to ensure that the plan remains fresh and usable. It's important to build maintenance procedures into the organization by using job descriptions that centralize responsibility for updates. Also, create audit procedures that can report regularly on the state of the plan. It's also important to ensure that multiple versions of the plan do not exist, because it could create confusion during an emergency. Always replace older versions of the text with updated versions throughout the enterprise when a plan is changed or replaced.

Testing the Disaster Recovery Plan

Testing the disaster recovery plan is very important (a tape backup system cannot be considered working until full restoration tests have been conducted); a disaster recovery plan has many elements that are only theoretical until they have actually been tested and certified. The test plan must be created and testing must be carried out in an orderly, standardized fashion, and be executed on a regular basis.

Also, there are five specific disaster recovery plan testing types that the CISSP candidate must know. Regular disaster recovery drills and tests are a cornerstone of any disaster recovery plan. No demonstrated recovery capability exists until the plan is tested. The tests must exercise every component of the plan for confidence to exist in the plan's ability to minimize the impact of a disruptive event.

Reasons for Testing

In addition to the general reason for testing we have previously mentioned, there are several specific reasons to test, primarily to inform management of the recovery capabilities of the enterprise. Other specific reasons are as follows:

- Testing verifies the accuracy of the recovery procedures and identifies deficiencies.
- Testing prepares and trains the personnel to execute their emergency duties.
- Testing verifies the processing capability of the alternate backup site.

Creating the Test Document

To get the maximum benefit and coordination from the test, a document outlining the test scenario must be produced, containing the reasons for the test, the objectives of the test, and the type of test to be conducted (see the five following types). Also, this document should include granular details of what will happen during the test, including:

- The testing schedule and timing
- The duration of the test

Plan Viability

Remember: The functionality of the recovery plan will directly determine the survivability of the organization! The plan shouldn't be a document gathering dust in the CIO's bookcase. It has to reflect the actual ability of the organization to recover from a disaster, and therefore needs to be tested regularly.

- The specific test steps
- Who will be the participants in the test
- The task assignments of the test personnel
- The resources and services required (supplies, hardware, software, documentation, and so forth)

Certain fundamental concepts will apply to the testing procedure. Primarily, the test must not disrupt normal business functions. Also, the test should start with the easy testing types (see the following section) and gradually work up to major simulations after the recovery team has acquired testing skills.

It's important to remember that the reason for the test is to find weaknesses in the plan. If no weaknesses were found, it was probably not an accurate test. The test is not a graded contest on how well the recovery plan or personnel executing the plan performed. Mistakes will be made, and this is the time to make them. Document the problems encountered during the test and update the plan as needed, then test again.

The Five Disaster Recovery Plan Test Types

There are five types of disaster recovery plan tests. The listing here is prioritized, from the simplest to the most complete testing type. As the organization progresses through the tests, each test is progressively more involved and more accurately depicts the actual responsiveness of the company. Some of the testing types, for example, the last two, require major investments of time, resources, and coordination to implement. The CISSP candidate should know all of these and what they entail.

The following are the testing types:

1. Checklist.
2. Structured walk-through.
3. Simulation.
4. Parallel.
5. Full-interruption.

Checklist Test. During a checklist type of disaster recovery plan, copies of the plan are distributed to each business unit's management. The plan is then reviewed to ensure the plan addresses all procedures and critical areas of the organization. In reality, this is considered a preliminary step to a real test, and is not a satisfactory test in itself.

Structured Walk-Through Test. In this type of test, business unit management representatives meet to walk through the plan. The goal is to ensure that the plan accurately reflects the organization's ability to recover successfully, at least on paper. Each step of the plan is walked-through in the meeting and marked as performed. Major glaring faults with the plan should be apparent during the walk-through.

Simulation Test. During a simulation test, all of the operational and support personnel expected to perform during an actual emergency meet in a practice session. The goal

here is to test the ability of the personnel to respond to a simulated disaster. The simulation goes to the point of relocating to the alternate backup site or enacting recovery procedures, but does not perform any actual recovery process or alternate processing.

Parallel Test. A parallel test is a full test of the recovery plan, utilizing all personnel. The difference between this and the full-interruption test below is that the primary production processing of the business does not stop; the test processing runs in parallel to the real processing. The goal of this type of test is to ensure that critical systems will actually run at the alternate processing backup site. Systems are relocated to the alternate site, parallel processing is initiated, and the results of the transactions and other elements are compared. This is the most common type of disaster recovery plan testing.

Full-Interruption Test. During a full-interruption test, a disaster is replicated even to the point of ceasing normal production operations. The plan is totally implemented as if it were a real disaster, to the point of involving emergency services (although for a major test, local authorities may be informed and help coordinate). This is a very scary form of test, as it can cause a disaster on its own. It's the absolute best way to test a disaster recovery plan, however, because it either works or it doesn't.

Table 8.2 lists the five disaster recovery plan testing types in priority.

Disaster Recovery Procedures

Like life insurance, these are the procedures that you hope you never have to implement. This part of the plan details what roles various personnel will take on, what tasks must be implemented to recover and salvage the site, how the company interfaces with external groups, and financial considerations.

Table 8.2: Disaster Recovery Plan Testing Types

Level	Type	Description
1	Checklist	Copies of plan are distributed to management for review.
2	Structured walk-through	Business unit management meets to review the plan.
3	Simulation	All support personnel meet in a practice execution session.
4	Parallel Test	Critical systems are run at an alternate site.
5	Full-Interruption Test	Normal production shut down, with real disaster recovery processes.

The primary elements of the disaster recovery process can be separated as follows:

The recovery team

- The salvage team
- Normal operations resume
- Other recovery issues

The Recovery Team

A recovery team will be clearly defined with the mandate to implement the recovery procedures at the declaration of the disaster. The recovery team's primary task is to get the pre-defined critical business functions operating at the alternate backup processing site.

Among the many tasks the recovery team will have will be the retrieval of needed materials from off-site storage, that is, backup tapes, media, workstations, and so on. When this material has been retrieved, the recovery team will install the necessary equipment and communications. The team will also install the critical systems, applications, and data required for the critical business units to resume working.

The Salvage Team

A salvage team, separate from the recovery team, will be dispatched to return the primary site to normal processing environmental conditions. It's advisable to have a different team, because this team will have a different mandate from the recovery team. They are not involved with the same issues the recovery team is concerned with, like creating production processing and determining the criticality of data. The salvage team has the mandate to quickly, and more importantly, safely clean, repair, salvage, and determine the viability of the primary processing infrastructure after the immediate disaster has ended.

Clearly, this cannot begin until all possibility of personal danger has ended. The return to the site may be controlled by fire or police. The salvage team must identify sources of expertise, equipment, and supplies that can make the return to the site possible. The salvage team supervises and expedites the cleaning of equipment or storage media which may have suffered from smoke damage, the removal of standing water, and the drying of water-damaged media and reports.

This team is often also given the authority to declare when the site is resumptive or not, that is, when the resumption of normal duties can begin at the primary site. This is a very large responsibility, as many elements of production must be examined before the green light is given to the recovery team that operations can return.

Normal Operations Resume

This is normally the task of the recovery team, or another, separate resumption team may be created. The plan must have full procedures on how the company will return production processing from the alternate site to the primary site with the minimum of disruption and risk. It's interesting to note that the steps to resume normal processing operations will be different than the steps in the recovery plan; that is, the least critical work should be brought back first to the primary site.

It's important to note that the emergency is not over until all operations are back in full production mode at the primary site (see sidebar).

All three of the implementation elements discussed here involve very well-coordinated logistical plans and resources. To manage and dispatch a recovery team, a salvage team, and perhaps a resumption team is a major effort, and the short descriptions we have here should not give the impression that is not a very serious task.

Other Recovery Issues

Several other issues must be discussed as important elements of a disaster scenario:

- Interfacing with external groups
- Employee relations
- Fraud and crime
- Financial disbursement
- Media relations

Interfacing with External Groups

Quite often the organization may be well-equipped to cope with a disaster in relation to its own employees, but it overlooks its relationship with external parties. The external parties could be municipal emergency groups like police, fire, EMS, medical, or hospital staff; they could be civic officials, utility providers, the press, customers, or shareholders. How all personnel, from senior management on down, interact with these groups will impact the success of the disaster recovery effort. The recovery plan must clearly define steps and escalation paths for communications with these external groups.

Note One of the elements of the plan will be to identify how close the operations site is to emergency facilities: medical (hospital, clinic), police, and fire. The timeliness of the response of emergency groups will have a bearing on implementation of the plan when a disruptive event occurs.

When Is a Disaster Over?

When is a disaster over? The answer is very important. The disaster is not over until all operations have been returned to their normal location and function. A very large window of vulnerability exists when transaction processing returns from the alternate backup site to the original production site. The disaster can be officially called over when all areas of the enterprise are back to normal in their original home, and all data has been certified as accurate.

Employee Relations

Another important facet of the disaster recovery plan is how the organization manages its relationship with its employees and their families. In the event of a major life and/or safety-endangering event, the organization has an inherent responsibility to its employees (and families, if the event is serious enough). The organization must make preparations to be able to continue salaries even when business production has stopped. This salary continuance may be for an extended period of time, and the company should be sure its insurance can cover this cost, if needed. Also, the employees and their families may need funds for various types of emergency assistance for re-location or extended living support, as can happen with a major natural event such as an earthquake or flood.

Fraud and Crime

Other problems related to the event may crop up. Beware of those individuals or organizations that may seek to capitalize financially on the disaster by exploiting security concerns or other opportunities for fraud. In a major physical disaster, vandalism and looting are common occurrences. The plan must consider these contingencies.

Financial Disbursement

An often overlooked facet of the disaster will be expense disbursement. Procedures for storing signed, authorized checks off-site must be considered in order to facilitate financial reimbursement. Also, the possibility that the expenses incurred during the event may exceed the emergency manager's authority must be addressed.

Media Relations

A major part of any disaster recovery scenario involves the media. An important part of the plan must address dealing with the media and with civic officials. It's important for the organization to prepare an established and unified organizational response that will be projected by a credible, trained, informed spokesperson. The company should be accessible to the media so they don't go to other sources; report your own bad news so as to not appear to be covering up. Tell the story quickly, openly, and honestly to avoid suspicion or rumors. Before the disaster, as part of the plan, determine the appropriate clearance and approval processes for the media. It's important to take control of dissemination of the story quickly and early in the course of the event.

Sample Questions

1. Which of the following is NOT one of the five disaster recovery plan testing types? ?
 - A. Simulation
 - B. Checklist
 - C. Mobile
 - D. Full Interruption

2. Why is it so important to test disaster recovery plans frequently? ?
 - A. The businesses that provide subscription services may have changed ownership.
 - B. A plan is not considered viable until a test has been performed.
 - C. Employees may get bored with the planning process.
 - D. Natural disasters can change frequently.

3. What is the purpose of the Business Impact Assessment (BIA)? ?
 - A. To create a document to be used to help understand what impact a disruptive event would have on the business.
 - B. To define a strategy to minimize the effect of disturbances and to allow for resumption of business processes.
 - C. To emphasize the organization's commitment to its employees and vendors.
 - D. To work with executive management to establish a DRP policy.

4. Which of the following is NOT considered an element of a backup alternative? ?
 - A. Electronic vaulting
 - B. Remote journaling
 - C. Warm site
 - D. Checklist

5. Which type of backup subscription service will allow a business to recover quickest? ?
 - A. A hot site
 - B. A mobile or rolling backup

service

C. A cold site

D. A warm site

6. Which of the following would best describe a “cold” backup site? ?

A. A computer facility with electrical power and HVAC, all needed applications installed and configured on the file/print servers, and enough workstations present to begin processing

B. A computer facility with electrical power and HVAC but with no workstations or servers on-site prior to the event and no applications installed

C. A computer facility with no electrical power or HVAC

D. A computer facility available with electrical power and HVAC and some file/ print servers, although the applications are not installed or configured and all of the needed workstations may not be on site or ready to begin processing

7. Which of the following is NOT considered a natural disaster? ?

A. Earthquake

B. Sabotage

C. Tsunami

D. Flood

8. What could be a major disadvantage to a “mutual aid” or “reciprocal” type of backup service agreement? ?

A. It’s free or at low cost to the organization.

B. The use of prefabricated buildings makes recovery easier.

C. In a major emergency, the site may not have the capacity to handle the operations required.

D. Annual testing by the Info Tech department is required to

- maintain the site.
9. What is considered the major disadvantage to employing a “hot” site for disaster recovery? ?
- A. Exclusivity is assured for processing at the site.
 - B. Maintaining the site is expensive.
 - C. The site is immediately available for recovery.
 - D. Annual testing is required to maintain the site.
10. When is the disaster considered to be officially over? ?
- A. When the danger has passed and the disaster has been contained.
 - B. When the organization has processing up and running at the alternate site.
 - C. When all of the elements of the business have returned to normal functioning at the primary site.
 - D. When all employees have been financially reimbursed for their expenses.
11. What is the number one priority of disaster response? ?
- A. Transaction processing
 - B. Personnel safety
 - C. Protecting the hardware
 - D. Protecting the software
12. Put the five disaster recovery testing types in their proper order, from the least extensive to the most. ?
- A. Full-interruption
 - B. Checklist
 - C. Structured walk-through
 - D. Parallel
 - E. Simulation
13. What is the difference between a “parallel” disaster recovery plan test and a “full interruption” disaster recovery plan test? ?
- A. There is no difference; both terms mean the same thing.
 - B. While a full-interruption test

tests the processing functionality of the alternate site, the parallel test actually replicates a disaster by halting production.

C. While a parallel test tests the processing functionality of the alternate site, the full-interruption test actually replicates a disaster by halting production.

D. Functional business unit representatives meet to review the plan to ensure it accurately reflects the organization's recovery strategy

14. Which of the following is NOT one of the primary goals of a BIA? ?

A. Resource requirements

B. Personnel safety

C. Criticality prioritization

D. Downtime estimation

Answers

1. *Answer:* c). Mobile. The other three are proper examples of elements of the five disaster recovery plan testing types.

2. *Answer:* b). A plan is not considered functioning and viable until a test has been performed. An untested plan sitting on a shelf is useless and might even have the reverse effect of creating a false sense of security. While the other answers, especially a), are good reasons to test, b) is the primary reason.

3. *Answer:* a). Create a document to be used to help understand what impact a disruptive event would have on the business. b), is the definition of business continuity planning.

4. *Answer:* d). A checklist is a type of disaster recovery plan test. Electronic vaulting is the batch transfer of backup data to an off-site location. Remote journaling is the parallel processing of transactions to an alternate site. A warm site is a backup processing alternative.

5. *Answer:* a). Warm and cold sites require more work after the event occurs to get them to full operating functionality. A "mobile" backup site might be useful for specific types of minor outages, but a hot site is still the main choice of backup processing site.

6. *Answer:* b). A computer facility with electrical power and HVAC, with workstations and servers available to be brought on-site when the event begins and no applications installed, is a cold site. a), is a hot site, and d), is a warm site. c), is just an empty room.

7. *Answer:* b). An easy one, although the more paranoid among us might think the others are Mother Nature's way of sabotage.
8. *Answer:* c). The site might not have the capacity to handle the operations required during a major disruptive event. While mutual aid might be a good system for sharing resources during a small or isolated outage, a major natural or other type of disaster can create serious resource contention between the two organizations.
9. *Answer:* b). The expense of maintaining the site. A hot site is commonly used for those extremely time-critical functions that the business must have up and running to continue operating, but the expense of duplicating and maintaining all of the hardware, software, and application elements is a serious resource drain to most organizations.
10. *Answer:* c). When all of the elements of the business have returned to normal functioning at the primary site. It's important to remember that a threat to continuity exists when processing is being returned to it's original site after salvage and cleanup has been done.
11. *Answer:* b). The number one function of all disaster response and recovery is the protection of the safety of people, all other concerns are vital to business continuity, but secondary to personnel safety.
12. *Answer:* b), c), e), d), a).
13. *Answer:* c). A parallel test tests the processing functionality of the alternate site, whereas the full-interruption test actually replicates a disaster by halting production. Answer d) is the definition of a checklist test type.
14. *Answer:* b). Personnel safety is the primary priority of BCP and DRP, not BIA.

Chapter 9: Law, Investigation, and Ethics

Introduction

Law as it applies to information systems security has multiple facets. A security professional is expected to know and understand what laws apply to computer crimes, how to determine if a crime has occurred, how to preserve evidence, the basics of conducting an investigation, and the liabilities under the law.

In addition to legal obligations, a security practitioner has ethical responsibilities to the employer, the constituency that is being served, and to the profession as a whole. These ethical factors are delineated by a number of professional organizations, including the International Information Systems Security Certification Consortium (ISC)², the Internet Activities Board (IAB), and the Computer Ethics Institute.

Types of Computer Crime

Numerous government and private sector surveys show that computer crimes are increasing. It is difficult to estimate the economic impact of these crimes because many are never detected or reported. It is not unreasonable to assume, however, that computer crimes result in billions of dollars in losses to companies in the worldwide economy. In general, computer crimes fall into two categories — *crimes committed against the computer* and *crimes using the computer*. The following is a general listing of the most prominent types of computer crimes:

- *Denial of Service (DoS) and Distributed Denial of Service.* Overloading or “hogging” a system’s resources so that it is unable to provide the required services. In the distributed mode, requests for service from a particular resource may be launched from large numbers of hosts where software has been planted to become active at a particular time or upon receiving a particular command.
- Theft of passwords.
- *Network Intrusions.* Unauthorized penetrations into networked computer resources.
- *Emanation Eavesdropping.* Receipt and display of information, which is resident on computers or terminals, through the interception of Radio Frequency (RF) signals generated by those computers or terminals. The U.S. Government established a program called *Tempest* that addressed this problem by requiring shielding and other emanation-reducing mechanisms to be employed on computers processing sensitive and classified government information.
- *Social Engineering.* Using social skills to obtain information, such as passwords or PIN numbers, to be used in an attack against computer-based systems.
- *Illegal Content of Material.* Pornography is an example of this type of crime.
- *Fraud.* Using computers or the Internet to perpetrate crimes such as auctioning material that will not be delivered after receipt of payment.
- *Software Piracy.* Illegal copying and use of software.
- *Dumpster Diving.* Obtaining sensitive data, such as manuals and trade-secrets, by gathering information that has been discarded as garbage in dumpsters or at recycling locations.
- *Malicious Code.* Programs (such as Viruses, Trojan Horses, and Worms) that, when activated, cause Denial of Service (DoS) or destruction/modification of the information on computers.

- *Spoofing of IP Addresses.* Inserting a false IP address into a message to disguise the original location of the message or to impersonate an authorized source.
- *Information Warfare.* Attacking the information infrastructure of a nation — including military/government networks, communication systems, power grids, and the financial community — to gain military and/or economic advantages.
- Espionage.
- Destruction or the Alteration of Information.
- *Use of Readily Available Attack Scripts on the Internet.* Scripts, which have been developed by others and are readily available through the Internet, that can be employed by unskilled individuals to launch attacks on networks and computing resources.
- *Masquerading.* Pretending to be someone else usually to gain higher access privileges to information that is resident on networked systems.
- *Embezzlement.* Illegally acquiring funds, usually through the manipulation and falsification of financial statements.
- *Data-Diddling.* The modification of data.
- Terrorism.

Examples of Computer Crime

The following are some specific instances of computer crimes:

- Distributed Denial of Service (DoS) attacks against Yahoo, Amazon.com, and ZDNet in February of 2000.
- Love Letter (Love Bug) worm released by Onel de Guzman in the Philippines that spread worldwide in May of 2000.
- Inadvertent transmission of emails containing personal client information to 19 unintended recipients by Kaiser Permanente HMO in August of 2000.
- Penetration of Microsoft Corporation's network in October of 2000 by cracker who gained access to software under development.
- Kevin Mitnick's attacks against telephone systems. Mitnick was convicted in 1989 for computer and access device fraud, but eluded police and the FBI for over two years while he was on probation. On Christmas of 1995, he broke into the computers of Tsutomu Shimomura in San Diego, California. Tsutomu tracked down Mitnick after a cross-country electronic pursuit, and he was arrested by the FBI in Raleigh, North Carolina, on February 15th, 1995.
- Teenagers in Wisconsin (area code 414) known as the 414 Gang who, in 1982, launched attacks into the Sloan-Kettering Cancer Hospital's medical records systems.
- The Morris Internet Worm that spread through the Internet in November of 1988 and resulted in a Denial of Service (DoS). The cause of this disruption was a small program written by Robert Tappan Morris, a 23-year-old doctoral student at Cornell University.
- Attacks against U.S. classified computer systems in 1986 by Germans working for the KGB described in the book *Cuckoo's Egg* written by Clifford Stoll. (Clifford Stoll, *The Cuckoo's Egg*, Doubleday, Copyright, 1989. ISBN, 0-385-24946-2.) Stoll uncovered this activity after he noticed a 75¢ error in a computer account at the Lawrence Livermore Laboratories.

Laws have been passed in many countries to address these crimes. Obviously, there are jurisdictional problems associated with the international character of the Internet that makes prosecution difficult and, sometimes, impossible. Some of the international organizations that are addressing computer crime are the United Nations, Interpol, the European Union, and the G8 leading industrial nations.

The rapid development of new technology usually outpaces the law. Thus, law enforcement uses traditional laws against embezzlement, fraud, Denial of Service (DoS), and wiretapping to prosecute computer criminals. The issues of digital signatures, e-commerce, and digital currency will certainly have to be addressed by the legal system as these technologies are deployed.

Law

There are many types of legal systems in the world that differ in how they treat evidence, the rights of the accused, and the role of the judiciary. Examples of these different legal systems are Common Law, Islamic and other Religious Law, and Civil Law. The Common Law System is employed in the United States, United Kingdom, Australia, and Canada. Civil Law Systems are used in France, Germany, and Quebec, and other places.

Example: The United States

Under the Common Law System of the United States, there are three “branches” of government that make the laws. These branches are the legislative branch, the administrative agencies, and the judicial branch. The legislative branch makes the *statutory laws*; the administrative agencies create the *administrative laws*, and the judicial branch makes the *common laws* found in court decisions.

Compilation of Statutory Law

Statutory laws are collected as session laws, which are arranged in order of enactment or as statutory codes, that arrange the laws according to subject matter. In the United States at the federal level, the session laws are found in the Statutes at Large (Stat.) and the statutory codes are held in the United States Code (U.S.C.) The statutory laws for the states are also arranged in these two categories.

Federal Statutes are usually cited to the United States Code and this citation contains the following elements:

- The Code title number (Each title is a grouping of statutes dealing with a particular subject matter)
- The abbreviation for the code (U.S.C.)
- The statutory section number within the title
- The date of the edition or supplement

For example, “18 U.S.C. § 1001 (1992)” refers to Section 1001 in Title 18 of the 1992 edition of the United States Code. Title 18 in the United States Code is Crimes and Criminal Procedures and many computer crimes are prosecuted under this title. The U.S. Computer Fraud and Abuse Act that addresses the use of federal interest computers to commit fraud can be found as “18 U.S.C. § 1030 (1986)” Other titles are

Title 12. Banks and Banking

Title 15. Commerce and Trade

Title 26. Internal Revenue Code

Title 49. Transportation

Compilation of Administrative Law

Administrative laws are also arranged either chronologically in administrative registers or by subject matter in administrative codes. At the federal level, these arrangements are respectively called the Federal Register (Fed. Reg.) and the Code of Federal Regulations (C.F.R.). A citation to the Code of Federal Regulations includes the following:

- The number of the C.F.R. title
- The abbreviation for the Code (C.F.R.)
- The section number
- The year of publication

Thus, the reference “12 C.F.R. § 100.4 (1992)” points to Section 100.4 in Title 12 of the 1992 edition of the Code of Federal Regulations.

Compilation of Common Law

Common law is compiled as Case Reporters in chronological fashion and in Case Digests arranged by subject matter.

Common Law System Categories

The main categories of laws under the Common Law System (not to be confused with common law resulting from court decisions) are criminal law, civil (tort) law, and administrative/regulatory law.

Criminal Law. Laws about individual conduct that violates government laws enacted for the protection of the public. Punishment can include financial penalties and imprisonment.

Civil Law. Laws about a wrong inflicted upon an individual or organization that results in damage or loss. Punishment cannot include imprisonment, but financial awards comprised of punitive, compensatory, or statutory damages can be mandated.

Administrative/Regulatory Law. Standards of performance and conduct expected by government agencies from industries, organizations, officials, and officers. Violations of these laws can result in financial penalties and/or imprisonment.

Other categories of law under the common law system that relate to information systems are intellectual property and privacy laws.

Intellectual Property Law

The following categories fall under intellectual property law:

Patent. Provides the owner of the patent with a legally enforceable right to exclude others from practicing the invention covered by the patent for a specified period of time (17 years in the United States)

Copyright. Protects “original works of authorship”; protects the right of the author to control the reproduction, adaptation, public distribution, and performance of these original works; can be applied to software and databases

Trade Secret. Secures and maintains the confidentiality of proprietary technical or business-related information that is adequately protected from disclosure by the owner. Corollaries to this definition are that the owner has invested resources to develop this information, it is valuable to the business of the owner, would be valuable to a competitor, and it is non-obvious.

Trademark. Establishes a word, name, symbol, color, sound, product shape, device, or combination of these that will be used to identify goods and to distinguish them from those made or sold by others.

Information Privacy Laws

The protection of information on private individuals from intentional or unintentional disclosure or misuse is the goal of the information privacy laws. The intent and scope of these laws widely varies from country to country. The European Union (EU) has defined privacy principles that, in general, are more protective of individual privacy than those applied in the United States. Therefore, the transfer of personal information from the EU to the United States when equivalent personal protections are not in place in the United States is prohibited. The EU principles include the following:

- Data should be collected in accordance with the law.
- Information collected about an individual cannot be disclosed to other organizations or individuals unless authorized by law or by consent of the individual.
- Records kept on an individual should be accurate and up to date.
- Individuals have the right to correct errors contained in their personal data.
- Data should be used only for the purposes for which it was collected, and it should be used only for reasonable period of time.
- Individuals are entitled to receive a report on the information that is held about them.
- Transmission of personal information to locations where “equivalent” personal data protection cannot be assured is prohibited.

An excellent example of the requirements and application of individual privacy principles is in the area of health care. The protection from disclosure and misuse of a private individual’s medical information is a prime example of a privacy law. Some of the common health care security issues are as follows:

- Access controls of most health care information systems do not provide sufficient granularity to implement the principle of least privilege among users.
- Most off-the-shelf applications do not incorporate adequate information security controls.
- Systems must be accessible to outside partners, members, and some vendors.
- Providing users with the necessary access to the Internet creates the potential for enabling violations of the privacy and integrity of information.
- Criminal and civil penalties can be imposed for the improper disclosure of medical information.
- A large organization’s misuse of medical information can cause the public to change its perception of the organization.
- Health care organizations should adhere to the following information privacy principles (based on European Union principles):
 - An individual should have the means to monitor the database of stored information about themselves and have the ability to change or correct that information.
 - Information obtained for one purpose should not be used for another purpose.
 - Organizations collecting information about individuals should ensure that the information is provided only for its intended use and should provide safeguards against the misuse of this information.
 - The existence of databases containing personal information should not be kept secret.

The U.S. *Kennedy-Kassenbaum Health Insurance Portability and Accountability Act (HIPAA-Public Law 104-191)* (effective August 21, 1996) addresses the issues of health care privacy and plan portability in the United States. With respect to privacy, this Act stated, “Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit . . . detailed recommendations on standards with respect to the privacy of individually identifiable health information.” This Act further stated “the recommendations . . . shall address at least the following:

- The rights that an individual who is a subject of individually identifiable health information should have
- The procedures that should be established for the exercise of such rights
- The uses and disclosures of such information that should be authorized or required”

The Privacy regulations were reopened for public comment for an additional period that closed on March 30, 2001. At the time of this writing, the Security and Electronic Signature Standards are also still in draft form. However, the Privacy regulations state the following in reference to information system security requirements:

“(1) Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) Implementation specification: safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.”

This information was excerpted as a summary from Appendix D of this text where additional HIPAA information is provided.

Electronic Monitoring

Additional personal security issues involve keystroke monitoring, email monitoring, surveillance cameras, badges, and magnetic entry cards. Key issues in electronic monitoring are that the monitoring is conducted in a lawful manner, and it is applied in a consistent fashion. With email for example, an organization monitoring employees’ email should

- Inform all that email is being monitored by means of a prominent log-on banner or some other frequent notification
 - This banner should state that by logging on to the system, the individual consents to electronic monitoring and is subject to a predefined punishment if the system is used for unlawful activities or the user violates the organization’s information security policy. It should also state that unauthorized access and use of the system is prohibited and subject to punishment.
- Ensure that monitoring is uniformly applied to all employees
- Explain what is considered acceptable use of the email system
- Explain who can read the email and how long it is backed-up
- Not provide a guarantee of email privacy

In this context, it is useful to examine the difference between *enticement* and *entrapment*. Enticement occurs after an individual has gained unauthorized access to a system. The intruder is then lured to an attractive area or “honey pot” in order to provide

time to determine the origin of the intrusion and, eventually, the identity of the intruder. For example, a student breaking into a professor's computer may be lured to a file entitled "Final Examination Questions." Entrapment, on the other hand, encourages the commission of a crime that the individual initially had no intention of committing.

Computer Security, Privacy, and Crime Laws

The following is a summary of laws, regulations, and directives and lists requirements pertaining to the protection of computer-related information:

1970 U.S. Fair Credit Reporting Act. Covers consumer reporting agencies.

1970 U.S. Racketeer Influenced and Corrupt Organization Act (RICO). Addresses both criminal and civil crimes involving racketeers influencing the operation of legitimate businesses — crimes cited in this act include mail fraud, securities fraud, and the use of a computer to perpetrate fraud.

1973 U.S. Code of Fair Information Practices. Applies to personal record-keeping.

1974 U.S. Privacy Act. Applies to federal agencies, provides for the protection of information about private individuals that is held in federal databases, and grants access by the individual to these databases.

1980 Organization for Economic Cooperation and Development (OECD) Guidelines. Provides for data collection limitations, the quality of the data, specifications of the purpose for data collection, limitations on data use, information security safeguards, openness, participation by the individual on whom the data is being collected, and accountability of the data controller.

1984 U.S. Medical Computer Crime Act. Addresses illegal access or alteration of computerized medical records through phone or data networks.

1984 (Strengthened in 1986 and 1994) First U.S. Federal Computer Crime Law Passed. Covered classified defense or foreign relations information, records of financial institutions or credit reporting agencies, and government computers. Unauthorized access or access in excess of authorization became a felony for classified information and a misdemeanor for financial information. This law made it a misdemeanor to knowingly access an U.S. Government computer without or beyond authorization if the U.S. Government's use of the computer would be affected.

1986 (Amended in 1996) U.S. Computer Fraud and Abuse Act. Clarified the 1984 law and added three new crimes:

1. When use of a federal interest computer furthers an intended fraud.
2. Altering, damaging, or destroying information in a federal interest computer or preventing the use of the computer or information that causes a loss of \$1000 or more or could impair medical treatment.
3. Trafficking in computer passwords if it affects interstate or foreign commerce or permits unauthorized access to government computers.

1986 U.S. Electronic Communications Privacy Act. Prohibits eavesdropping or the interception of message contents without distinguishing between private or public systems.

1987 U.S. Computer Security Act. Places requirements on federal government agencies to conduct security-related training, to identify sensitive systems, and to develop a security plan for those sensitive systems. A category of sensitive information called *Sensitive But Unclassified* (SBU) has to be considered. This category, formerly called Sensitive Unclassified Information (SUI), pertains to information below the Government's Classified level that is important enough to protect, such as medical information, financial information and research and development knowledge. This act also partitioned the government's responsibility for security between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA.) NIST was given responsibility for information security in general, (primarily for the

commercial and SBU arenas), and NSA retained the responsibility for cryptography for classified government and military applications.

1990 United Kingdom Computer Misuse Act. Defines computer-related criminal offenses.

1991 U.S. Federal Sentencing Guidelines. Provides punishment guidelines for those found guilty of breaking federal law. These guidelines are as follows:

1. Treat the unauthorized possession of information without the intent to profit from the information as a crime.
2. Address both individuals and organizations.
3. Make the degree of punishment a function of the extent to which the organization has demonstrated *due diligence* (*due care or reasonable care*) in establishing a prevention and detection program.
4. Invoke the *prudent man rule* that requires senior officials to perform their duties with the care that ordinary, prudent people would exercise under similar circumstances.
5. Place responsibility on senior organizational management for the prevention and detection programs with fines of up to \$290 million for nonperformance.

1992 OECD Guidelines to Serve as a Total Security Framework. Framework includes laws, policies, technical and administrative measures, and education.

1994 U.S. Communications Assistance for Law Enforcement Act. Requires all communications carriers to make wiretaps possible.

1994 U.S. Computer Abuse Amendments Act. This act accomplished the following:

1. Changed the federal interest computer to a computer used in interstate commerce or communications.
2. Covers viruses and worms.
3. Included intentional damage as well as damage done with “reckless disregard of substantial and unjustifiable risk”
4. Limited imprisonment for the unintentional damage to one year.
5. Provides for civil action to obtain compensatory damages or other relief.

1995 Council Directive (Law) on Data Protection for the European Union (EU). Declares that each EU nation is to enact protections similar to those of the OECD Guidelines.

1996 U.S. Economic and Protection of Proprietary Information Act. Addresses industrial and corporate espionage and extends the definition of property to include proprietary economic information in order to cover theft of this information.

1996 U.S. Kennedy-Kassenbaum Health Insurance and Portability Accountability Act (HIPAA) (with the additional requirements added in December of 2000). Addresses the issues of personal health care information privacy and health plan portability in the United States.

1996 U.S. National Information Infrastructure Protection Act. Enacted in October of 1996 as part of Public Law 104-294, it amended the Computer Fraud and Abuse Act, which is codified at 18 U.S.C. § 1030. The amended Computer Fraud and Abuse Act is patterned after the OECD Guidelines for the Security of Information Systems and addresses the protection of the confidentiality, integrity, and availability of data and systems. This path is intended to encourage other countries to adopt a similar framework, thus creating a more uniform approach to addressing computer crime in the existing global information infrastructure.

Generally Accepted Systems Security Principles (GASSP). These items are not laws, but are accepted principles that have a foundation in the OECD Guidelines:

1. Computer security supports the mission of the organization.
2. Computer security is an integral element of sound management.

3. Computer security should be cost-effective.
4. Systems owners have security responsibilities outside their organizations.
5. Computer security responsibilities and accountability should be made explicit.
6. Computer security requires a comprehensive and integrated approach.
7. Computer security should be periodically reassessed.
8. Computer security is constrained by societal factors.

As of this writing, there is also pending legislation dealing with U.S. Government procurement issues and electronic transactions. These pending laws are the *Uniform Electronic Transactions Act (UETA)* and the *Uniform Computer Information Transactions Act (UCITA)*. The UETA applies to practices at the state level that are covered in the *Federal Electronic Signatures in Global and Nation Commerce Act of 2000 (E-Sign.)* As the result of this legislation, a major change would be the permission to use electronic signatures for certain transactions.

UCITA legislation deals with shrink-wrap and click-wrap licensing agreements. With these agreements, a user explicitly agrees to the licensing terms upon opening the shrink-wrapped box of new software or when asked to click agreement to terms in order to install the new software. It makes such licensing agreements legally binding, but does not hold the software developer liable for consequential damages due to the software's failure to perform. UCITA, essentially, confirms the status quo.

Investigation

The field of investigating computer crime is also known as *computer forensics*. Specifically, computer forensics is the collecting of information from and about computer systems that is admissible in a court of law.

Computer Investigation Issues

Because of the nature of information that is stored on the computer, investigating and prosecuting computer criminal cases have unique issues, such as the following:

- Investigators and prosecutors have a compressed time frame for the investigation.
- The information is intangible.
- The investigation may interfere with the normal conduct of the business of an organization.
- There may be difficulty in gathering the evidence.
- Data associated with the criminal investigation may be located on the same computer as data needed for the normal conduct of business (co-mingling of data).
- In many instances, an expert or specialist is required.
- Locations involved in the crime may be geographically separated by long distances in different jurisdictions. This separation may result in differences in laws, attitudes toward computer crimes, definitions of computer crimes, as well as difficulty in obtaining search warrants, lack of cooperation, and so forth.
- Many jurisdictions have expanded the definition of property to include electronic information.

Evidence

The gathering, control, storage, and preservation of evidence are extremely critical in any legal investigation. Because the evidence involved in a computer crime may be

intangible and subject to easy modification without a trace, evidence must be carefully handled and controlled throughout its entire life cycle. Specifically, there is a *chain of evidence* that one must follow and protect. The following are the major components of this chain of evidence:

- Location of evidence when obtained
- Time evidence was obtained
- Identification of individual(s) who discovered evidence
- Identification of individual(s) who secured evidence
- Identification of individual(s) who controlled evidence and/or who maintained possession of that evidence

The *evidence life cycle* covers the evidence gathering and application process. This life cycle has the following components:

- Discovery and recognition
- Protection
- Recording
- Collection
 - Collect all relevant storage media
 - Make image of hard disk before removing power
 - Print out screen
 - Avoid degaussing equipment
- Identification (tagging and marking)
- Preservation
 - Protect magnetic media from erasure
 - Store in proper environment
- Transportation
- Presentation in a court of law
- Return of evidence to owner
- Evidence Admissibility

To be admissible in a court of law, evidence must meet certain stringent requirements. The evidence must be *relevant*, *legally permissible*, *reliable*, properly *identified*, and properly *preserved*. The main points of these requirements are as follows:

- *Relevant*. The evidence is related to the crime in that it shows that the crime has been committed, can provide information describing the crime, can provide information as to the perpetrator's motives, can verify what had occurred, and can fix the crime's time of occurrence.
- *Legally Permissible*. The evidence was obtained in a lawful manner.
- *Reliability*. The evidence has not been tampered with or modified.
- *Identification*. The evidence is properly identified without changing or damaging the evidence. In computer forensics, this process includes the following:
 - Labeling printouts with permanent markers.
 - Identifying the operating system used, the hardware types, and so on.
 - Recording serial numbers.
 - Marking evidence without damaging it, or by placing it in sealed containers that are marked.
- *Preservation*. The evidence is not subject to damage or destruction. The following are the recommended procedures for preservation:
 - Do not prematurely remove power.
 - Back up the hard disk image using disk imaging hardware or software.
 - Avoid placing magnetic media in the proximity of sources of magnetic fields.

- Store media in a dust and smoke-free environment at proper temperature and humidity.
- Write protect media.
- Authenticate the file system by creating a digital signature based on the contents of a file or disk sector. One-way hash algorithms, such as the Secure Hash Algorithm (SHA) as described in the Chapter 4, “Cryptography,” can be used.

Types of Evidence

Legal evidence can be classified into the following types.

- *Best evidence*. Original or primary evidence rather than a copy or duplicate of the evidence.
- *Secondary evidence*. A copy of evidence or oral description of its contents; not as reliable as best evidence.
- *Direct evidence*. Proves or disproves a specific act through oral testimony based on information gathered through the witness’s five senses.
- *Conclusive evidence*. Incontrovertible; overrides all other evidence.
- *Opinions*. The following are the two types of opinions:
 - *Expert*. May offer an opinion based on personal expertise and facts
 - *Nonexpert*. May testify only as to facts
- *Circumstantial evidence*. Inference of information from other, intermediate, relevant facts.
- *Hearsay evidence (3rd party)*. Evidence that is not based on personal, first-hand knowledge of the witness, but was obtained from another source. Under the U.S. Federal Rules of Evidence (803), hearsay evidence is generally not admissible in court. Computer-generated records and other business records fall under the category of hearsay evidence because these records cannot be proven accurate and reliable. This inadmissibility is known as the *hearsay rule*. However, there are certain exceptions to the hearsay rule for records that are
 - Made during the regular conduct of business and authenticated by witnesses familiar with their use
 - Relied upon in the regular course of business
 - Made by a person with knowledge of the records
 - Made by a person with information transmitted by a person with knowledge
 - Made at or near the time of occurrence of the act being investigated
 - In the custody of the witness on a regular basis

Searching and Seizing Computers

The U.S. Department of Justice (DOJ) Computer Crime and Intellectual Property Section (CCIPS) has issued the publication *Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations (January, 2001)*. The document introduction states, “This publication provides a comprehensive guide to the legal

issues that arise when federal law enforcement agents search and seize computers and obtain electronic evidence in criminal investigations. The topics covered include the application of the Fourth Amendment to computers and the Internet, the Electronic Communications and Privacy Act, workplace privacy, the law of electronic surveillance and evidentiary information system security uses.” The document also cites the following U.S. Codes relating to searching and seizing computers:

18 U.S.C. § 12510. Definitions

18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

18 U.S.C. § 2701. Unlawful access to stored communications

18 U.S.C. § 2702. Disclosure of contents

18 U.S.C. § 2703. Requirements for governmental access

18 U.S.C. § 2705. Delayed notice

18 U.S.C. § 2711. Definitions

18 U.S.C. § 2000aa. Searches and seizures by government officers and employees in connection with the investigation or prosecution of criminal offenses

The headings of these codes illustrate the areas covered and, in general, the increased concern for the privacy of the individual.

Export Issues and Technology

In July of 2000, the U.S. announced a relaxation of its encryption export policy to certain countries. To quote the President’s Chief of Staff, John D. Podesta, “Under our new policy, American companies can export any encryption product to any end user in the European Union and eight other trading partners. We’re also speeding up the time to market by eliminating the thirty-day waiting period when exporting encryption goods to these countries.” Podesta also pointed out the effect that advancing technology has had on the Electronic Communications and Privacy Act (ECPA). He pointed out that, “ECPA, like its predecessors, has, in many ways, become outdated by the new advances in computer technology and electronic communication. Since its passage in 1986, we’ve seen a communications revolution with the explosion of the cell phone and the development and use of the World Wide Web. Today, there more than 95 million cell phone users, and more than 50 million households on line in the United States. More than 1.4 billion e-mails [sic] change hands every day . . . ECPA was not devised to address many of the issues related to these newer, faster means of electronic communication. It doesn’t extend the stringent Title III protections to the capture of email that you send to your friends or business partners.” Podesta cited legislation, which is being proposed to amend existing statutes and outmoded language, which applies primarily to wiretapping and to define protections for hardware and software systems in general.

Conducting the Investigation

There are many issues involved in the conduct of an investigation of suspected computer crime. For example, in a corporate environment, an investigation should involve management, corporate security, human resources, the legal department, and other appropriate staff members. The act of investigating may also affect critical operations. For example, it may prompt a suspect to commit retaliatory acts that may compromise data or result in a Denial of Service (DoS), generate negative publicity, or open individual privacy issues. Thus, it is important to prepare a plan beforehand on how to handle reports of suspected computer crimes. A committee of appropriate personnel should be set up beforehand to address the following issues:

- Establishing a prior liaison with law enforcement

- Deciding when and if to bring in law enforcement (in the United States, the FBI and Secret Service have jurisdiction over computer crimes)
- Setting up means of reporting computer crimes
- Establishing procedures for handling and processing reports of computer crime
- Planning for and conducting investigations
- Involving senior management and the appropriate departments, such as legal, internal audit, information systems, and human resources
- Ensuring the proper collection of evidence, which includes identification and protection of the various storage media

If a computer crime is suspected, it is important not to alert the suspect. A preliminary investigation should be conducted to determine if a crime has been committed by examining the audit records and system logs, interviewing witnesses, and assessing the damage incurred. It is critical to determine if disclosure to legal authorities is required by law or regulation. U.S. Federal Sentencing Guidelines require organizations to report criminal acts. There are a number of pertinent issues to consider relative to outside disclosure. Negative publicity resulting in a lack of confidence in the business of the organization is an obvious concern. Once an outside entity such as law enforcement is involved, information dissemination is out of the hands of the organization. Law enforcement involvement necessarily involves support from the organization in terms of personnel time.

The timing of requesting outside assistance from law enforcement is another major issue. In the United States, law enforcement personnel are bound by the Fourth Amendment to the U.S. Constitution and must obtain a warrant to search for evidence. This amendment protects individuals from unlawful search and seizure. Search warrants are issued when there is probable cause for the search and provide legal authorization to search a location for specific evidence. Private citizens are not held to this strict requirement and, thus, in some cases, a private individual can conduct a search for possible evidence without a warrant. However, if a private individual were asked by a law enforcement officer to search for evidence, a warrant would be required because the private individual would be *acting as an agent of law enforcement*.

An exception to the search warrant requirement for law enforcement officers is the *Exigent Circumstances Doctrine*. Under this doctrine, if probable cause is present and destruction of the evidence is deemed imminent, the search can be conducted without the delay of having the warrant in-hand.

Thus, if law enforcement is called in too early when a computer crime is suspected, the law enforcement investigators will be held to a stricter standard than the organization's employees in regard to searching for and gathering evidence. However, there is a higher probability that any evidence acquired will be admissible in court because law enforcement personnel are trained in preserving the chain of evidence. As stated previously, the dissemination of information and the corresponding publicity will also be out of the organization's control when the investigation is turned over to law enforcement. Conversely, if law enforcement is called in too late to investigate a possible computer crime, improper handling of the investigation and evidence by untrained organization employees may reduce or eliminate the chances of a successful prosecution.

Good sources of evidence include telephone records, video cameras, audit trails, system logs, system backups, witnesses, results of surveillance, and emails.

A standard discriminator used to determine whether a subject may be the perpetrator of a crime is to evaluate whether the individual had a *Motive*, the *Opportunity*, and *Means* to commit the crime. This test is known as *MOM*.

If the investigation is undertaken internally, the suspect should be interviewed to acquire information and to determine who committed the offense. This interrogation should be planned in advance, and expert help should be obtained in the conduct of the interview. Obviously, the suspect is alerted when he or she is scheduled for interrogation and a common mistake in setting up and conducting the interview is providing the suspect with too much information. With this information, the suspect may try to alter additional evidence, leave the premises, or warn other co-conspirators. In the conduct of the interrogation, the pertinent information relative to the crime should be obtained and the questions should be scripted beforehand. Original documents should not be used in the conduct of the interview to avoid the possible destruction of critical information by the suspect.

Liability

In 1997, the Federal Sentencing Guidelines were extended to apply to computer crime. Recall that, under these guidelines, senior corporate officers can be personally subject to up to \$290 million in fines if their organizations do not comply with the law. These guidelines also treat the possession of illegally acquired material without intent to resell as a crime.

Management has the obligation to protect the organization from losses due to natural disasters, malicious code, compromise of proprietary information, damage to reputation, violation of the law, employee privacy suits, and stockholder suits. Management must follow the *prudent man rule* that “requires officers to perform duties with diligence and care that ordinary, prudent people would exercise under similar circumstances.” The officers must exercise *due care* or *reasonable care* to carry out their responsibilities to the organization. In exercising due care, corporate officers must institute the following protections:

- Means to prevent the organization’s computer resources from being used as a source of attack on another organization’s computer system (such as in Distributed DoS attacks)
 - Relates to the principle of *proximate causation* in which an action that was taken or not taken was part of a chain that resulted in negative consequences
- Backups
- Scans for malicious code
- Business continuity/disaster recovery plans
- Local and remote access control
- Elimination of unauthorized and unsecured modems
- Organizational security policies, procedures, and guidelines
- Personnel screening procedures
 - Ensuring the confidentiality, integrity, and availability of organizational databases
 - Addressing the organization’s responsibilities to other entities such as customers and prime contractors
 - Establishing an organizational incident-handling capability

The criteria for evaluating the legal requirements for implementing safeguards is to evaluate the cost (**C**) of instituting the protection versus the estimated loss (**L**) resulting from exploitation of the corresponding vulnerability. If **C** < **L**, then a legal liability exists.

Incident handling noted in the prevention list is an important part of contingency planning that addresses handling malicious attacks, usually by technical means. Incident handling or an emergency response should be planned for prior to the occurrence of any incidents and should address the following:

- What is considered an incident
- How an incident should be reported
- To whom should the incident be reported
- When should management be informed of the incident
- What action should be taken if an incident is detected
- Who should handle the response to the incident
- How much damage was caused by the incident
- What information was damaged or compromised by the incident
- Are recovery procedures required to remediate damages caused by the incident
- What type of follow-up and review should be conducted after the incident is handled
- Should additional safeguards be instituted as a result of the incident

Incident handling can be considered as the portion of contingency planning that responds to malicious technical threats and can be addressed by establishing a Computer Incident Response Team (CIRT.) A proper incident response is important to limit the resulting damage, to provide information for prevention of future incidents, and to serve as a means of increasing employee awareness. The majority of incidents do not occur from outside crackers and malicious code. Many incidents are the result of incompetent employees, malicious employees, other insiders, accidental actions, and natural disasters. The Carnegie Mellon University Computer Emergency Response Team Coordination Center (CERT²/CC) is an excellent source of information for establishing and maintaining organizational CIRTs.

Ethics

Ethical computing is a phrase that is often used but difficult to define. Certified professionals are morally and legally held to a higher standard of ethical conduct. In order to instill proper computing behavior, ethics should be incorporated into an organizational policy and further developed into an organizational ethical computing policy. A number of organizations have addressed the issue of ethical computing and have generated guidelines for ethical behavior. A few of these ethical codes are presented to provide a familiarization with the items addressed in such codes. Some of these lists are under revision, however, the versions illustrate the general areas that are important in ethical computing behavior.

(ISC)² Code of Ethics

Certified Information Systems Security Professionals (CISSPs) shall

1. Conduct themselves in accordance with the highest standards of moral, ethical, and legal behavior.
2. Not commit or be a party to any unlawful or unethical act that may negatively affect their professional reputation or the reputation of their profession.
3. Appropriately report activity related to the profession that they believe to be unlawful and shall cooperate with resulting investigations.

4. Support efforts to promote understanding and acceptance of prudent information security measures throughout the public, private, and academic sectors of our global information society.
5. Provide competent service to their employers and clients, and shall avoid any conflicts of interest.
6. Execute responsibilities in a manner consistent with the highest standards of their profession.
7. Not misuse the information in which they come into contact during the course of their duties, and they shall maintain the confidentiality of all information in their possession that is so identified.

The Computer Ethics Institute's Ten Commandments of Computer Ethics

In 1992, the Coalition for Computer Ethics incorporated as the Computer Ethics Institute (CEI) to focus on the interface of advances in information technologies, ethics and corporate and public policy. CEI addresses industrial, academic, and public policy organizations. The Institute's founding organizations are the Brookings Institution, IBM, the Washington Consulting Group and the Washington Theological Consortium. The Institute is concerned with the ethical issues associated with the advancement of information technologies in society and has generated the following ten commandments of computer ethics.

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or the proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing for the system you are designing.
10. Thou shalt use a computer in ways that ensure consideration and respect for your fellow humans.

The Internet Activities Board (IAB) Ethics and the Internet (RFC 1087)

“Access to and use of the Internet is a privilege and should be treated as such by all users of the system.”

Any activity is defined as unacceptable and unethical that purposely

1. Seeks to gain unauthorized access to the resources of the Internet.
2. Destroys the integrity of computer-based information.
3. Disrupts the intended use of the Internet.
4. Wastes resources such as people, capacity and computers through such actions.
5. Compromises the privacy of users.
6. Involves negligence in the conduct of Internet-wide experiments.
7. The U.S. Department of Health, Education, and Welfare Code of Fair Information Practices

The United States Department of Health, Education and Welfare has developed the following list of fair information practices that focuses on the privacy of individually, identifiable personal information.

1. There must not be personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about them is in a record and how it is used.
3. There must be a way for a person to prevent information about them, which was obtained for one purpose, from being used or made available for another purposes without their consent.
4. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take precautions to prevent misuses of that data.

Individual ethical behavior widely varies because a person's perception of ethics is a function of many variables in that person's background. Because one is not stealing physical property, the "borrowing" or "viewing" of information on an organization's computers is perceived by many as innocent behavior. Some crackers (malicious hackers) feel that any information available for access or subject to access by virtue of inadequate control measures is fair game. Others are of the opinion that hacking into an organization's information systems is performing a service by alerting the organization to weaknesses in their system safeguards. These naïve and incorrect perspectives trample on the rights of individual privacy and compromise critical and organizational proprietary information.

These breaches of security can result in million dollars losses to an organization through the destruction or unavailability of critical data and resources or through stock devaluation. From the national perspective, destructive cracker behavior could seriously affect a nation's critical infrastructure, economic health, and national security. Clearly, these types of malicious hacking results cannot be explained away by claims of freedom of speech and freedom of expression rights.

Sample Questions

1. According to the Internet Activities Board (IAB), an activity that causes which of the following is considered a violation of ethical behavior on the Internet? ?
 - A. Wasting resources
 - B. Appropriating other people's intellectual output
 - C. Using a computer to steal
 - D. Using a computer to bear false witness

2. Which of the following best defines social engineering? ?
 - A. Illegal copying of software
 - B. Gathering information from discarded manuals and printouts
 - C. Using people skills to obtain proprietary information
 - D. Destruction or alteration of data

3. Because the development of new technology usually outpaces the law, law enforcement uses which traditional laws to prosecute computer criminals? ?
- A. Malicious mischief
 - B. Embezzlement, fraud, and wiretapping
 - C. Immigration
 - D. Conspiracy and elimination of competition
4. Which of the following is NOT a category of law under the Common Law System: ?
- A. Criminal law
 - B. Civil law
 - C. Administrative/Regulatory law
 - D. Derived law
5. A trade secret ?
- A. Provides the owner with a legally enforceable right to exclude others from practicing the art covered for a specified time period
 - B. Protects "original" works of authorship
 - C. Secures and maintains the confidentiality of proprietary technical or business-related information that is adequately protected from disclosure by the owner
 - D. Is a word, name, symbol, color, sound, product shape, or device used to identify goods and to distinguish them from those made or sold by others
6. Which of the following is NOT a European Union (EU) principle? ?
- A. Data should be collected in accordance with the law.
 - B. Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is permissible.
 - C. Data should be used only for the purposes for which it was collected and should be used only for reasonable period of

time.

- D. Information collected about an individual cannot be disclosed to other organizations or individuals unless authorized by law or by consent of the individual

7. The Federal Sentencing Guidelines

?

- A. Hold senior corporate officers personally liable if their organizations do not comply with the law
- B. Prohibit altering, damaging, or destroying information in a federal interest computer
- C. Prohibit eavesdropping or the interception of message contents
- D. Established a category of sensitive information called Sensitive But Unclassified (SBU)

8. What does the prudent man rule require?

?

- A. Senior officials to post performance bonds for their actions
- B. Senior officials to perform their duties with the care that ordinary, prudent people would exercise under similar circumstances
- C. Senior officials to guarantee that all precautions have been taken and that no breaches of security can occur
- D. Senior officials to follow specified government standards

9. Information Warfare is

?

- A. Attacking the information infrastructure of a nation to gain military and/or economic advantages.
- B. Developing weapons systems based on artificial intelligence technology
- C. Generating and disseminating propaganda material

10. The chain of evidence relates to ?
- A. Securing laptops to desks during an investigation
 - B. DNA testing
 - C. Handling and controlling evidence
 - D. Making a disk image
11. The Kennedy-Kassenbaum Act is also known as ?
- A. RICO
 - B. OECD
 - C. HIPAA
 - D. EU Directive
12. Which of the following refers to a U.S. Government program that reduces or eliminates emanations from electronic equipment? ?
- A. CLIPPER
 - B. ECHELON
 - C. ECHO
 - D. TEMPEST
13. Imprisonment is a possible sentence under ?
- A. Civil (tort) law
 - B. Criminal law
 - C. Both civil and criminal law
 - D. Neither civil or criminal law
14. Which one of the following conditions must be met if legal electronic monitoring of employees is conducted by an organization? ?
- A. Employees must be unaware of the monitoring activity.
 - B. All employees must agree with the monitoring policy.
 - C. Results of the monitoring cannot be used against the employee.
 - D. The organization must have a policy stating that all employees are regularly notified that monitoring is being conducted.
15. Which of the following is a key principle in the evolution of computer crime laws in many countries? ?

- A. All members of the United Nations have agreed to uniformly define and prosecute computer crime.
 - B. Existing laws against embezzlement, fraud, and wiretapping cannot be applied to computer crime.
 - C. The definition of property was extended to include electronic information.
 - D. Unauthorized acquisition of computer-based information without the intent to resell is not a crime.
- 16.** The concept of Due Care states that senior organizational management must ensure that ?
- A. All risks to an information system are eliminated.
 - B. Certain requirements must be fulfilled in carrying out their responsibilities to the organization.
 - C. Other management personnel are delegated the responsibility for information system security.
 - D. The cost of implementing safeguards is greater than the potential resultant losses resulting from information security breaches.
- 17.** Liability of senior organizational officials relative to the protection of the organizations information systems is prosecutable under ?
- A. Criminal law
 - B. Civil law
 - C. International law
 - D. Financial law
- 18.** Responsibility for handling computer crimes in the United States is assigned to ?
- A. The Federal Bureau of Investigation (FBI) and the Secret Service
 - B. The FBI only
 - C. The National Security Agency (NSA)

- D. The Central Intelligence Agency (CIA)
19. In general, computer-based evidence is considered ?
- A. Conclusive
 - B. Circumstantial
 - C. Secondary
 - D. Hearsay
20. Investigating and prosecuting computer crimes is made more difficult because ?
- A. Backups may be difficult to find.
 - B. Evidence is mostly intangible.
 - C. Evidence cannot be preserved.
 - D. Evidence is hearsay and can never be introduced into a court of law.
21. Which of the following criteria are used to evaluate suspects in the commission of a crime? ?
- A. Motive, Intent, and Ability
 - B. Means, Object, and Motive
 - C. Means, Intent, and Motive
 - D. Motive, Means, and Opportunity
22. 18 U.S.C. §2001 (1994) refers to ?
- A. Article 18, U.S. Code, Section 2001, 1994 edition
 - B. Title 18, University of Southern California, Article 2001, 1994 edition
 - C. Title 18, Section 2001 of the U.S. Code, 1994 edition
 - D. Title 2001 of the U.S. Code, Section 18, 1994 edition
23. What is enticement? ?
- A. Encouraging the commission of a crime when there was initially no intent to commit a crime
 - B. Assisting in the commission of a crime
 - C. Luring the perpetrator to an attractive area or presenting the perpetrator with a lucrative target after the crime has

- already been initiated
- D. Encouraging the commission of one crime over another
24. Which of the following is NOT a computer investigation issue? ?
- A. Evidence is easy to obtain.
 - B. The time frame for investigation is compressed.
 - C. An expert may be required to assist.
 - D. The information is intangible.
25. Conducting a search without the delay of obtaining a warrant if destruction of evidence seems imminent is possible under ?
- A. Federal Sentencing Guidelines
 - B. Proximate Causation
 - C. Exigent Circumstances
 - D. Prudent Man Rule

Answers

1. *Answer:* a). Answers b), c), and d) are ethical considerations of other organizations.
2. *Answer:* c). Using people skills to obtain proprietary information. Answer a is software piracy; answer b) is dumpster diving; and answer d) is a violation of integrity.
3. *Answer:* b). Answer a is not a law; answer; c) is not applicable because it applies to obtaining visas and so on; and answer d) is not correct because the crimes in answer b) are more commonly used to prosecute computer crimes.
4. *Answer:* d). It is a distractor, and all of the other answers are categories under common law.
5. *Answer:* c). It defines a trade secret. Answer a) refers to a patent. Answer b) refers to a copyright. Answer d) refers to a trademark.
6. *Answer:* b). The transmission of data to locations where “equivalent” personal data protection cannot be assured is NOT permissible. The other answers are EU principles.
7. *Answer:* a). Answer b) is part of the U.S. Computer Fraud and Abuse Act. Answer c) is part of the U.S. Electronic Communications Privacy Act. Answer d) is part of the U.S. Computer Security Act.
8. *Answer:* b). Answer a) is a distractor and is not part of the prudent man rule. Answer c) is incorrect because it is not possible to guarantee that breaches of security can never occur. Answer d) is incorrect since the prudent man rule does not refer to a specific government standard but relates to what other prudent persons would do.
9. *Answer:* a). Answer b) is a distractor and has to do with weapon systems development. Answer c) is not applicable.

- Answer d) is the conventional acquisition of information from radio signals.
10. *Answer: c).* Answer a) relates to physical security; answer b) is a type of biological testing; and answer d) is part of the act of gathering evidence.
11. *Answer: c).* The others refer to other laws or guidelines.
12. *Answer: d).* Answer a) refers to the U.S. government Escrowed Encryption Standard. Answer b) refers to the large-scale monitoring of RF transmissions. Answer c) is a distractor.
13. *Answer: b).* It is the only one of the choices where imprisonment is possible.
14. *Answer: d).* Answer a) is incorrect since employees must be made aware of the monitoring if it is to be legal; answer b) is incorrect since employees do not have to agree with the policy; answer c) is incorrect since the results of monitoring might be used against the employee if the corporate policy is violated.
15. *Answer: c).* Answer a) is incorrect since all nations do not agree on the definition of computer crime and corresponding punishments. Answer b) is incorrect since the existing laws can be applied against computer crime. Answer d) is incorrect since, in some countries, possession without intent to sell is considered a crime.
16. *Answer: b).* Answer a) is incorrect since all risks to information systems cannot be eliminated; answer c) is incorrect since senior management cannot delegate its responsibility for information system security under Due Care; answer d) is incorrect since the cost of implementing safeguards should be less than or equal to the potential resulting losses relative to the exercise of Due Care.
17. *Answer: b).*
18. *Answer: a).* Making the other answers incorrect.
19. *Answer: d).* Answer a) refers to incontrovertible evidence; answer b) refers to inference from other, intermediate facts; answer c) refers to a copy of evidence or oral description of its content.
20. *Answer: b).* Answer a) is incorrect since, if backups are done, they usually can be located. Answer c) is incorrect since evidence can be preserved using the proper procedures. Answer d) is incorrect since there are exceptions to the Hearsay Rule.
21. *Answer: d).*
22. *Answer: c).*
23. *Answer: c).* The definition of enticement. Answer a) is the definition of entrapment. Answers b) and d) are distractors.
24. *Answer: a).* In many instances, evidence is difficult to obtain in computer crime investigations. Answers b), c) and d) are computer investigation issues.
25. *Answer: c).* The other answers refer to other principles, guidelines or rules

Chapter 10: Physical Security

Overview

The Physical Security Domain of Information Systems Security is a fairly clear and concise domain. Simply put, the Physical Security Domain examines those elements of the surrounding physical environment and supporting infrastructure that affect the confidentiality, integrity, and availability of information systems. We are not talking about logical controls here, but you will notice that some of the physical controls described are duplicated in some of the other domains, such as Operations and Access Control (for example, Biometrics). Natural disasters are an example of physical threats to security. Facility controls to unauthorized entry or theft are elements of physical security. The area known as Industrial Security contains many of these concepts (Closed Circuit Television (CCTV), guards, fencing, lighting, and so forth). To most engineers or security professionals, this domain is probably the least sexy of the ten domains. Who cares how high perimeter fencing should be to protect critical buildings? But you need to know this stuff because 1) some of this will be on the test, and 2) the best configured firewall in the world will not stand up to a well placed brick.

From the published (ISC)² goals for the CISSP candidate:

A CISSP professional should fully understand the following:

- *The elements involved in choosing a secure site and its design and configuration*
- *The methods for securing a facility against unauthorized access*
- *The methods for securing the equipment against theft of either the equipment or its contained information*
- *The environmental and safety measures needed to protect personnel, and the facility and its resources*

Our Goals

A security practitioner needs to be aware of the elements that threaten the physical security of an enterprise, and those controls that can mitigate the risk incurred from those threats. In this chapter, we will examine threats to physical security and controls for physical security.

Domain Definition

The Physical Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information. These resources include personnel, the facility in which they work, and the data, equipment, support systems, and media with which they work. Physical security often refers to the measures taken to protect systems, buildings, and their related supporting infrastructure against threats that are associated with the physical environment.

Physical computer security can also be defined as the process used to control personnel, the physical plant, equipment, and data involved in information processing. A CISSP candidate will be expected to understand the threats and controls that are related to physically protecting the enterprise's sensitive information assets.

Threats to Physical Security

Before we can begin an investigation into the various ways an enterprise can implement proper physical security, we obviously need to know what aspects of our environment constitute a threat to our computing infrastructure. When a risk analysis or business impact assessment is performed, a list of all possible threats must be compiled. It does not matter if the likelihood of any specific vulnerability is low or nonexistent (a tsunami in Ohio, for example), all possible threats must be compiled and examined. Many assessment methods (SSE-CMM or IAM) have the practitioner compile these complete lists before making a determination as to their likelihood.

The triad of Confidentiality, Availability, and Integrity are at risk in the physical environment and must be protected. Examples of risks to C.I.A. include the following:

- Interruptions in providing computer services — Availability
- Physical damage — Availability
- Unauthorized disclosure of information — Confidentiality
- Loss of control over system—Integrity
- Physical theft — Confidentiality, Integrity, and Availability

Examples of threats to physical security are as follows:

- Emergencies
 - Fire and smoke contaminants
 - Building collapse or explosion
 - Utility loss (electrical power, air conditioning, heating)
 - Water damage (pipe breakage)
 - Toxic materials release
- Natural Disasters
 - Earth movement (such as earthquakes and mud slides)
 - Storm damage (such as snow, ice, and floods)
- Human Intervention
 - Sabotage
 - Vandalism
 - War
 - Strikes

Donn B. Parker, in his book, *Fighting Computer Crime* (Wiley, 1998), has compiled a very comprehensive list that he calls the seven major sources of physical loss, with examples provided for each.

1. *Temperature*. Extreme variations of heat or cold, such as sunlight, fire, freezing, and heat are included.
2. *Gases*. War gases, commercial vapors, humidity, dry air, and suspended particles are included. Examples of these would be Sarin nerve gas, PCP from exploding transformers, air conditioning failures, smoke, smog, cleaning fluid, fuel vapors, and paper particles from printers.
3. *Liquids*. Water and chemicals are included. Examples of these are floods, plumbing failures, precipitation, fuel leaks, spilled drinks, acid and base chemicals used for cleaning, and computer printer fluids.
4. *Organisms*. Viruses, bacteria, people, animals, and insects are included. Examples of these are sickness of key workers, molds, contamination from skin oils and hair, contamination and electrical shorting from defecation and release of body fluids, consumption of information media such as paper or cable insulation, and shorting of microcircuits from cobwebs.

5. *Projectiles*. Tangible objects in motion and powered objects are included. Examples of these are meteorites, falling objects, cars and trucks, bullets and rockets, explosions, and wind.
6. *Movement*. Collapse, shearing, shaking, vibration, liquefaction, flows, waves, separation, and slides are included. Examples of these are dropping or shaking of fragile equipment, earthquakes, earth slides, lava flows, sea waves, and adhesive failures.
7. *Energy anomalies*. Types of electric anomalies are electric surges or failure, magnetism, static electricity, aging circuitry, radiation, sound light, and radio, microwave, electromagnetic, and atomic waves. Examples of these include electric utility failures, proximity of magnets and electromagnets, carpet static, decomposition of circuit materials, decomposition of paper and magnetic disks, Electro-Magnetic Pulse (EMP) from nuclear explosions, lasers, loudspeakers, high-energy radio frequency (HERF) guns, radar systems, cosmic radiation, and explosions.

Controls for Physical Security

Under the heading of Physical Security Controls, there are several areas. In general, these controls should match up with the listed threats. In this chapter, we have grouped the controls into two areas — Administrative Controls, and Physical and Technical Controls.

Administrative Controls

Administrative controls, as opposed to physical or technical controls, can be thought of as the area of physical security protection that benefits from the proper administrative steps. These steps encompass proper emergency procedures, personnel control (in the area of Human Resources), proper planning, and policy implementation.

We will look at the following various elements of Administrative Controls:

- Facility Requirements Planning
- Facility Security Management
- Administrative Personnel Controls

Facility Requirements Planning

Facility Requirements Planning describes the concept of the need for planning for physical security controls in the early stages of the construction of a data facility. There may be an occasion when security professionals are able to provide input at the construction phase of a building or data center. Some of the physical security elements involved at the construction stage include choosing and designing a secure site.

Choosing a Secure Site

The environmental placement of the facility is also a concern during initial planning. Security professionals need to consider such questions as:

- *Visibility*. What kind of neighbors will the proposed site have? Will the site have any external markings that will identify it as a sensitive processing area? Low visibility is the rule here.
- *Local considerations*. Is the proposed site near possible hazards (for example, a waste dump)? What is the local rate of crime (such as forced entry and burglary)?

- *Natural disasters.* Is it likely this location will have more natural disasters than other locations? Natural disasters can include weather-related problems (wind, snow, flooding, and so forth) and the existence of an earthquake fault.
- *Transportation.* Does the site have a problem due to excessive air, highway, or road traffic?
- *Joint tenancy.* Are access to environmental and HVAC controls complicated by a shared responsibility? A data center may not have full access to the systems when an emergency occurs.
- *External services.* Do you know the relative proximity of the local emergency services, such as police, fire, and hospitals or medical facilities?

Designing a Secure Site

Information Security processing areas are the main focus of physical control. Examples of areas that require attention during the construction planning stage are

- *Walls.* Entire walls, from the floor to the ceiling must have an acceptable fire rating. Closets or rooms that store media must have a high fire rating.
- *Ceilings.* Issues of concern regarding ceilings are the weight bearing rating and the fire rating.
- *Floors.* The following are the concerns about flooring:
 - *Slab.* If the floor is a concrete slab, the concerns are the physical weight it can bear (known as loading, which is commonly 150 lbs. per sq. ft.), and its fire rating.
 - *Raised.* The fire rating, its electrical conductivity (grounding against static buildup), and that it employs a non-conducting surface material are concerns of raised flooring in the data center.
- *Windows.* Windows are normally not acceptable in the data center. If they do exist, however, they must be translucent and shatterproof.
 - *Doors.* Doors in the data center must resist forcible entry and have a fire rating equal to the walls. Emergency exits must be clearly marked and monitored or alarmed. Electric door locks on emergency exits should revert to a disabled state if power outages occur to enable safe evacuation. While this may be considered a security issue, personnel safety always takes precedence, and these doors should be manned in an emergency.
 - *Sprinkler system.* The location and type of fire suppression system must also be known.
 - *Liquid or gas lines.* Security professionals should know where the shutoff valves are to water, steam, or gas pipes entering the building. Also, water drains should be “positive,” that is, they should flow outward, away from the building, so they do not carry contaminants into the facility.
 - *Air conditioning.* AC units should have dedicated power circuits. Security professionals should know where the Emergency Power Off (EPO) switch is. As with water drains, the AC system should provide outward, positive air pressure and have protected intake vents to prevent air-carried toxins from entering the facility.

- *Electrical requirements.* The facility should have established backup and alternate power sources. Dedicated feeders and circuits are required in the data center. Security professionals should check for access controls to the electrical distribution panels and circuit breakers.

Facility Security Management

Under the grouping of Facility Security Management, we list Audit Trails and Emergency Procedures. These are elements of the Administrative Security Controls that are not related to the initial planning of the secure site, but are required to be implemented on an on-going basis.

Audit Trails

An audit trail (or access log) is a record of events. A computer system may have several audit trails, each focused on a particular type of activity, such as detecting security violations, performance problems, and design and programming flaws in applications. In the domain of physical security, audit trails and access control logs are vital because management needs to know where access attempts existed and by whom they were attempted.

The audit trails or access logs must record the following:

- The date and time of the access attempt
- Whether the attempt was successful or not
- Where the access was granted (which door, for example)
- Who attempted the access
- Who modified the access privileges at the supervisor level

Some audit trail systems can also send alarms or alerts to personnel if multiple access failure attempts have been made.

Remember that audit trails and access logs are detective, rather than preventative. They do not stop an intrusion — although knowing that an audit trail of the entry attempt is being compiled may influence the intruder to not attempt entry . However, audit trails do help an administrator reconstruct the details of an intrusion post-event.

Emergency Procedures

The implementation of emergency procedures, and the employee training and knowledge of these procedures is an important part of administrative physical controls. These procedures should be clearly documented, readily accessible (including copies stored off-site in the event of a disaster), and updated periodically.

Elements of emergency procedure administration should include the following:

- Emergency system shutdown procedures
- Evacuation procedures
- Employee training, awareness programs, and periodic drills
- Periodic equipment and systems tests

Administrative Personnel Controls

Administrative Personnel Controls encompass those administrative processes that are implemented commonly by the Human Resources Department during employee hiring and firing. Examples of personnel controls implemented by HR often include the following:

- Pre-employment screening
 - Employment, references, or educational history checks
 - Background investigation or credit rating checks for sensitive positions
- On-going employee checks
 - Security clearances — generated only if the employee is to have access to classified documents
 - On-going employee ratings or reviews by their supervisor
- Post-employment procedures
 - Exit interview
 - Removal of network access and change of passwords
 - Return of computer inventory or laptops

Environmental and Life Safety Controls

Environmental and Life Safety Controls are considered to be those elements of physical security controls that are required to sustain either the computer's operating environment or the personnel's operating environment. The following are the three main areas of environmental control:

1. Electrical power
2. Fire Detection and suppression
3. Heating, Ventilation, and Air Conditioning (HVAC)

Electrical Power

Electrical systems are the lifeblood of computer operations. The continued supply of clean, steady power is required to maintain the proper personnel environment as well as to sustain data operations. Many elements can threaten power systems, the most common being noise, brownouts, and humidity.

Noise

Noise in power systems refers to the presence of electrical radiation in the system that is unintentional and interferes with the transmission of clean power. Some power issues have been covered in Chapter 3, "Telecommunications and Network Security," such as Uninterruptible Power Supplies (UPS) and backup power. In this section, we will go into more detail about these types of power problems and their recommended solutions.

There are several types of noise, the most common being Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI).

EMI is noise that is caused by the generation of radiation due to the charge difference between the three electrical wires — the hot, neutral, and ground wires.

Two common types of EMI generated by electrical systems are

1. *Common-mode noise*. Noise from the radiation generated by the difference between the hot and ground wires.
2. *Traverse-mode noise*. Noise from the radiation generated by the difference between the hot and neutral wires.

RFI is generated by the components of an electrical system, such as radiating electrical cables, fluorescent lighting, and electric space heaters. RFI can be so serious that it not

only interferes with computer operations, but it also can permanently damage sensitive components.

Several protective measures for noise exist. Some of the ones that need to be noted are

- Power line conditioning
- Proper grounding of the system to the earth
- Cable shielding
- Limiting exposure to magnets, fluorescent lights, electric motors, and space heaters

Table 10.1 lists various electrical power terms and descriptions.

Table 10.1: Electrical Power Definitions	
Element	Description
Fault	Momentary power loss
Blackout	Complete loss of power
Sag	Momentary low voltage
Brownout	Prolonged low voltage
Spike	Momentary high voltage
Surge	Prolonged high voltage
Inrush	Initial surge of power at the beginning
Noise	Steady interfering disturbance
Transient	Short duration of line noise disturbances
Clean	Non-fluctuating pure power
Ground	One wire in an electrical circuit must be grounded

Brownouts

Unlike a sag, a brownout is a prolonged drop in supplied usable voltage that can do serious physical damage to delicate electronic components. The American National Standards Institute (ANSI) standards permit an 8 percent drop between the power source and the building's meter, and permit a 3.5 percent drop between the meter and the wall. In New York City, 15 percent fluctuations are common, and a prolonged brownout can lower the supplied voltage over 10 percent.

In addition, surges and spikes occurring when the power comes back up from either a brownout or an outage can also be damaging to the components. All computer equipment should be protected by surge suppressers and critical equipment will need a UPS.

Humidity

The ideal operating humidity range is defined as 40 percent to 60 percent. High humidity, which is defined as greater than 60 percent, can produce a problem by creating condensation on computer parts. High humidity also creates problems with the corrosion of electrical connections. A process similar to electroplating occurs, causing

the silver particles to migrate from the connectors onto the copper circuits, thus impeding the electrical efficiency of the components.

Low humidity of less than 40 percent increases the static electricity damage potential. A static charge of 4000 volts is possible under normal humidity conditions on a hardwood or vinyl floor, and charges up to 20,000 volts or more are possible under conditions of very low humidity with non-static—free carpeting. Although you cannot control the weather, you certainly can control your relative humidity level in the computer room through your HVAC systems. Table 10.2 lists the damage various static electricity charges can do to computer hardware.

Static Charge in Volts	Will Damage
40	Sensitive circuits and transistors
1,000	Scramble monitor display
1,500	Disk drive data loss
2,000	System shutdown
4,000	Printer Jam
17,000	Permanent chip damage

Check Your Carpets!

A major New York City legal client once brought me into an emergency situation. They were scheduled for a cut over to a major new computer system the next weekend, and were having problems keeping their system online. They had been operating it successfully in parallel for a few weeks in the lab, but once the system was moved to the operations center it would frequently abort and reset for no apparent reason. After examining every conceivable parameter of the configuration and scratching my head for a bit, I noticed that I could cause a very small static discharge when I touched the case, thereby resetting the unit. Evidently the building contractor had run out of static-free carpet in the operations center and had finished the job with regular carpeting! Once we relocated the system, everything ran fine. —RDV

Some precautions you can take to reduce static electricity damage are:

- Use anti-static sprays where possible.
- Operations or computer centers should have anti-static flooring.
- Building and computer rooms should be grounded properly.
- Anti-static table or floor mats may be used.
- HVAC should maintain the proper level of relative humidity in computer rooms.
- Fire Detection and Suppression

The successful detection and suppression of fire is an absolute necessity for the safe, continued operation of information systems. A CISSP candidate will need to know the classes, combustibles, detectors, and suppression methods of fire safety.

Fire Classes and Combustibles

Table 10.3 lists the three main type of fires, what type of combustible gives the fire its class rating, and the recommended extinguishing agent.

Class	Description	Suppression Medium
A	Common combustibles	Water or soda acid
B	Liquid	CO ₂ , soda acid, or Halon
C	Electrical	CO ₂ or Halon

For rapid oxidation to occur (a fire), three elements must be present — oxygen, heat, and fuel. Each suppression medium affects a different element and is therefore better suited for different types of fires.

- *Water.* Suppresses the temperature required to sustain the fire.
- *Soda Acid.* Suppresses the fuel supply of the fire.
- *CO₂.* Suppresses the oxygen supply required to sustain the fire.
- *Halon.* A little different, it suppresses combustion through a chemical reaction that kills the fire.

Anyone who has had the misfortune to throw water on a grease fire in a skillet and has suffered the resultant explosion will never need to be reminded that certain combustibles require very specific suppression methods.

Fire Detectors

Fire detectors respond to heat, flame, or smoke to detect thermal combustion or its by-products. Different types of detectors have various properties and use the different properties of a fire to raise an alarm.

Heat-sensing. Heat-actuated sensing devices usually detect one of the two conditions: 1) the temperature reaches a predetermined level, or 2) the temperature rises quickly regardless of the initial temperature. The first type, the fixed temperature device, has a much lower rate of false positives (false alarms) than the second, the rate-of-rise detector.

Flame-actuated. Flame-actuated sensing devices are fairly expensive, as they sense either the infrared energy of a flame or the pulsation of the flame, and have a very fast response time. They are usually used in specialized applications for the protection of valuable equipment.

Smoke-actuated. Smoke-actuated fire sensing devices are used primarily in ventilation systems where an early-warning device would be useful. Photoelectric devices are triggered by the variation in the light hitting the photoelectric cell as a result of the smoke condition. Another type of smoke detector, the Radioactive Smoke Detection device, generates an alarm when the ionization current created by its radioactive material is disturbed by the smoke.

Automatic Dial-up Fire Alarm. This is a type of signal response mechanism that dials the local fire and/or police stations and plays a prerecorded message when a fire is

detected. This alarm system is often used in conjunction with the previous fire detectors. These units are inexpensive, but can easily be intentionally subverted.

Fire Extinguishing Systems

Fire extinguishing systems come in two flavors — water sprinkler systems and gas discharge systems.

Water sprinkler systems come in four variations:

Wet Pipe. Wet pipe sprinkler systems always contain water in them, and are also called a closed head system. In the most common implementation: In the event of a heat rise to 165° F, the fusible link in the nozzle melts causing a gate valve to open, allowing water to flow. This is considered the most reliable sprinkler system, however its main drawbacks are that nozzle or pipe failure can cause a water flood, and the pipe can freeze if exposed to cold weather.

Dry Pipe. In a dry pipe system, there is no water standing in the pipe — it is being held back by a clapper valve. Upon the fire conditions previously described, the valve opens, the air is blown out of the pipe, and the water flows. While this system is considered less efficient, it is commonly preferred over wet pipe systems for computer installations because a time delay may enable the computer systems to power down before the dry pipe system activates.

Deluge. A deluge system is a type of dry pipe, but the volume of water discharged is much larger. Unlike a sprinkler head, a deluge system is designed to deliver a large amount of water to an area quickly. It is not considered appropriate for computer equipment, however, due to the time required to get back on-line after an incident.

Preaction. This is currently the most recommended water system for a computer room. It combines both the dry and wet pipe systems, by first releasing the water into the pipes when heat is detected (dry pipe), then releasing the water flow when the link in the nozzle melts (wet pipe). This allows manual intervention before a full discharge of water on the equipment occurs.

Gas discharge systems employ a pressurized inert gas and are usually installed under the computer room raised floor. The fire detection system typically activates the gas discharge system to quickly smother the fire either under the floor in the cable areas or throughout the room. Typical agents of a gas discharge system are carbon dioxide (CO₂) or Halon. Halon 1211 does not require the sophisticated pressurization system of Halon 1301 and is used in self-pressurized portable extinguishers. Of the various replacements for Halon, FM-200 is now the most common.

Suppression Mediums

Carbon Dioxide (CO₂). CO₂ is a colorless and odorless gas commonly used in gas discharge fire suppression systems. It is very effective in fire suppression due to the fact that it quickly removes any oxygen that can be used to sustain the fire. This oxygen removal also makes it very dangerous for personnel and it is potentially lethal. It is primarily recommended for use in unmanned computer facilities, or if used in manned operations centers, the fire detection and alarm system must enable personnel ample time to either exit the facility or to cancel the release of the CO₂.

Portable fire extinguishers commonly contain CO₂ or Soda Acid, and should be

- Commonly located at exits
- Clearly marked with their fire types
- Checked regularly by licensed personnel

Halon. At one time, Halon was considered the perfect fire suppression method in computer operations centers, due to the fact that it is not harmful to the equipment, mixes thoroughly with the air, and spreads extremely fast. The benefits of using Halons

are that they do not leave liquid or solid residues when discharged. Therefore, they are preferred for sensitive areas, such as computer rooms and data storage areas.

However, several issues arose with its deployment, such as that it cannot be breathed safely in concentrations greater than 10 percent, and when deployed on fires with temperatures greater than 900°, it degrades into seriously toxic chemicals — hydrogen fluoride, hydrogen bromide, and bromine. Implementation of halogenated extinguishing agents in computer rooms must be extremely well designed to enable personnel to evacuate immediately when deployed, whether Halon is released under the flooring or overhead in the raised ceiling.

At the Montreal Protocol of 1987, Halon was designated an ozone-depleting substance due to its use of Chlorofluorocarbon Compounds (CFCs). Halon has an extremely high ozone depleting potential (three to ten times more than CFCs), and its intended use results in its release into the environment.

No new Halon 1301 installations are allowed, and existing installations are encouraged to replace Halon with a non-toxic substitute, like the ones in the following list. Current federal regulations prohibit the production of Halons, and the import and export of recovered Halons except by permit. There are federal controls on the uses, releases, and mandatory removal of Halon prior to decommissioning equipment, and reporting Halon releases, accidental or not, is mandatory.

There are alternatives to Halon. Many large users of Halon are taking steps to remove Halon-containing equipment from all but the most critical areas. Most Halon 1211 in commercial and industrial applications is being replaced and recovered. Halon 1301 is being banked for future use.

The two types of Halon used are

1. Halon 1211. A liquid steaming agent that is used in portable extinguishers.
2. Halon 1301. A gaseous agent that is used in fixed total flooding systems.

Some common EPA-acceptable Halon replacements are

- FM-200 (HFC-227ea)
- CEA-410 or CEA-308
- NAF-S-III (HCFC Blend A)
- FE-13 (HFC-23)
- Argon (IG55) or Argonite (IG01)
- Inergen (IG541)
- Low pressure water mists

Contamination and Damage

Environmental contamination resulting from the fire (or its suppression) can cause damage to the computer systems by depositing conductive particles on the components.

The following are some examples of fire contaminants:

Smoke

- Heat
- Water
- Suppression medium contamination (Halon or CO₂)

Table 10.4 lists the temperatures required to damage various computer parts.

Table 10.4: Heat Damage Temperatures

Item	Temperature
Computer Hardware	175° F
Magnetic Storage	100° F
Paper Products	350° F

Heating, Ventilation, and Air Conditioning

HVAC is sometimes referred to HVACR, for the addition of refrigeration. HVAC systems can be quite complex in modern high rise buildings, and are the focal point for environmental controls. An IT manager needs to know who is responsible for HVAC, and clear escalation steps need to be defined well in advance of an environment-threatening incident. The same department is often responsible for fire, water, and other disaster response, all of which impact the availability of the computer systems.

Physical and Technical Controls

Under this general grouping, we discuss those elements of physical security that are not considered specifically administrative solutions, although they obviously have administrative aspects. Here we have the areas of environmental controls, fire protection, electrical power, guards, and locks.

We will discuss the elements of control as they relate to the areas of

- Facility Control Requirements
- Facility Access Control Devices
- Intrusion Detection and Alarms
- Computer Inventory Control
- Media Storage Requirements

Facility Control Requirements

Several elements are required to maintain physical site security for facility control:

- Guards
- Dogs
- Fencing
- Lighting
- Locks
- CCTV

Guards

Guards are the oldest form of security surveillance. Guards still have a very important and primary function in the physical security process, particularly at perimeter control. A guard can make determinations that hardware or other automated security devices cannot make due to his ability to adjust to rapidly changing conditions, to learn and alter recognizable patterns, and to respond to various conditions in the environment. Guards provide deterrent capability, response, and control capabilities, in addition to receptionist and escort functions. Guards are also the best resource during periods of personnel safety risks (they maintain order, crowd control, and evacuation), and are better at making value decisions at times of incidents. They are appropriate whenever immediate, discriminating judgment is required by the security entity.

Guards have several drawbacks, however, such as the following:

- *Availability.* They cannot exist in environments that do not support human intervention.
- *Reliability.* The pre-employment screening and bonding of guards is not foolproof.
- *Training.* Guards can be socially engineered, or may not always have up-to-date lists of access authorization.
- *Cost.* Maintaining a guard function either internally or through an external service is expensive.

Dogs

Using guards dogs is almost as old a concept as using people to guard. Dogs are loyal, reliable (they rarely have substance abuse issues), and have a keen sense of smell and hearing. However, a guard dog is primarily acceptable for perimeter physical control, and is not as useful as a human guard for making judgment calls. Some additional drawbacks include cost, maintenance, and insurance/liability issues.

Fencing

Fencing is the primary means of perimeter/boundary facility access control. The category of fencing includes fences, gates, turnstiles, and mantraps.

Fencing and other barriers provide crowd control and help deter casual trespassing by controlling access to entrances. Drawbacks to fencing include its cost, its appearance (it may be ugly), and its inability to stop a determined intruder. Table 10.5 is a very important table; a CISSP candidate should know these heights.

Table 10.5: Fencing Height Requirements

Height	Protection
3' to 4' high	Deters casual trespassers
6' to 7' high	Too hard to climb easily
8' high with 3 strands of barbed wire	Deters intruders

Mantrap. A physical access control method where the entrance is routed through a set of double doors that may monitored by a guard.

Lighting

Lighting is also one of the most common forms of perimeter or boundary protection. Extensive outside protective lighting of entrances or parking areas can discourage prowlers or casual intruders. Critical protected buildings should be illuminated up to 8' high with 2' candle power. Common types of lighting include floodlights, streetlights, fresnel lights, and searchlights.

Locks

After the use of guards, locks are probably one of the oldest access control methods ever used. Locks can be divided into two types — preset and programmable.

Preset Locks. These are your typical door locks. The combinations to enter cannot be changed except by physically removing them and replacing the internal mechanisms. There are various types of preset locks, including key-in-knob, mortise, and rim locks. These all consist of variations of latches, cylinders, and dead bolts.

Programmable Locks. These locks can be either mechanically- or electronically-based. A mechanical, programmable lock is often a typical dial combination lock, like the kind you would use on your gym locker. Another type of mechanical programmable lock is the common five-key pushbutton lock that requires the user to enter a combination of numbers. This is a very popular lock for IT operations centers. An electronic programmable lock requires the user to enter a pattern of digits on a numerical-style keypad, and it may display the digits in random order each time to prevent shoulder surfing for input patterns. It is also known as a cipher lock or keypad access control.

Closed Circuit Television

Visual surveillance or recording devices such as closed circuit television are used in conjunction with guards in order to enhance their surveillance ability and to record events for future analysis or prosecution. These devices can either be photographic in nature (as in still or movie film cameras), or electronic in nature (the closed-circuit TV camera). CCTV may be used to monitor live events occurring in an area remote to the guard, or they can be used in conjunction with a Video Cassette Recorder (VCR) for a cost-effective method of recording these events.

Remember that the monitoring of live events is preventative, and the recording of events is considered detective in nature.

Facility Access Control Devices

This includes personnel access control to the facility and general operations centers, in addition to specific data center access control.

Security Access Cards

Security access cards are a common method of physical access control. There are two common card types — photo-image and digitally-encoded cards. These two groups are also described as dumb and smart cards. Dumb cards require a guard to make a decision as to its validity, while smart cards make the entry decision electronically.

Photo-Image Cards. Photo-image cards are simple identification cards with the photo of the bearer for identification. These are your standard photo ID cards, like a drivers license or employee ID badge. These cards are referred to as “dumb” cards because they have no intelligence imbedded in them, and they require an active decision to be made by the entry personnel as to their authenticity.

Digital-Coded Cards. Digitally-encoded cards contain chips or magnetically encoded strips (possibly in addition to a photo of the bearer). The card reader may be programmed whether to accept an entry based upon an online access control computer that can also provide information about the date and time of entry. These cards may also be able to create multi-level access groupings. There are two common forms of digitally-encoded cards, which are referred to as smart and smarter cards.

Smart entry cards may either have a magnetic stripe or a small Integrated Circuit (IC) chip imbedded in them. This card may require knowledge of a password or Personal Identification Number (PIN) to enable entry. A bank ATM card is an example of this card type. These cards may contain a processor encoded with the host system's authentication protocol, read-only memory storage of programs and data, and even some kind of user interface.

In some scenarios, a smart card may be coupled with an authentication token that generates a one-time or challenge-response password or PIN. While two-actor (or dual-factor) authentication is most often used for logical access to network services, it can be combined with an intelligent card reader to provide extremely strong facility access control.

Wireless Proximity Readers. A proximity reader does not require the user to physically insert the access card. This card may also be referred to as a wireless security card. The card reader senses the card in possession of a user in the general area (proximity) and enables access. There are two general types of proximity readers — user activated and system sensing.

A user-activated proximity card transmits a sequence of keystrokes to a wireless keypad on the reader. The key pad on the reader contains either a fixed preset code or a programmable unique key pattern.

A system-sensing proximity card recognizes the presence of the coded device in the reader's general area. The following are the three common types of system-sensing cards, which are based upon the way the power is generated for these devices:

1. *Passive devices.* These cards contain no battery or power on the card, but sense the electromagnetic field transmitted by the reader and transmit at different frequencies using the power field of the reader.
2. *Field-powered devices.* They contain active electronics, a radio frequency transmitter, and a power supply circuit on the card.
3. *Transponders.* Both the card and reader each contain a receiver, transmitter, active electronics, and a battery. The reader transmits an interrogating signal to the card, which in turn causes it to transmit an access code. These systems are often used as portable devices for dynamically assigning access control.

Table 10.6 lists the various types of security access cards.

Type of Card	Description
Photo ID	Facial photograph
Optical-coded	Laser-burned lattice of digital dots
Electric circuit	Printed IC on the card
Magnetic stripe	Stripe of magnetic material
Magnetic strip	Rows of copper strips
Passive electronic	Electrically-tuned circuitry read by RF
Active Electronic	Badge transmitting encoded electronics

What Are Those Three Things Again?

What are the three elements, which we learned, that are commonly used for authentication? 1) Something you have (like a token card), 2) Something you know (like your PIN or password), and 3) Something you are (biometrics).

Biometric Devices

Biometric access control devices and techniques, such as fingerprinting or retinal scanning, are discussed thoroughly in Chapter 2, "Access Control Systems." Keep in mind that because they constitute a physical security control, biometric devices are also considered a physical access security control device.

Intrusion Detectors and Alarms

Intrusion detection refers to the process of identifying attempts to penetrate a system or building to gain unauthorized access. While Chapter 3 details Intrusion Detection (ID) systems that detect logical breaches of the network infrastructure, here we are talking about devices that detect physical breaches of perimeter security, such as a burglar alarm.

Perimeter Intrusion Detectors

The two most common types of physical perimeter detectors are either based on photoelectric sensors or dry contact switches.

- *Photoelectric sensors.* Photoelectric sensors receive a beam of light from a light-emitting device creating a grid of either visible, white light, or invisible, infrared light. An alarm is activated when the beams are broken. The beams can be physically avoided if seen; therefore invisible infrared light is often used. Also, employing a substitute light system can defeat the sensor.
- *Dry contact switches.* Dry contact switches and tape are probably the most common types of perimeter detection. This can consist of metallic foil tape on windows, or metal contact switches on door frames. This type of physical intrusion detection is the cheapest and easiest to maintain, and is very commonly used for shop front protection.

Motion Detectors

In addition to the two types of intrusion detectors previously mentioned, motion detectors are used to sense unusual movement within a predefined interior security area. They can be grouped into three categories: wave pattern motion detectors, capacitance detectors, and audio amplification devices.

- *Wave Pattern.* Wave pattern motion detectors generate a frequency wave pattern and send an alarm if the pattern is disturbed as it is reflected back to its receiver. These frequencies can either be in the low, ultrasonic, or microwave range.
- *Capacitance.* Capacitance detectors monitor an electrical field surrounding the object being monitored. They are used for spot protection within a few inches of the object, rather than for overall room security monitoring used by wave detectors. Penetration of this field changes the electrical capacitance of the field enough to generate an alarm.

- *Audio Detectors.* Audio detectors are passive, in that they do not generate any fields or patterns like the previous two methods. Audio detectors simply monitor a room for any abnormal sound wave generation and trigger an alarm. This type of detection device generates a higher number of false alarms than the other two methods, and should only be used in areas that have controlled ambient sound.

Alarm Systems

The detection devices previously listed monitor and report on a specific change in the environment. These detectors can be grouped together to create alarm systems. There are four general types of alarm systems:

1. *Local Alarm Systems.* A local alarm system rings an audible alarm on the local premises that it protects. This alarm must be protected from tampering and be audible for at least 400 feet. It also requires guards to respond locally to the intrusion.
2. *Central Station Systems.* Private security firms operate these systems that are monitored around the clock. The central stations are signaled by detectors over leased lines. These stations typically offer many additional features, such as CCTV monitoring and printed reports, and the customers' premises are commonly less than 10 minutes travel time from the central monitoring office.
3. *Proprietary Systems.* These systems are similar to the central station systems, except that the monitoring system is owned and operated by the customer. They are like local alarms, except that a sophisticated computer system provides many of the features in-house that a third-party firm would provide with a central station system.
4. *Auxiliary Station Systems.* Any of the previous three systems may have auxiliary alarms that ring at the local fire or police stations. Most central station systems include this feature, which requires permission from the local authorities before implementation.

Two other terms related to alarms are:

- *Line supervision.* Line supervision is a process where an alarm-signaling transmission medium is monitored to detect any line tampering to subvert its effectiveness. The Underwriters Laboratory (UL) standard 611-1968 states, "the connecting line between the central station and the protection shall be supervised so as to automatically detect a compromise attempt by methods of resistance substitution, potential substitution, or any single compromise attempt." Secure detection and alarm systems require line supervision.
- *Power supplies.* Alarm systems require separate circuitry and backup power with 24 hours minimum discharge time. These alarms help reduce the probability of an alarm system's failure due to a power failure.

Computer Inventory Control

Computer Inventory Control is the control of computers and computer equipment from physical theft and protection from damage. The two main areas of concern are computer physical control and laptop control.

PC Physical Control

Due to the proliferation of distributed computing and the proliferation of laptops, inventory control at the microcomputer level is a major headache. Some groups estimate that 40 percent of computer inventory shrinkage is due to microcomputer parts walking out the door. Several physical controls must be taken to minimize this loss:

- *Cable locks.* A cable lock consists of a vinyl-covered steel cable anchoring the PC or peripherals to the desk. They often consist of screw kits, slot locks, and cable traps.
- *Port controls.* Port controls are devices that secure data ports (such as a floppy drive), or a serial or parallel port and prevents their use.
- *Switch controls.* A switch control is a cover for the on/off switch, which prevents a user from switching off the file server's power.
- *Peripheral switch controls.* These types of controls are lockable switches that prevent a keyboard from being used.
- *Electronic security boards.* These boards are inserted into an expansion slot in the PC and forces a user to enter a password when the unit is booted. This is also a standard part of the Basic Input Output System (BIOS) of many off-the-shelf PCs. They may also be called cryptographic locks.

Laptop Control

The proliferation of laptops and portables is the next evolution of distributed computing and constitutes a challenge to security practitioners. Now the computing resources can be strewn all over the globe, and physical inventory control is nearly impossible for an organization without a substantive dedication of IT resources. A laptop theft is a very serious issue because it creates a failure of all three elements of C.I.A.: Confidentiality, as the data can now be read by someone outside of a monitored environment; Availability, as the user has lost the unit's computing ability; and Integrity, as the data residing on the unit and any telecommunications from it are now suspect.

Media Storage Requirements

The on-going storage of data media and the proper disposal of unneeded media and reports is a serious concern to security practitioners. Sometimes an organization will devote a large amount of resources to perimeter protection and network security, then will dispose of reports improperly. Or, they will reuse laptops or diskettes without fully and appropriately wiping the data.

Because laptop theft is rampant, encryption of any sensitive data on a portable is also an absolute necessity. An associate of mine was recently lent a laptop while working at a top brokerage firm, only to discover that the hard drive had not been reformatted, and contained dozens of sensitive emails pertaining to the 1996 presidential election (the previous owner had worked as an advisor to the GOP Bob Dole campaign).

The following types of media commonly require storage, destruction, or reuse:

Data backup tapes

- CDs
- Diskettes
- Hard drives
- Paper printouts and reports

The common storage areas for such media are

- *On-site*. Areas within the facility, such as operations centers, offices, desks, storage closets, cabinets, safes, and so on.
- *Off-site*. Areas outside of the facility, such as data backup vault services, partners and vendors, and disposal systems. Transportation to or from an external data vault services vendor is a security concern, and it should be examined for problems relating to theft, copying, alteration, or destruction of data.

We have the following resources and elements in our control to protect the media:

- Physical access control to the storage areas
- Environmental controls, such as fire and water protections
- Diskette inventory controls and monitoring
- Audits of media use

Data Destruction and Reuse

Data that is no longer needed or used must be destroyed. Information on magnetic media is typically “destroyed” by degaussing or overwriting. Formatting a disk once does not completely destroy all data, the entire media must be overwritten or formatted seven times to conform to standards for object reuse.

Paper reports should be shredded by personnel with the proper level of security clearance. Some shredders cut in straight lines or strips, others cross-cut or disintegrate the material into pulp. Care must be taken to limit access to the reports prior to disposal and those stored for long periods. Reports should never be disposed of without shredding, such as when they are placed in a dumpster intact. Burning is also sometimes used to destroy paper reports, especially in the Department of Defense and military.

Object Reuse and Data Remanence

Object Reuse is the concept of reusing data storage media after its initial use. Data Remanence is the problem of residual information remaining on the media after erasure, which may be subject to restoration by another user, thereby resulting in a loss of confidentiality. Diskettes, hard drives, tapes, and any magnetic or writable media are susceptible to data remanence. Retrieving the bits and pieces of data that have not been thoroughly removed from storage media is a common method of computer forensics, and is often used by law enforcement personnel to preserve evidence and to construct a trail of misuse. Anytime a storage medium is reused (and also when it is discarded), there is the potential for the media’s information to be retrieved. Methods must be employed to properly destroy the existing data to ensure that no residual data is available to new users. The “Orange Book” standard recommends that magnetic media be formatted seven times before discard or reuse.

Diskette Storage Tips

A few basic controls should be put in place to protect diskettes (or other magnetic media) from damage or loss, such as

1. Keep the disks in locked cases.
2. Don't bend the diskettes.
3. Maintain the proper temperature and humidity.
4. Avoid external magnetic fields (such as TVs or radios).
5. Don't write directly on the jacket or sleeve.

The Joy of Dumpster Diving

New York is the capital of ticker-tape parades. New Yorkers never seem to tire of trying to find some reason to throw large volumes of paper out of high story office windows. Sometimes, however, the enthusiasm for the moment overrides the immediate availability of shredded reports, and some office workers will begin to toss out unshredded, full-page printed pages. Local reporters have begun to collect these reports before they are swept up by sanitation, and have reported that the information contained is considerable (especially due to the fact that the parades are often down Broadway, past Wall Street). These pages often contain credit card account numbers, bank account numbers and balances, credit rating details, and so forth. I wonder if the Yankees know my American Express balance? —RDV

Terminology relative to the various stages of data erasure are as follows:

- *Clearing*. This term refers to the overwriting of data media (primarily magnetic) intended to be reused in the same organization or monitored environment.
- *Purging*. This term refers to degaussing or overwriting media intended to be removed from a monitored environment, such as during resale (laptops) or donations to charity.
- *Destruction*. This term refers to completely destroying the media, and therefore the residual data. Paper reports, diskettes, and optical media (CD-ROMs) need to be physically destroyed before disposal.

The following are the common problems with magnetic media erasure that may cause data remanence:

1. Erasing the data through an operating system does not remove the data, it just changes the File Allocation Table and renames the first character of the file. This is the most common way computer forensics investigators can restore files.
2. Damaged sectors of the disk may not be overwritten by the format utility. Degaussing may need to be used, or formatting seven times is recommended.
3. Rewriting files on top of the old files may not overwrite all data areas on the disk, because the new file may not be as long as the older file, and data may be able to be retrieved past the file end control character.
4. Degausser equipment failure or operator error may result in an inadequate erasure.
5. There may be an inadequate number of formats. Magnetic media containing sensitive information should be formatted seven times or more.

Walk-Through Security List

The simplest way to get a handle on your office's state of physical security is to do a minimal "walk-about." This consists of an after-hours walk-through of your site, checking for these specific things:

1. Sensitive company information is not lying open on desks or in traffic areas.
2. Workstations are logged out and turned off.
3. Offices are locked and secured.
4. Stairwell exits are not propped open (I have seen them propped open with fire extinguishers, so folks wouldn't have to use the elevators!).
5. Files cabinets and desks are locked and secured.
6. Diskettes and data tapes are put away and secured.

These things can help you establish a baseline of the state of physical data security at your site. The first time you do this, it is not uncommon to find less than 10 percent of the office exhibiting acceptable security procedures.

Sample Questions

1. The recommended optimal relative humidity range for computer operations is ?
 - A. 10%—30%
 - B. 30%—40%
 - C. 40%—60%
 - D. 60%—80%

2. How many times should a diskette be formatted to comply with TCSEC Orange book object reuse recommendations? ?
 - A. Three
 - B. Five
 - C. Seven
 - D. Nine

3. Which of the following more closely describes the combustibles in a Class B-rated fire? ?
 - A. Paper
 - B. Gas
 - C. Liquid
 - D. Electrical

4. Which of the following is NOT the proper suppression medium for a Class B fire? ?
 - A. CO₂
 - B. Soda Acid
 - C. Halon
 - D. Water

5. What does an audit trail or access log usually NOT record? ?
 - A. How often a diskette was formatted
 - B. Who attempted access
 - C. The date and time of the access attempt
 - D. Whether the attempt was successful

6. A brownout can be defined as a ?
 - A. Prolonged power loss
 - B. Momentary low voltage
 - C. Prolonged low voltage
 - D. Momentary high voltage

7. A surge can be defined as a(n) ?
 - A. Prolonged high voltage
 - B. Initial surge of power at start

8. Which is NOT a type of a fire detector? ?
- C. Momentary power loss
 - D. Steady interfering disturbance
 - A. Heat-sensing
 - B. Gas-discharge
 - C. Flame-actuated
 - D. Smoke-actuated
9. Which of the following is NOT considered an acceptable replacement for Halon discharge systems? ?
- A. FA200
 - B. Inergen (IG541)
 - C. Halon 1301
 - D. Argon (IG55)
10. Which type of fire extinguishing method contains standing water in the pipe, and therefore generally does not enable a manual shutdown of systems before discharge? ?
- A. Dry Pipe
 - B. Wet pipe
 - C. Preaction
 - D. Deluge
11. Which type of control below is NOT an example of a physical security access control? ?
- A. Retinal scanner
 - B. Guard dog
 - C. Five-key programmable lock
 - D. Audit trail
12. Which is NOT a recommended way to dispose of unwanted used data media? ?
- A. Destroying CD-ROMs
 - B. Formatting diskettes seven or more times
 - C. Shredding paper reports by cleared personnel
 - D. Copying new data over existing data on diskettes
13. Which of the following is an example of a "smart" card? ?
- A. A drivers license
 - B. A bank ATM card
 - C. An employee photo ID
 - D. A library card

14. Which is NOT an element of two-factor authentication? ?
- A. Something you are
 - B. Something you know
 - C. Something you have
 - D. Something you ate
15. The theft of a laptop poses a threat to which tenet of the C.I.A. triad? ?
- A. Confidentiality
 - B. Integrity
 - C. Availability
 - D. All of the above
16. Which is a benefit of a guard over an automated control? ?
- A. Guards can use discriminating judgment.
 - B. Guards are cheaper.
 - C. Guards do not need training.
 - D. Guards do not need pre-employment screening.
17. Which is NOT considered a preventative security measure? ?
- A. Fences
 - B. Guard
 - C. Audit trails
 - D. Preset locks
18. Which is NOT a PC security control device? ?
- A. A cable lock
 - B. A switch control
 - C. A port control
 - D. A file cabinet lock
19. What is the recommended height of perimeter fencing to keep out casual trespassers? ?
- A. 1' to 2' high
 - B. 3' to 4' high
 - C. 6' to 7' high
 - D. 8' to 12' high
20. Why should extensive exterior perimeter lighting of entrances or parking areas be installed? ?
- A. To enable programmable locks to be used
 - B. To create two-factor authentication

- C. To discourage prowlers or casual intruders
- D. To prevent data remanence
21. Which of the following is NOT a form of data erasure? ?
- A. Clearing
- B. Remanence
- C. Purging
- D. Destruction
22. Which is NOT considered a physical intrusion detection method? ?
- A. Audio motion detector
- B. Photoelectric sensor
- C. Wave pattern motion detector
- D. Line Supervision

Answers

1. *Answer: c).* 40% to 60% relative humidity is recommended for safe computer operations. Too low humidity can create static discharge problems, too high humidity can create condensation and electrical contact problems.
2. *Answer: c).* Most computer certification and accreditation standards recommend that diskettes be formatted seven times to prevent any possibility of data remanence.
3. *Answer: c).* Paper is described as a common combustible and is therefore rated a class A fire. An electrical fire is rated Class C. Gas is not defined as a combustible.
4. *Answer: d).* Water is not a proper suppression medium for a class B fire. The other three are commonly used.
5. *Answer: a).* How often a diskette was formatted. The other three answers are common elements of an access log or audit trail.
6. *Answer: c).* Answer a) prolonged power loss is a blackout; answer b) momentary low voltage is a sag; and d), momentary high voltage is a spike.
7. *Answer: a).* Answer b), initial surge of power at start or power on is called an inrush; c) momentary power loss is a fault; and d) a steady interfering disturbance is called noise.
8. *Answer: b).* Gas-discharge is a type of fire extinguishing system, not a fire detection system.
9. *Answer: c).* Existing installations are encouraged to replace Halon 1301 with one of the substitutes listed.
10. *Answer: b).* The other three are variations on a dry pipe discharge method, with the water not standing in the pipe until a fire is detected. The deluge method is not recommended for computer equipment, however, due to the volume of water discharged.
11. *Answer: d).*

12. *Answer: d).* Copying new data over existing data on diskettes. While this method might overwrite the older files, if the new data file is smaller than the older data file, recoverable data might exist past the file end marker of the new file.
13. *Answer: b).* The other three cards are “dumb” cards, because it is assumed that they contain no electronics, magnetic stripes or integrated circuits.
14. *Answer: d).* An easy one.
15. *Answer: d).* Confidentiality, as the data can now be read by someone outside of a monitored environment, Availability, as the user has lost the computing ability provided by the unit, and Integrity, as the data residing on and any telecommunications from the portable are now suspect.
16. *Answer: a).* Guards can use discriminating judgment. Guards are typically more expensive than automated controls, need training as to the protection requirements of the specific site, and need to be screened and bonded.
17. *Answer: c).* Audit trails are detective, rather than preventative, as they are used to piece together the information of an intrusion or intrusion attempt after the fact.
18. *Answer: d).* A cable lock is used to attach the PC to a desk, a switch control is used to prevent powering off a unit, and a port control (such as a diskette drive lock) is used to prevent data from being downloaded from the PC.
19. *Answer: b).* 3' to 4' high fencing is considered minimal protection, only for restricting casual trespassers. c) and d) are better protection against intentional intruders.
20. *Answer: c).* The other answers have nothing to do with lighting.
21. *Answer: b).* Clearing refers to the overwriting of data media intended to be reused in same organization. Purging refers to degaussing or overwriting media intended to be removed from the organization. Destruction refers to completely destroying the media.
22. *Answer: d).* Line supervision is the monitoring of the alarm signaling transmission medium to detect tampering. Audio detectors monitor a room for any abnormal sound wave generation. Photoelectric sensors receive a beam of light from a light-emitting device. Wave pattern motion detectors generate a wave pattern and send an alarm if the pattern is disturbed.

Appendix B: The RAINBOW Series—Minimum Security Requirements for Multi-user Operating Systems NISTIR 5153^[*]

Note This document has been superseded by the common criteria.

Abstract

The *minimum security requirements* (MSR) for Multi-User Operating Systems documents provides basic commercial computer system security requirements applicable to both government and commercial organizations. These requirements include technical measures that can be incorporated into multi-user, remote-access, resource-sharing, and information-sharing computer systems. The MSR document was written from the prospective of protecting the confidentiality and integrity of an organization's resources and promoting the continual availability of these resources. The MSR presented in this document forms the basis for the commercially oriented protection profiles in Volume II of the draft Federal Criteria for Information Technology Security document (known as the Federal Criteria). The Federal Criteria is currently a draft and supersedes this document.

The MSR document has been developed by the MSR Working Group of the Federal Criteria Project under *National Institute of Standards and Technology* (NIST) leadership with a high level of private-sector participation. Its contents are based on the *Trusted Computer System Evaluation Criteria* (TCSEC) C2 criteria class, with additions from current computer industry practice and commercial security requirements specifications.

1. INTRODUCTION

Government and commercial organizations rely heavily on *information technology* (IT) products to meet their operational, financial, and information requirements.

The confidentiality, integrity, and availability of key software systems, databases, and data networks are major concerns throughout these sectors. The corruption, unauthorized disclosure, or theft of an organization's electronically maintained resources can have a disruptive effect on the continuity of operations as well as serious and immediate financial, legal, and public confidence impact.

The MSR contained in this document are intended to provide both government and commercial organizations with a basic set of security requirements to protect the confidentiality and integrity of an organization's resources and to promote the continual availability of these resources.

1.1 BACKGROUND

In 1991, NIST and the *National Security Agency* (NSA) established a joint project termed the Federal Criteria for Information Technology Security (known as the Federal Criteria Project) to develop new federal criteria for trusted systems technology. The purpose of this project is to produce a *Federal Information Processing Standard* (FIPS) for developing, specifying, and evaluating IT security products that will perform the following functions:

- Be consistent with international marketplace demands.
- Provide for mutual recognition of security evaluation results between the United States and the European Community.

- Replace the existing *Trusted Computer System Evaluation Criteria* (TCSEC) [1] with a second-generation iteration that has a less-restrictive approach and wider commercial appeal.
- Provide for the open distributed computing environment of the 1990s and beyond.

The MSR form the basis of one of the protection profiles of Volume II of the preliminary Federal Criteria FIPS, the CS2, as mentioned in Section 1.1. It is hoped that this Protection Profile, if widely accepted, will form the basis for the mutual recognition of system evaluations between nations.

The MSR specify a set of security requirements needed in a class of products colloquially called “general purpose, multi-user operating systems.” These requirements have been developed by the MSR Working Group of the Federal Criteria Project under NIST leadership with a high level of private-sector participation. They are based on the TCSEC C2 criteria class, with additions from current computer industry practice, from commercial security requirements specifications, and from the ongoing work of the Federal Criteria Project.

The following subsections provide descriptions of each of these sources and also provide further background on the motivation for and development of the MSR.

1.1.1 Trusted Computer System Evaluation Criteria (TCSEC)

The TCSEC [1], originally published in 1983 and revised in 1985, was the first publicly available document that expressed general security requirements that could apply to a specific class of technology (for example, operating systems). It represents the culmination of many years of effort to address IT security issues within the *Department of Defense* (DoD) classified world. Since its publication, the TCSEC has influenced vendors, consumers, and the authors of other requirements documents both in the United States and abroad. The impact of the TCSEC on the field of IT security is widely recognized.

The TCSEC is made up of IT security features and assurances that are derived and engineered to support a very specific DoD security policy—the prevention of unauthorized disclosure, or “leakage,” of classified information (in other words, confidentiality). Although it has been helpful, the TCSEC does not completely address the security requirements of organizations that are handling sensitive (but unclassified) information. Besides confidentiality, organizations outside the classified world are also concerned with the other two components of security: integrity and availability.

Until recently, the government paid more attention to classified information processing than to addressing the IT security needs of commercial and government organizations that process unclassified, sensitive information. During the past few years, commercial and government organizations that are processing sensitive information have begun to pay increasing attention to IT security needs. Although the TCSEC-motivated security features address some security problems, these features do not provide a complete solution. TCSEC requirements were specified because a more appropriate set of security functions were not available.

The MSR are intended to be the first step in providing a set of security requirements that are appropriate for commercial and government organizations that are concerned with protecting sensitive information.

1.1.2 Information Technology Security Evaluation Criteria (ITSEC)

In recognition of the fact that a harmonized criteria was necessary to permit the mutual recognition of evaluation results, Germany, France, the United Kingdom, and the Netherlands created a harmonized set of security criteria referred to as the *Information Technology Security Evaluation Criteria* (ITSEC) [2]. Version 1 was published in June 1990, with a second version released in June 1991.

The ITSEC does not specify security requirements for specific IT systems. Instead, it provides a framework within which specific IT security requirements can be defined. The ITSEC defines two distinct evaluation criteria: functionality and assurance.

Functionality requirements are the technical security features (referred to as “security enforcing functions”) that are implemented in an IT system in order to support the system’s requirements for the maintenance of confidentiality, integrity, and availability. The ITSEC defines 10 example functionality classes: F1, F2, F3, F4, F5, F6, F7, F8, F9, and F10. Functionality classes F1—F5 are roughly equivalent to the TCSEC classes C1, C2, B1, B2, and B3. Functionality classes F6—F10 represent integrity, availability, data communications integrity, data communications confidentiality, and data communications confidentiality and integrity, respectively.

Assurance requirements provide confidence to the customer of the system as to how well the functionality has been implemented. The ITSEC considers assurance to be a combination of correctness (of the security enforcing functions) and effectiveness (of these functions). The evaluation levels range from E0 (no confidence) through E1, E2, E3, E4, E5, and E6 (the highest level of assurance). These ratings correspond roughly to the TCSEC D, C1, C2, B1, B2, B3, and A1 levels, respectively. Assurance is measured as a combination of a correctness rating and a judgment as to the effectiveness of the security-enforcing functions.

The ITSEC describes an approach for specifying and justifying the security functionality and the level of assurance (in other words, a combination of a correctness level and a judgment of effectiveness) required in a particular system.

1.1.3 Security Requirements in the Commercial Sector

Recognizing that the TCSEC was a valuable starting point but not sufficient enough for their security needs, two commercial companies— Bellcore and American Express *Travel-Related Services* (TRS)— independently initiated efforts to develop security requirements for their environments. At Bellcore, these efforts resulted in a Bellcore Standard Operating Environment Security Requirements (3) document, and at American Express, the efforts resulted in the internal C2-Plus company security standard.

The Bellcore document was developed to meet the security needs of Bellcore and its client companies, the *Regional Bell Operating Companies* (RBOCs). The requirements specified in the Bellcore document were derived both from commonly recurring security requirements for RBOC computer applications and from experiences of Bellcore’s computer security assessment group.

In developing the C2-Plus document, TRS found that while the TCSEC met many requirements of the commercial sector, the prescribed features at the C2-level (and its F2-level counterpart in the European standards) fell short in several areas that were either introduced at higher TCSEC levels or were not addressed at all. Consequently, the TRS document was developed as an enhanced, commercialized version of the TCSEC C2 level.

Using the TRS document as the base document, the *Commercial International Security Requirements* (CISR) [4] was developed by the *International Information Integrity*

Institute (I-4), a consortium of large, international corporations. Part of the rationale for the development of the CISR was as follows:

“Military-oriented information security requirements (for example, TCSEC) are not suitable in many respects for the needs of international businesses.” [4]

The final version of the CISR was published in April 1992.

1.1.4 System Security Study Committee

The System Security Study Committee was formed in 1988 in response to a request from the *Defense Advance Research Projects Agency* (DARPA) to address the security and trustworthiness of U.S. computing and communications systems. The committee, composed of 16 individuals from industry and academia including computer and communications security researchers and practitioners and software engineers, was charged with developing a national research, engineering, and policy agenda to help the United States achieve a more trustworthy computing technology base by the end of the century. In 1991, the committee published the “Computers at Risk — Safe Computer in the Information Age [5]” report, which presents the committee’s assessment of key computer and communications security issues and its recommendations for enhancing the security and trustworthiness of the U.S. computing and communications infrastructure.

The development of the MSR was guided by one of the recommendations from this report that:

“ . . . a basic set of security-related principles for the design, use, and management of systems that are of such broad applicability and effectiveness that they ought to be a part of any system with significant operational requirements” [5] should be developed.

1.1.5 Federal Criteria Project

As a result of the Computer Security Act of 1987 [6], NIST was assigned responsibility “for developing standards and guidelines for federal computer systems — drawing on the technical advice and assistance — of the National Security Agency, where appropriate.” In addition, NIST was “authorized to assist the private sector, upon request, in using and applying the results of the [NIST-initiated] programs and activities under the” Act. In 1991 (as mentioned previously), NIST and NSA established a working agreement to develop a new FIPS for Trusted Systems Technology called the *Federal Criteria* (FC) for Information Technology Security.

One of the first tasks addressed by the Federal Criteria Working Group was the development of a framework within which distinct sets of security requirements intended to meet the protection needs of varied interest groups can be specified.

This framework is referred to as a protection profile. A protection profile “describes generic protection needs” and is “product independent, describing a range of systems that could meet this same need.” Finally, a protection profile addresses the following items: rationale, functionality, and assurance.

The rationale includes the following elements: 1) the intended use of products built to meet the protection profile, 2) the assumed environment within which products built to meet the protection profile will operate, and 3) the threats that the protection profile is intended to counter.

The functionality describes the security features that must be provided by a system that is built to meet the protection profile.

The assurance describes assurance requirements that are levied on the vendor who is building a product to meet the protection profile and on the product's evaluations. Two types of assurance requirements are defined: development assurance requirements and evaluation assurance requirements.

1.1.6 Minimum Security Requirements

As noted in Section 1.1, one of the objectives of the Federal Criteria Project is replacement of the TCSEC with a second-generation iteration. As the first step of satisfying that objective, the MSR Working Group was given the task of developing a protection profile that described an enhanced C2-like class of requirements intended to satisfy the most common security needs of computer system users. The MSR are the NIST effort to satisfy this objective. Much of the MSR are derived from the TCSEC, the ITSEC, the Bellcore Standard Operating Environment Security Requirements, and the CISR, with overall guidance from the Computers at Risk report.

The MSR form the basis of one of the protection profiles of volume II of the preliminary Federal Criteria FIPS, the CS2, as mentioned in Section 1.1. It is hoped that this protection profile, if widely accepted, will form the basis for the mutual recognition of system evaluations between nations.

1.2 Scope of the MSR

The MSR specify computer-based protection mechanisms for the design, use, and management of information systems. These requirements include technical measures that can be incorporated into multi-user, remote-access, resource-sharing, and information-sharing computer systems. The MSR provide administrators of the MSR-conformant computer system with the tools to control the sharing of information and resources based primarily on the identity of users but also based on the time of day, terminal location, or type of access requested by users. The technical measures also provide tools to protect both against common user actions that might compromise security and against deliberate penetration attempts by "crackers." In addition, there are requirements that a conformant computer system provide a tailorable capability to log events that might impact the security of either the system or the information that it is processing.

Systems conforming to this protection profile are intended to be useful to a broad base of users, including those in commercial, civil government, and national defense environments. Recognizing that *information technology* (IT) product vendors operate in an international marketplace, this profile has been built to complement international efforts, such as the ITSEC and *International Standards Organization* (ISO) initiatives.

This protection profile specifies "baseline" requirements that constitute generally accepted security expectations for multi-user operating systems. These requirements apply commonly to multi-user workstations, minicomputers, and mainframes. Most required mechanisms are specified to be configurable so that individual customers can satisfy their unique security policies and objectives.

The intent of this protection profile is to promote the wide availability of products that possess security-enforcing functions that are of such broad applicability and effectiveness that they become part of the "normal" operational requirements of all multi-user operating systems.

1.3 Audience

These requirements are targeted at three distinct audiences: users, vendors, and evaluators.

Users

The MSR address the basic security needs of general-purpose computer operating systems users, including application developers, end users, and administrators in the private, civil, and defense government sectors. The requirements focus on the basic security requirements of most commercially available multi-user operating systems. All functionality requirements are based on existing and well-understood security practices. It is hoped that this set of security requirements will set a basic level of expectation within the user community for the security of the operating systems that they purchase.

Vendors

This document provides vendors with a single, well-defined set of security requirements that can be accepted across their entire customer base. These requirements represent the integration of a number of security requirement specifications from various sources into a single set that is expected to have very wide acceptance. Vendors can more confidently use this set to focus on a single system that offers what will meet the needs of a significant customer base. The level of detail provided by these requirements should help clarify what the vendor must do in order to comply.

Evaluators

This document provides product and system evaluators, certifiers, and accrediters with a well-defined set of security requirements. The detailed level of the requirements significantly decreases the need for evaluator interpretation. It is hoped that the similarity of the MSR format to the ITSEC Security Target format will provide a basis for international acceptance that can help lead to the mutual recognition of evaluations.

1.4 Terminology

The following terminology is used throughout this document:

Requirement — A feature or function that is necessary to satisfy the needs of a typical commercial or government organization. Failure to meet a requirement might cause application restrictions, result in improper functioning of the system, or hinder operations. A requirement contains the word *shall* and is identified by the letter “R” in parentheses (R).

Advisory — A feature or function that might be desired by a typical commercial or government organization. An advisory represents a goal to be achieved. An advisory can be reclassified as a requirement at some future date. An advisory contains the word *should* and is identified by the letter “A” in parentheses (A).

1.5 Document Organization

The MSR are divided into four sections and include an appendix, a glossary, and references. Section 1, the introduction (this section), provides introductory and background information. Section 2, Rationale, provides rationale to support the MSR Protection Profile. This rationale includes descriptions of the intended use of the system, the environmental assumptions that were made for the MSR-compliant system, and the expected threats. Section 3, Functionality Requirements, specifies the security functionality that the MSR-compliant system is required to provide. Section 4, Assurance Requirements, specifies the assurances that the MSR-compliant system is required to provide. The appendix provides a threat analysis, which describes how each threat (identified in Section 2) is countered. The list of documents in the References

section acts as a guide, inspiration, or information in preparing this document. Those referenced have a square bracket around a number ([]). The glossary defines key terms and acronyms used throughout the document. The reader will note that the first occurrence of any term defined in the glossary has been underlined as an aid to the reader.

2. Rationale

This section provides information for prospective purchasers of the MSR-conformant IT system. This information is to aid the purchaser in deciding whether the system will satisfy the security objectives. Specifically, it discusses how the system is intended to be used, the assumptions about the environment in which the system is intended to operate, the threats within that environment, and the security features and assurances that are intended to counter these threats.

2.1 Intended Method of Use

A product that is designed to meet this protection profile is intended to be a general-purpose, multi-user operating system that runs on either a workstation, minicomputer, or mainframe. This system is expected to support a variety of applications and might support application software development. These applications are for commercial as well as government environments.

The MSR-conformant operating system is intended to control access to information based on the identity of individual users or groups of users. The information might be unclassified, sensitive-but-unclassified, or single-level classified, but it cannot be multi-level classified information. Such a system is not intended to control access to information at multiple classification levels based on the clearance of the user.

2.2 Environmental Assumptions

The following specific environmental conditions have been assumed in specifying this protection profile:

- a. The hardware base (for example, CPU, printers, terminals, and so on) will be protected from unauthorized physical access.
- b. There will be one or more personnel assigned to manage the system, including the security of the information that it contains.
- c. If a network interface is supported, the attached networks will provide some facility to independently confirm the claimed identity of remote machines.
- d. The operational environment will be managed according to the operational environment documentation that is required in the Assurance Requirements Section of this protection profile.

2.3 Expected Threats

The MSR-conformant system is intended to be a “reasonable first-line of defense” against an unauthorized user’s attempt to gain access to the system or against an authorized user’s inadvertent attempt to gain access to information for which he or she has not been granted access.

You should understand that highly-motivated attackers who are willing to apply the necessary level of effort might be able to circumvent the security features of the system. These features are not expected to completely eliminate the threat from malicious users or software, however, such as computer viruses or Trojan horses.

The following threats have been assumed in specifying this protection profile:

- a. An unauthorized user might attempt to gain access to the system.
- b. An authorized user might attempt to gain access to resources for which he or she is not allowed access.
- c. Security-relevant actions might not be traceable to the individual who is associated with the event.
- d. The system might be delivered, installed, or used in an unsecured manner.
- e. Data that are transmitted over a public or shared data network can be modified either by an unauthorized user or because of a transmission error or other communication-related error.
- f. Security breaches might occur because available security features are not used or are used improperly.
- g. Users might be able to bypass the security features of the system.
- h. Users can be denied continued accessibility to the resources of the system (in other words, denial of service).

2.4 Security Features and Assurances

This section summarizes the security features and assurances that are required to counter the threats discussed in Section 2.3. Detailed requirements for these features and assurances can be found in Sections 3 and 4, respectively, of this protection profile.

2.4.1 Identification and Authentication

The MSR-conformant operating system provides the capability to establish, maintain, and protect a unique identifier for each authorized user. The system also provides the capability to establish, maintain, and protect from unauthorized access information that can be used to authenticate the association of a user with that identifier.

These features are intended to counter the threat that an unauthorized user might attempt to gain access to the system or to the information that it contains. It also intends to counter the threat that an authorized user might attempt to gain access to resources for which he or she is not allowed access.

2.4.2 Access Control

The MSR-conformant operating system provides the capability for a privileged user, such as a system administrator, to establish, maintain, and protect from unauthorized access information that defines the identities of users and conditions under which users can access the system. These conditions can include controls based on user identification, time, location, and method of access. The system is also required to display a warning about unauthorized attempts to access the system to each user who is attempting access. This feature is intended to counter the threat that an unauthorized user might attempt to gain access to the system or to the information that it contains.

The system provides the capability for an authorized user to specify and control access to information that he or she owns. By default, the system protects newly created information. Furthermore, once information is deleted, it is not available to subsequent users. This feature is intended to counter the threat that an authorized user might attempt to gain access to resources to which he or she is not allowed access.

The system is designed so that security features can be easily implemented, operated, and maintained. This design is intended to counter the threats that the system might be

delivered, installed, or used in an unsecured manner and that security breaches might occur because available security features are not used or are used improperly.

2.4.3 Audit

The MSR-conformant operating system creates, maintains, and protects a security audit trail that provides individual user accountability and contains information that is sufficient for an after-the-fact investigation of loss or impropriety.

This feature is intended to counter all of the threats discussed in Section 2.4.2 in the event that the system's access control features have failed to deny unauthorized access.

2.4.4 System Integrity

The MSR-conformant operating system continuously protects itself from users who are changing or circumventing the security functionality that it provides. This system is intended to provide assurance that the security features of the system operate as expected. This setup also counters the threats that security breaches might occur because available security features are not used or are used improperly, that users are able to bypass the security features of the system, or that users can be denied continued accessibility to the resources of the system.

2.4.5 Data Integrity

The MSR-conformant operating system protects the consistency and integrity of information. This protection is intended to provide assurance that the security features of the system operate as expected. This protection is also intended to counter the threats that security breaches might occur because available security features are not used or are used improperly, that users might be able to bypass the security features of the system, or that users can be denied continued accessibility to the resources of the system.

2.4.6 Reliability of Service

The MSR-conformant system provides the capability to detect and recover from any discontinuity of service, using some combination of automatic and procedural techniques.

This capability is intended to counter the threat that users might be denied continued accessibility to the resources of the system.

2.4.7 Product Development Assurance

The MSR-conformant system has been designed, implemented, and tested to ensure that it meets acceptable minimum security assurance requirements. Specifically, the system has not been designed with any mode of access that would violate or bypass the minimum security functionality requirements of the product.

This system is intended to provide assurance that the security features of the system operate as expected. This protection is also intended to counter the threats that security breaches might occur because available security features are not used or are used improperly, that users might be able to bypass the security features of the system, or that users can be denied continued accessibility to the resources of the system.

2.4.8 Product Documentation Assurance

The MSR-conformant system provides documentation to support the secure installation, operation, administration, and use of the product.

This documentation is intended to counter the threat that a system might be delivered, installed, or used in an unsecured manner. This protection is also intended to counter the threat that security breaches might occur because available security features are not used or are used improperly.

3. Functionality Requirements

This section provides detailed functionality requirements that must be satisfied by the MSR-compliant system.

3.1 Identification and Authentication

In this document, the term “user” refers to an individual human or a remote system that can access the target system to which these requirements apply. The identification and authentication process begins the user’s interaction with the target system. First, the user supplies a unique identifier (userID) to the system. Then, the user is asked to authenticate that claimed identity by the system. The requirements for identification are presented in the first subsection. The requirements for authentication are presented in the subsequent subsection.

3.1.1 Identification

A userID uniquely represents a user. The userID is used for both access control and accountability. Therefore, the proper maintenance and control of the identification mechanism and the identification databases are vital to system security. The requirements that follow support identification.

Requirements:

1. The system shall use userIDs to identify users. (R)
2. The system shall require users to identify themselves with their unique userIDs before the user is allowed to perform any actions on the system. (R)
3. The system shall internally maintain the identity of all active users (in other words, users who are currently logged on). (R)
 - a. Every process running on behalf of a user shall have associated with it the identity of that user. That is, if the process is invoked by a user, it shall have the userID of that user associated with it. If a process is invoked by another process (that was invoked by the user), the invoked process shall have the userID associated with the invoking process, and so on. (R)
 - b. Every process that is running “autonomously” (in other words, without user invocation), such as print spoolers, database management system servers, and transaction processing monitors, shall have associated with it an identification code indicating system ownership or a unique process identification code. (R)
4. The system shall provide a mechanism to administratively disable userIDs. This mechanism shall provide an option for automatic re-enabling of disabled userIDs after a customer-specifiable period of time. The use of this mechanism shall require privileges. (R)

5. The system shall automatically disable userIDs after a period of time during which the userID has not been used. The time period shall be customer- specifiable, with a default of 60 days. (R)
6. The system shall provide a mechanism to administratively re-enable or delete disabled userIDs. The use of this mechanism shall require privileges. (R)
7. The system shall provide a mechanism to obtain the status of any userID. (R)
8. The system shall provide a mechanism that enables a collection of userIDs to be referenced together as a group. (R)
 - a. A userID shall be able to be associated with more than one group. (R)
 - b. The system shall provide a mechanism to modify the group membership of a userID. The use of this mechanism shall require privileges. (R)
 - c. The system shall provide a mechanism to list the names of all groups. (R)
 - d. The system shall provide a mechanism to list the membership of any group. (R)
9. For those systems that have the architecture to support multiple logons per userID, the system shall provide a mechanism that limits the number of multiple logon sessions for the same userID. The mechanism shall allow limits for userIDs and groups to be specified. The system-supplied default shall limit each userID to one simultaneous logon session. The use of this mechanism shall require privileges. (R)
10. If the system provides a mechanism by which the userID associated with a process can be changed while the process is active, then it shall also provide a mechanism for limiting the userIDs that might change to a userID that would provide any additional privileges. (R)
11. The system shall provide a mechanism to associate customer-specifiable information (for example, a username and affiliation) with each userID. The use of this mechanism shall require privileges. (R)

3.1.2 Authentication

Once a user has supplied an identifier to the system, the system must verify that the user really corresponds to the claimed identifier. This action is performed by the authentication mechanism, as described by the following requirements. Because passwords are the most commonly used authentication mechanism, a subsection on password requirements follows this section. Although authentication and system access control processes are often combined for standalone systems, the mixing of these processes is less appropriate for distributed or client/server systems. An authenticated user might not have access to every host in a distributed system and might not be allowed direct access to a server. Therefore, this document treats system access control and authentication separately. System access control is in Section 3.2.1.

Note: Network-related issues of authentication (such as proxies and cascading trust) are beyond the scope of this document.

Requirements:

1. The system shall provide a mechanism to authenticate the claimed identity of a user. (R)
2. The system shall appear to perform the entire user authentication procedure even if the userID that was entered was not valid. Error

- feedback shall contain no information regarding which part of the authentication information is incorrect. (R)
3. The system shall provide a mechanism to support the initial entry or modification of authentication information. (R)
 4. The system shall be able to incorporate and use customer-supplied alternative authentication mechanisms, such as token-based cards, biometrics, or trusted third-party techniques, in place of or in addition to the system-supplied authentication mechanism. (R)
 - a. If multiple authentication mechanisms are provided, the system shall also provide a separate mechanism to specify the authentication mechanism(s) to be used for specific userIDs and groups. The use of this separate mechanism shall require privileges. (R)
 5. The system shall require a privilege to access any internal storage of authentication data. (R)
 - a. Authentication data transmitted over public or shared data networks should be encrypted. (A)
 6. The system shall support an application program interface to an authentication mechanism. (R)
 7. If the system provides network access (for example, dial-in, X.25, or Internet), then it shall also provide at least a Class 2 authentication mechanism (as defined in *Draft International Standard [DIS] 10181-2 [7]*) that can be used at the customer's discretion. The networking software shall be able to be disabled or configured out of the system. (R)

3.1.2.1 Password Requirements

Although systems are not required to use passwords as the user authentication mechanism, passwords are still the most commonly used mechanism for authentication. Extensive experience with password mechanisms has led to a solid understanding of what constitutes good password management. The following requirements capture this understanding:

Note These requirements apply only to systems that use passwords. Other authentication methods, such as token-based authentication, cryptographic-based authentication, and biometrics, are beyond the scope of this text.

Requirements:

1. The system shall provide no mechanism whereby a single stored password entry is explicitly shared by multiple userIDs. The system shall provide no means to facilitate the sharing of passwords by multiple users. (R)
2. The system shall allow a user to choose a password that is already associated with another userID. The system shall provide no indication that a password is already associated with another userID. (R)
3. The system shall store passwords in a one-way encrypted form. (R)
 - a. The system shall require privilege to access encrypted passwords. (R)
 - b. Unencrypted passwords shall be inaccessible to all users. (R)

4. The system shall automatically suppress or fully blot out the clear-text representation of the password on the data entry/display device. (R)
5. The system shall, by default, prohibit the use of null passwords during normal operation. (R)
6. The system shall provide a mechanism to allow a user to change his or her password. This mechanism shall require reauthentication of the user's identity. The system shall provide a mechanism to set or initialize passwords for users. The use of this mechanism shall require privileges. (R)
7. The system shall enforce password aging on a per-userID or per-group basis (in other words, a user shall be required to change his or her password after a customer-specifiable minimum time). The system-supplied default for all non-privileged users shall be 60 days. (R)
 - a. The system-supplied default for those userIDs that might acquire privileges shall be 30 days. (R)
 - b. After the password aging threshold has been reached, the password shall no longer be valid. (R)
8. The system shall provide a mechanism to notify users in advance of requiring them to change their passwords. This action can be performed by either:
 - a. Notifying users in a customer-specifiable period of time prior to their password expiring. The system-supplied default shall be seven days. (R)
 - b. Upon password expiration, notifying the user but allowing a customer-specifiable subsequent number of additional logons prior to requiring a new password. The system-supplied default shall be two additional logons. (R)
9. Passwords shall not be reusable by the same userID for a customer-specifiable period of time. The system-supplied default shall be six months. (R)
10. The system shall provide an algorithm for ensuring the complexity of user-entered passwords that meets the following requirements:
 - a. Passwords shall meet a customer-specifiable minimum length requirement. The system-supplied default minimum length shall be eight characters. (R)
 - b. The password complexity-checking algorithm shall be modifiable by the customer. The system-supplied default algorithm shall require passwords to include at least one alphabetic character, one numeric character, and one special character. (R)
 - c. The system should provide a mechanism that enables customers to specify a list of excluded passwords (for example, company acronyms and common surnames). (A)
11. The system should prevent users from selecting a password that matches any of those on the list of excluded passwords. (A)
12. If system-supplied password-generation algorithms are present in the system, they shall meet the following requirements:
 - a. The password-generation algorithm shall generate passwords that are easy to remember (in other words, pronounceable or pass-phrases). (R)

- b. The system should give the user a choice of alternative passwords from which to choose. (A)
 - c. Passwords shall be reasonably resistant to brute-force password guessing attacks (in other words, the total number of system-generated passwords shall be of at least the same order of magnitude as what a user could generate by using the rules specified in requirement 10). (R)
 - d. If the “alphabet” used by the password-generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet. (R)
 - e. The generated sequence of passwords shall have the property of randomness (in other words, consecutive instances shall be uncorrelated and the sequences shall not display periodicity). (R)
13. The system shall provide a mechanism by which a data entry/display device might force a direct connection between the port to which it is connected and the authentication mechanism. (R)

3.2 Access Control

Access control determines what an authenticated user can do with the system. Two types of access control are considered here: system access and resource access. The requirements for system access control are presented in the first subsection. The requirements for resource access control are presented in the subsequent subsection.

3.2.1 System Access Control

Once a user is authenticated, a check is made to determine whether the user is allowed to access the system. The qualifying checks for system access can include time-of-day, day-of-week, date, location of terminal, or means of access (for example, a dial-up port or local area network port).

The requirements for system access control are as follows:

Requirements:

1. The identity of all users shall be authenticated before access is granted to any resources or system information. (R)
 - a. The system shall provide no userIDs that permit unauthenticated system access during normal system operation. (R)
 - b. The system should authenticate remote machines during the establishment of an inter-system association. (A)
2. The system shall provide a mechanism to authorize users to access the system, to revoke users from accessing the system, and to modify the security information associated with users. The use of this mechanism shall require privileges. (R)
 - a. The system shall allow access to only those users who are authorized to access the system. (R)
 - b. The system shall provide a mechanism that lists all users who are authorized to access the system. The use of this mechanism shall require privileges. (R)

3. The system shall provide a mechanism for user-initiated locking of interactive sessions (for example, keyboard locking) that includes the following:
 - a. Requiring user authentication prior to unlocking the session (R)
 - b. Disabling all data entry/display devices from any activity other than unlocking the session (R)
 - c. Clearing or over-writing the display to make its current contents unreadable (R)
4. For interactive sessions, the system shall lock the session after a customer-specifiable period of user inactivity. The system-supplied default shall be 15 minutes. (R)
 - a. The system shall provide a mechanism to specify that sessions be terminated rather than locked after a period of inactivity. The use of this mechanism shall require privileges. (R)
5. The system logon procedure shall exit and end the attempted session if the user authentication procedure is incorrectly performed a customer-specifiable number of times. The system-supplied default shall be three times. (R)
 - a. The system shall generate an alarm when this threshold is exceeded. (R)
 - b. When the above threshold has been exceeded, a customer-specifiable interval of time shall elapse before the logon process can be restarted on that data entry/display device. The system-supplied default shall be 60 seconds. (R)
6. The system should increment the time interval on successive violations. (A)
 - a. The system shall provide a mechanism to disable the userID when this threshold is exceeded. (R)
7. By default, this mechanism shall be disabled. (R)
8. The system shall provide a mechanism to allow or deny specified userIDs to access the system during specified ranges of time. The use of this mechanism shall require privileges. The ranges shall include the following:
 - a. Time-of-day (R)
 - b. Day-of-week (R)
 - c. Calendar date (R)
9. The system shall provide a mechanism to allow or deny specified userIDs to access the system based on means of access or port of entry. The use of this mechanism shall require privileges. (R)
 - a. The system shall provide a mechanism to specify the userIDs that are authorized to access the system via dial-up facilities. The use of this mechanism shall require privileges. (R)
 - b. The system shall provide a mechanism to specify the userIDs that are authorized to access the system via network facilities. The use of this mechanism shall require privileges. (R)
10. The system shall provide a mechanism to limit the privilege that a user can obtain based on means of access or port of entry. The use of this mechanism shall require privileges. (R)
11. If the system provides network access, then it shall also provide a mechanism to end an abnormally terminated session such that a new user does not have access to a previous user's session. (R)
12. Prior to initiating the system logon procedure, the system shall display an advisory warning message to the user regarding unauthorized use

of the system and the possible consequences of failure to heed this warning. (R)

- a. The message shall be customer-specifiable. (R)
- b. The system shall be able to display a message of up to 20 lines in length. (R)
- c. The following message shall be displayed by default:

NOTICE: This is a private computer system. Unauthorized access or use is prohibited and may lead to prosecution. (R)

54. Upon a user's successful access to the system, the system shall display the following to the user and shall not remove it without user intervention:

- a. The date, time, and means of access or port of entry of the user's last successful system access. (R)
- b. The number of unsuccessful attempts to access the system since the last successful system access by that userID. (R)

3.2.2 Resource Access Control

Once the user has been granted access to the system as a whole, the question of which resources that authenticated user can access still remains. An owner, or a privileged user, uses provided mechanisms to allow or deny other users access to that resource. The following requirements support resource access control.

The additional requirements for protection of data in deallocated resources are presented in the subsection on object reuse.

Requirements:

1. The system shall control access to all resources. (R)
2. The system shall control access to resources based on authenticated userIDs. (R)
3. For each resource, the system shall provide a mechanism to specify a list of userIDs or groups with their specific access rights to that resource (in other words, an access control list). (R)
 - a. The access rights that can be specified shall, at a minimum include "read," "write," and "execute-only." (R)
4. There should be separate "create" and "delete" access rights for modification of entries in directories or catalogs. (A)
5. The system should support the explicit denial of all access rights to a userID or group. (A)
 - a. The access rights associated with a userID shall take precedence over the access rights associated with any groups of which that userID is a member. (R)
 - b. For systems where a userID can be an active member of multiple groups simultaneously, if any group entry allows an access right for that userID, then the userID is allowed that right (subject to "a" above). (R)
 - c. The system shall provide a mechanism to specify default access rights for userIDs not otherwise specified either explicitly by userID or implicitly by group membership. (R)
6. A userID's access rights to a resource shall be checked, at a minimum, when access to that resource is initiated. (R)
7. The system shall provide a mechanism to specify the owner(s) of the resource (in other words, the user(s) who can modify the contents of a resource's access control list). The use of this mechanism shall be limited to current owner(s) and user(s) who have privileges. (R)

- a. There should be a distinct access right to modify the contents of a resource's access control list (for example, an "ownership" or "control" access right). (A)
8. The system shall provide a mechanism to modify the contents of a resource's access control list. The use of this mechanism shall be limited to owner(s) and user(s) who have privileges. (R)
9. The system shall provide a mechanism to specify the default contents of the access control list of a newly created resource. The system-supplied default contents shall specify that only the creator of the resource has any access rights. (R)
10. The system should provide a mechanism to control access to resources based on the following items (the use of this mechanism should be limited to the owner(s) of the resource and users who have privileges):
 - a. Means of access or port of entry (A)
 - b. Time of day (A)
 - c. Day of the week (A)
 - d. Calendar date (A)
 - e. Specific program used to access the resource (A)
11. The system shall provide a mechanism to identify all resources in the system that are owned by a specified userID, the resources to which that userID is allowed access, and the specific access right(s) for each resource. The use of this mechanism shall require privileges. (R)
12. The system shall provide a mechanism to deny specific access rights to all resources for specified userIDs or groups. This mechanism shall override the standard resource access control mechanisms. The use of this mechanism shall require privileges. (R)
13. Each resource delivered with the system shall have the most restrictive access rights possible to permit the intended use of that resource. (R)
14. The system shall protect all information used for resource access control decisions (for example, access control lists, group lists, and system date and time). (R)

3.2.2.1 Object Reuse

Resources owned by a user or by the system are deallocated when no longer needed, but data that are left in these deallocated resources continue to be protected from disclosure. This protection is the purpose of the following requirements for object reuse:

Requirements:

1. The system shall ensure that users who do not possess an appropriate privilege are not able to access the contents of a resource that has been returned to the system after use. (R)
2. The system shall ensure that a user is not able to access the prior contents of a resource that has been allocated to that user by the system. (R)

3.2.3 Privileges

A privilege enables a user to perform a security-relevant operation or a command that, by default, is denied to that user. Privileges must be tightly controlled, and users who have privileges must be accountable for security-relevant actions. The requirements supporting the privilege mechanism are as follows:

Requirements:

- A. The system shall support a privilege mechanism that meets the following requirements:
 - 1. Separate privileges shall be associated with groups of related security- relevant operations or commands. (R)
 - a. Separate and distinct privileges should be associated with distinct security-relevant operations. (A)
 - b. Privileges that permit overriding or bypassing the access control mechanisms should be separate and distinct from any and all other privileges. (A)
 - 2. A user shall be assigned a privilege in order to invoke the corresponding operation. (R)
 - a. There should be an *application program interface* (API) that enables an application with privileges to dynamically assign privileges to itself. (A)
 - b. The system shall provide a mechanism to associate privileges with userIDs. The use of this mechanism shall require a separate and distinct privilege. (R)

3.3 Audit

Audit supports accountability by providing a trail of user actions. Actions are associated with individual users for all security-relevant events and are stored in an audit trail. This audit trail can be examined to determine what happened and which user was responsible for a security-relevant event. The audit trail data must be protected from unauthorized access, modification, or destruction. In addition, the audit trail data must be available in an easily readable form and in a timely manner for analysis. The requirements for data recording are presented in the first subsection. The requirements for data reporting are presented in the subsequent subsection.

3.3.1 Data Recording

Audit data is recorded from several sources (such as the logon host's operating system or a remote application) to produce a complete picture of a user's security-relevant actions. Therefore, audit data must be correlated across audit collection systems. The mechanisms providing audit data recording must be tailorable to each system's needs. Both the audit data itself and the mechanisms to determine what audit data is recorded are protected by privileges. The following requirements support data recording:

Requirements:

- 1. The system shall provide a mechanism for generating a security audit trail that contains information to support after-the-fact investigation of loss or impropriety and appropriate management response. The system shall support an API that enables an application that has privileges to append data to the security audit trail or to an applications-specified alternative security audit trail. (R)
- 2. The system shall provide end-to-end user accountability for all security-relevant events. The user identification information associated with any system request or activity shall be maintained and passed on to any other connected systems so that the initiating user can be made accountable for the lifetime of the request or activity. (R)
- 3. The system shall protect the security audit trail from unauthorized access. (R)
 - a. Maintenance and management of the security audit trail files shall require privileges. (R)

- b. The system should support an option to maintain the security audit trail data in encrypted format. (A)
- 4. The system shall provide a mechanism to dynamically control, during normal system operation, the types of events recorded. This mechanism shall include selective disabling of the recording of default audit events and the enabling and disabling of other events. The use of this mechanism shall require privileges. (R)
 - a. It shall not be possible to disable the recording of activities that require privileges. (R)
 - b. The system shall record any modification to the set of audited events. (R)
- 5. The system shall protect the audit control mechanisms from unauthorized access. (R)
- 6. The system shall, by default, cause a record to be written to the security audit trail for at least each of the following events:
 - a. Failed user authentication attempts (R)
 - b. Resource access attempts that are denied by the resource access control mechanism (R)
 - c. Attempts, both successful and unsuccessful, to obtain privileges (R)
 - d. Activities that require privileges (R)
 - e. Successful accesses of security-critical resources (R)
 - f. Changes to users' security information (R)
 - g. Changes to the set of privileges associated with a user (R)
 - h. Changes to access rights of resources (R)
 - i. Changes to the system security configuration (R)
 - j. Modification of system-supplied software (R)
- 7. The system shall provide a mechanism to enable or disable the recording of other events into the security audit trail. The use of this mechanism shall require privileges. These events shall include, at a minimum, the following elements:
 - a. Successful user authentication attempts (R)
 - b. Creation and deletion of resources (R)
 - c. Disk file access (R)
 - d. Tape volume or tape file access (R)
 - e. Program execution (R)
 - f. Online command execution (R)
 - g. Customer-defined events (R)
 - h. Activities of a specified userID (R)
- 8. For each recorded event, the audit record shall identify, at a minimum, the following items:
 - a. Date and time of the event (R)
 - b. UserID and associated point of physical access (for example, the terminal, port, network address, or communication device) (R)
 - c. Type of event (R)
 - d. Names of resources accessed (R)
 - e. Success or failure of the event (R)
- 9. The character strings inputted as a response to a password challenge shall not be recorded in the security audit trail. (R)
- 10. The audit control mechanism shall provide an option to enable or disable the recording of invalid userIDs during failed user authentication attempts. (R)

11. Audit control data (for example, audit event masks) shall survive system restarts. (R)
12. The system shall provide a mechanism for the automatic copying of security audit trail files to an alternative storage area after a customer-specifiable period of time. (R)
13. The system shall provide a mechanism for the automatic deletion of security audit trail files after a customer-specifiable period of time. It shall be possible to disable this mechanism. The system-supplied default shall be 30 days. (R)
14. The system shall allow site control of the procedure to be invoked when audit records are unable to be recorded. Options provided to handle this condition shall include the following:
 - a. Generate an alarm. This action shall be the default action. (R)
 - b. Initiate secure system shutdown. (R)
15. The system shall provide tools to monitor the activities (in other words, capture the keystrokes) of specific terminals or network connections in real time. The use of these tools shall require a separate and distinct privilege. (R)

3.3.2 Data Reporting

Once the audit data is recorded, it is analyzed and reported. Reporting can be done by reports generated on request or by alarms that are generated immediately when security violations are detected. The following requirements support data reporting:

Requirements:

1. The system shall provide a mechanism for reporting alarms. The system shall provide a mechanism for specifying how (for example, where or to whom) alarms are reported. The use of this mechanism shall require privileges. (R)
2. The system shall provide post-collection audit-analysis tools that can produce exception reports, summary reports, and detailed reports concerning specific data items, users, or communications facilities. The use of these tools shall require privileges. (R)
 - a. The system shall provide a tool to independently and selectively review the actions of any one or more users, including users who have privileges, based on individual user identity. (R)
 - b. The system shall provide a tool to produce a report of all occurrences of modifications to any resources. (R)
 - c. These tools shall be capable of being run concurrently with normal system operations. (R)
3. The system should contain a real-time mechanism that is able to monitor the occurrence or accumulation of security-relevant events that might indicate an imminent security violation. This mechanism should be able to generate an alarm when thresholds are exceeded, and if the occurrence or accumulation of these security-relevant events continues, the system should take the least-disruptive action in order to terminate the event. (A)

3.4 System Integrity

Users expect to share computer resources without interference or damage from other users. This concept is called system integrity. The requirements that follow provide for mechanisms that promote the separation of user and system processes and data,

protection of software, firmware, and hardware from unauthorized modifications (whether deliberate or accidental), and control of operator and maintenance personnel actions.

Requirements:

1. The system shall separate and protect a user process and its internal data from other user processes. The system's internal programs and internal data shall be separated and protected from any user processes. (R)
2. Mechanisms (for example, modification dates, checksums, and digital signatures) shall exist that make it possible to verify that the currently installed software has remained consistent with the delivered software (in other words, no unauthorized modifications have been made). (R)
3. The system shall restrict the use of the following items:
 - a. Privileged instructions (R)
 - b. Supervisory state or other privileged hardware states (R)
4. The system shall control and audit the use of any operator consoles. (R)
5. Modification or replacement of the software provided with the system shall require privilege. (R)
6. Execution of system maintenance and repair software shall require privileges. (R)
7. The system shall provide mechanisms that can be used to validate the correct operation of the system. These mechanisms shall address the following items:
 - a. Monitoring of system resources (R)
 - b. Correct operation of on-site hardware and firmware elements (R)
 - c. Corruption of access control information (R)
 - d. Detection of communication errors above a customer-specifiable threshold (R)

3.5 Data Integrity

Users expect data to be entered and maintained in a correct, consistent state. This concept is called data integrity. This expectation applies to both user data and system data. The requirements that follow provide for mechanisms that promote the tracking of changes to resources and the protection of data against exposure, unauthorized modification, or deletion as it is transmitted and while it is stored:

Requirements:

1. The system shall provide a mechanism to determine the date and time that a resource was last modified. The use of this mechanism shall be limited to users who have access rights to that resource and users who have privileges. (R)
2. The system shall provide a mechanism to verify the integrity of data in a resource (for example, a checksum or digital signature). The system shall provide a mechanism to verify the integrity of information passed across a communication channel. (R)
3. The system should provide an encryption mechanism that can be used to preserve the integrity of data in a resource. (A)
4. The system shall provide a tool for checking file system and storage medium integrity. The system shall execute this tool periodically. (R)
5. The system shall provide a mechanism to generate a status report detailing the values of all parameters and flags that affect the secure operation of the system. The use of this mechanism shall require privileges. (R)

6. If the system command interpreter provides a mechanism for users to control the order of directory/path search for command resolution, then:
 - a. System-supplied commands shall be executed by default. (R)
 - b. The system should enable a user who has privileges to revoke user access to this mechanism on a per-userID basis. (A)

3.6 Reliability of Service

Users expect a quantifiable and reliable level of service from a system. The requirements that follow provide for mechanisms that promote the continuous accessibility and usability of resources by an authorized user. These mechanisms also enable the prevention or limitation of interference with time-critical operations and enable the system to maintain its expected level of service in the face of any user action that is threatening this level, whether the action is deliberate or accidental.

Requirements:

1. The system should detect and report all conditions that degrade service below a customer-specifiable minimum. When possible, the system should isolate and report the source of the condition. (A)
2. The system shall provide a mechanism for controlling the consumption of disk space and CPU usage on a per-userID and per-group basis. (R)
3. The system shall provide a mechanism to allow recovery after a system failure or other discontinuity without a security compromise. (R)
4. The system shall provide a mechanism to support software and data backup and restoration. (R)
5. The system shall provide synchronization points (for example, checkpoint restarts) in order to facilitate recovery. (R)

4. Assurance Requirements

The TCSEC and ITSEC recognize that the presence of security features alone is not sufficient for ensuring a secure product. Underlying the security features must be a process of product development in order to provide assurance that the security features actually work as claimed and that no security flaws were introduced as a result of the development process. In addition, documentation must be provided that supports the secure installation, operation, administration, and use of the product.

The requirements that constrain the product development process and that specify the documentation to be produced are commonly called assurance requirements. The assurance requirements that follow have been included in order to complete the document. Originally, these requirements were part of the functionality requirements.

Requirements

Section 4.1 presents assurance requirements for the product development process, and Section 4.2 presents the product documentation requirements.

4.1 Product Development Assurances

The MSR-conformant system is one that has been designed, implemented, and tested in order to ensure that it meets acceptable, basic security assurance requirements. Specifically, the system has not been designed with any mode of access that would violate or bypass the basic security functionality requirements of the product. The following requirements are intended to provide assurance that the security features of the system will operate as expected.

1. Security mechanisms shall be protected from external interference (for example, modifications to its code or data structures). (R)

4.2 Product Documentation Assurances

The MSR-conformant system provides documentation for users, administrators, and operators in order to support the secure installation, operation, administration, and use of the product. The requirements for product documentation assurances are intended to ensure that security breaches do not occur because available security features are not used or are used improperly.

The requirements for user documentation are presented in the first subsection. The requirements for administrator and operator documentation are presented in subsequent subsections.

1. Instructions and documentation on security considerations shall be provided separately for users of the system, administrators of the system, and operators of the system. (R)

4.2.1 User Documentation

1. User documentation shall include a description of the security mechanisms that are non-transparent to the user, an explanation of their purpose, and guidelines as to their use. (R)

4.2.2. Administrator Documentation

1. Administrator documentation shall include the following components:
 - a. Cautions about functions and privileges that need to be controlled when running a secure facility. (R)
 - b. Documentation on the use of all audit tools. This documentation shall contain:
 1. Recommended procedures for examining and maintaining the audit trail files (R)
 2. A detailed audit record structure for each type of audit event (R)
 3. Recommended procedures for the periodic backup and deletion of audit trail files (R)
 4. Recommended procedures for checking the amount of free disk space available for the audit trail files (R)
 - a. Detailed descriptions of the administrative functions related to security, including adding or deleting a userID, changing the security characteristics of a user, and so on (R)
 - b. A description of the basic set of privileges required for an operator and for an administrator (R)
 - c. Recommended procedures for protecting vendor-supplied userIDs (R)
 - d. Recommendations on setting the basic access permissions on all files and directories (R)
 - e. Recommendations for running file system or disk integrity-checking utilities on a regular basis (R)
 - f. Guidelines on the consistent and effective use of the protection features of the system, how they interact, and how to securely generate a new system (R)

- g. A list of all security parameters that are under administrator control (R)
- h. Recommendations for site security self-assessment techniques, procedures, and reports (R)
- i. Recommendations for password requirements, dial-access restrictions, contingency plans, disaster recovery plans, and so on (R)
- j. A section that addresses common intrusion techniques and other threats and procedures for detecting and preventing them (R)

4.2.3 Operator Documentation

1. Operator documentation shall include the following items:
 - a. Procedures that are necessary to initially start (in other words, boot) the system in a secure manner (R)
 - b. Procedures to resume secure system operation after any lapse in system operation (R)
 - c. Recommendations and procedures for running software and data backup and restoration (R).

[*]Source: Computer Security Division, Computer Systems Laboratory, National Institute of Standards and Technology. March 1993.

Appendix C: Answers to Sample Questions

Chapter 1—Security Management Practices

1. Which formula accurately represents an Annualized Loss Expectancy (ALE) calculation? ?
- A. MAN stands for Metropolitan Area Network
 - B. Asset Value (AV) x EF
 - C. ARO x EF – SLE
 - D. % of ARO x AV
2. What is an ARO? ?
- A. A dollar figure that is assigned to a single event
 - B. The annual expected financial loss to an organization from a threat
 - C. A number that represents the estimated frequency of an occurrence of an expected threat
 - D. The percentage of loss a realized threat event would have on a specific asset
3. Which choice MOST accurately describes the difference between the role of a data owner versus the role of data custodian? ?
- A. The custodian implements the information classification scheme after the initial assignment by the owner.
 - B. The data owner implements the information classification scheme after the initial assignment by the custodian.
 - C. The custodian makes the initial information classification assignments and the operations manager implements the scheme.
 - D. The custodian implements the information classification scheme after the initial assignment by the operations manager.
4. Which choice is NOT an accurate description of C.I.A.? ?

- A. C stands for confidentiality
B. I stands for integrity
C. A stands for availability
D. A stands for authorization
5. Which group represents the MOST likely source of an asset loss through inappropriate computer use? ?
- A. Crackers
B. Hackers
C. Employees
D. Saboteurs
6. Which choice is the BEST description of authentication as opposed to authorization? ?
- A. The means in which a user provides a claim of their identity to a system
B. The testing or reconciliation of evidence of a user's identity
C. A system's ability to determine the actions and behavior of a single individual within a system
D. The rights and permissions granted to an individual to access a computer resource
7. What is a noncompulsory recommendation on how to achieve compliance with published standards called? ?
- A. Procedures
B. Policies
C. Guidelines
D. Standards
8. Place the following four information classification levels in their proper order, from the least sensitive classification to the most sensitive. ?
- A. SBU
B. Top secret
C. Unclassified
D. Secret
9. How is an SLE derived? ?
- A. (Cost 2 benefit) 3 (% of Asset Value)
B. AV 3 EF
C. ARO 3 EF

10. D. % of AV 2 implementation cost
What are the detailed instructions on how to perform or implement a control called? ?
- A. Procedures
 - B. Policies
 - C. Guidelines
 - D. Standards
11. What the BEST description of risk reduction? ?
- A. Altering elements of the enterprise in response to a risk analysis
 - B. Removing all risk to the enterprise at any cost
 - C. Assigning any costs associated with risk to a third party
 - D. Assuming all costs associated with the risk internally
12. Which choice MOST accurately describes the differences between standards, guidelines, and procedures? ?
- A. Standards are recommended policies and guidelines are mandatory policies.
 - B. Procedures are step-by-step recommendations for complying with mandatory guidelines.
 - C. Procedures are the general recommendations for compliance with mandatory guidelines.
 - D. Procedures are step-by-step instructions for compliance with mandatory standards.
13. A purpose of a security awareness program is to improve ?
- A. The security of vendor relations
 - B. The performance of a company's intranet
 - C. The possibility for career advancement of the IT staff
 - D. The company's attitude about safeguarding data.
14. What is the MOST accurate definition of a safeguard? ?

- A. A guideline for policy recommendations
 - B. A step-by-step instructional procedure
 - C. A control designed to counteract a threat
 - D. A control designed to counteract an asset
15. What does an Exposure Factor (EF) describe? ?
- A. A dollar figure that is assigned to a single event
 - B. A number that represents the estimated frequency of the occurrence of an expected threat
 - C. The percentage of loss a realized threat event would have on a specific asset
 - D. The annual expected financial loss to an organization from a threat
16. Which choice would be an example of a cost-effective way to enhance security awareness in an organization? ?
- A. Train every employee in advanced InfoSec
 - B. Create an award or recognition program for employees
 - C. Calculate the cost-to-benefit ratio of the asset valuations for a risk analysis
 - D. Train only managers in implementing InfoSec controls
17. What is the prime directive of Risk Management? ?
- A. Reduce the risk to a tolerable level
 - B. Reduce all risk regardless of cost
 - C. Transfer any risk to external third parties
 - D. Prosecute any employees that are violating published security policies
18. Which choice MOST closely depicts the difference between qualitative and quantitative risk analysis? ?

- A. A quantitative RA does not use the hard costs of losses and a qualitative RA does.
- B. A quantitative RA uses less guesswork than a qualitative RA.
- C. A qualitative RA uses many complex calculations.
- D. A quantitative RA cannot be automated.
19. Which choice is NOT a good criteria for selecting a safeguard? ?
- A. The ability to recover from a reset with the permissions set to "allow all"
- B. Comparing the potential dollar loss of an asset to the cost of a safeguard
- C. The ability to recover from a reset without damaging the asset
- D. The accountability features for tracking and identifying operators
20. Which policy type is MOST likely to contain mandatory or compulsory standards? ?
- A. Guidelines
- B. Advisory
- C. Regulatory
- D. Informative
21. What are high-level policies? ?
- A. They are recommendations for procedural controls.
- B. They are the instructions on how to perform a Quantitative Risk Analysis.
- C. They are statements that indicate a senior management's intention to support InfoSec.
- D. They are step-by-step procedures to implement a safeguard.

Answers

1. *Answer:* a). b) is the formula for an SLE, and c) and d) are nonsense.

2. *Answer: c).* a) is the definition of SLE, b) is an ALE, and d) is an EF.
3. *Answer: a).*
4. *Answer: d).*
5. *Answer: c).* Internal personnel far and away constitute the largest amount of dollar loss due to unauthorized or inappropriate computer use.
6. *Answer: b).* a) is identification, c) is accountability, and d) is authorization.
7. *Answer: c).*
8. *Answer: c), a), d), and b).*
9. *Answer: b).* The other answers do not exist.
10. *Answer: a).*
11. *Answer: a).* b) is not possible or desirable, c) is risk transference, and d) is risk acceptance
12. *Answer: d).* The other answers are faulty.
13. *Answer: d).*
14. *Answer: c).* a) is a guideline, b) is a procedure, and d) is nonsense
15. *Answer: c).* a) is a SLE, b) is an ARO, and d) is a ALE
16. *Answer: b)*
17. *Answer: a).* Risk can never be eliminated, and Risk Management must find the level of risk the organization can tolerate and still function effectively.
18. *Answer: b).* The other answers are incorrect.
19. *Answer: a).* Permissions should be set to “deny all” during reset.
20. *Answer: c).* Advisory policies might specify penalties for non-compliance, but regulatory policies are required to be followed by the organization. The other two are informational or recommended only.
21. *Answer: c).* High-level policies are senior management statements of recognition of the importance of InfoSec controls.

Chapter 2—Access Control Systems and Methodology

1. The goals of integrity do NOT include
 - A. Accountability of responsible individuals
 - B. Prevention of the modification of information by unauthorized users
 - C. Prevention of the unauthorized or unintentional modification of information by authorized users
 - D. Preservation of internal and external consistency

?

2. Kerberos is an authentication scheme that can be used to implement ?
A. Public key cryptography
B. Digital signatures
C. Hash functions
D. Single Sign-On
3. The fundamental entity in a relational database is the ?
A. Domain
B. Relation
C. Pointer
D. Cost
4. In a relational database, security is provided to the access of data through ?
A. Candidate keys
B. Views
C. Joins
D. Attributes
5. In biometrics, a “one-to-one” search to verify an individual’s claim of an identity is called ?
A. Audit trail review
B. Authentication
C. Accountability
D. Aggregation
6. Biometrics is used for identification in the physical controls and for authentication in the ?
A. Detective controls
B. Preventive controls
C. Logical controls
D. Corrective controls
7. Referential Integrity requires that for any foreign key attribute, the referenced relation must have ?
A. A tuple with the same value for its primary key
B. A tuple with the same value for its secondary key
C. An attribute with the same value for its secondary key
D. An attribute with the same value for its other foreign key
8. A password that is the same for each log-on is called a ?
A. Dynamic password

- B. Static password
C. Passphrase
D. One-time pad
9. The number of times a password should be changed is NOT a function of ?
- A. The criticality of the information to be protected
B. The frequency of the password's use
C. The responsibilities and clearance of the user
D. The type of workstation used
10. The description of a relational database is called the ?
- A. Attribute
B. Record
C. Schema
D. Domain
11. A statistical anomaly-based intrusion detection system ?
- A. Acquires data to establish a normal system operating profile
B. Refers to a database of known attack signatures
C. Will detect an attack that does not significantly change the system's operating characteristics
D. Does not report an event that caused a momentary anomaly in the system
12. Intrusion detection systems can be all of the following types EXCEPT ?
- A. Signature-based
B. Statistical anomaly-based
C. Network-based
D. Defined-based
13. In a relational data base system, a primary key is chosen from a set of ?
- A. Foreign keys
B. Secondary keys
C. Candidate keys
D. Cryptographic keys

14. A standard data manipulation and relational database definition language is ?
- A. OOD
 - B. SQL
 - C. SLL
 - D. Script
15. An attack that can be perpetrated against a remote user's callback access control is ?
- A. Call forwarding
 - B. A Trojan horse
 - C. A maintenance hook
 - D. Redialing
16. The definition of CHAP is ?
- A. Confidential Hash Authentication Protocol
 - B. Challenge Handshake Authentication Protocol
 - C. Challenge Handshake Approval Protocol
 - D. Confidential Handshake Approval Protocol
17. Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network and facilitates communications through the assignment of ?
- A. Public keys
 - B. Session keys
 - C. Passwords
 - D. Tokens
18. Three things that must be considered for the planning and implementation of access control mechanisms are ?
- A. Threats, assets, and objectives
 - B. Threats, vulnerabilities, and risks
 - C. Vulnerabilities, secret keys, and exposures
 - D. Exposures, threats, and countermeasures
19. In mandatory access control, the authorization of a subject to have access to an object is dependent upon ?
- A. Labels
 - B. Roles
 - C. Tasks

20. D. Identity
The type of access control that is used in local, dynamic situations where subjects have the ability to specify what resources certain users may access is called
- A. Mandatory access control
 - B. Rule-based access control
 - C. Sensitivity-based access control
 - D. Discretionary access control
21. Role-based access control is useful when
- A. Access must be determined by the labels on the data
 - B. There are frequent personnel changes in an organization
 - C. Rules are needed to determine clearances
 - D. Security clearances must be used
22. Clipping levels are used to
- A. Limit the number of letters in a password
 - B. Set thresholds for voltage variations
 - C. Reduce the amount of data to be evaluated in audit logs
 - D. Limit errors in callback systems
23. Identification is
- A. A user being authenticated by the system
 - B. A user providing a password to the system
 - C. A user providing a shared secret to the system
 - D. A user professing an identity to the system
24. Authentication is
- A. The verification that the claimed identity is valid
 - B. The presentation of a user's ID to the system
 - C. Not accomplished through the use of a password
 - D. Only applied to remote users

25. An example of two-factor authentication is ?
 A. A password and an ID
 B. An ID and a PIN
 C. A PIN and an ATM card
 D. A fingerprint
26. In biometrics, a good measure of performance of a system is the ?
 A. False detection
 B. Crossover Error Rate (CER)
 C. Positive acceptance rate
 D. Sensitivity
27. In finger scan technology, ?
 A. The full fingerprint is stored.
 B. Features extracted from the fingerprint are stored.
 C. More storage is required than in fingerprint technology.
 D. The technology is applicable to large one-to-many database searches.
28. An acceptable biometric throughput rate is ?
 A. One subject per two minutes
 B. Two subjects per minute
 C. Ten subjects per minute
 D. Five subjects per minute
29. In a relational database, the *domain* of a relation is the set of allowable values ?
 A. That an attribute can take
 B. That tuples can take
 C. That a record can take
 D. Of the primary key
30. Object-Oriented Database (OODB) systems: ?
 A. Are ideally suited for text-only information
 B. Require minimal learning time for programmers
 C. Are useful in storing and manipulating complex data such as images and graphics
 D. Consume minimal system resources

Answers

1. *Answer:* a). Accountability is holding individuals responsible for

- their actions. Answers b, c and d are the three goals of integrity.
2. *Answer: d).* Kerberos is a third-party authentication protocol that can be used to implement single sign-on. Answer a is incorrect since public key cryptography is not used in the basic Kerberos protocol. Answer b is a public key-based capability, and answer c is a one-way transformation used to disguise passwords or to implement digital signatures.
 3. *Answer: b).* The fundamental entity in a relational database is the relation in the form of a table. Answer a is the set of allowable attribute values and answers c and d are distractors.
 4. *Answer: b).* Answer a, candidate keys, are the set of unique keys from which the primary key is selected. Answer c, Joins, are operations that can be performed on the database, and the attributes (d) denote the columns in the relational table.
 5. *Answer: b).* Answer a is a review of audit system data, usually done after the fact. Answer c is holding individuals responsible for their actions, and answer d is obtaining higher sensitivity information from a number of pieces of information of lower sensitivity.
 6. *Answer: c).* The other answers are different categories of controls where preventive controls attempt to eliminate or reduce vulnerabilities before an attack occurs; detective controls attempt to determine that an attack is taking place or has taken place; and corrective controls involve taking action to restore the system to normal operation after a successful attack.
 7. *Answer: a).* Answers b and c are incorrect since a secondary key is not a valid term. Answer d is a distractor since referential integrity has a foreign key referring to a primary key in another relation.
 8. *Answer: b).* In answer a, the password changes at each logon. For answer c, a passphrase is a long word or phrase that is converted by the system to a password. In answer d, a one-time pad refers to a using a random key only once when sending a cryptographic message.
 9. *Answer: d).* The type of workstation used as the platform is not the determining factor. Items a, b and c are determining factors.
 10. *Answer: c).* The other answers are portions of a relation or table.
 11. *Answer: a).* A statistical anomaly-based intrusion detection system acquires data to establish a normal system operating profile. Answer b is incorrect since it is used in signature-based intrusion detection. Answer c is incorrect since a statistical anomaly-based intrusion detection system will not detect an attack that does not significantly change the system operating characteristics. Similarly, answer d is incorrect since the statistical anomaly-based IDS is susceptible to reporting an event that caused a momentary anomaly in the system.
 12. *Answer: d).* All the other answers are types of IDS.
 13. *Answer: c).* Candidate keys by definition. Answer a is incorrect

since a foreign key in one table refers to a primary key in another. Answer b is a made-up distractor and answer d refers to keys used in encipherment and decipherment.

14. *Answer:* b). All other answers do not apply.
15. *Answer:* a). A cracker can have a person's call forwarded to another number to foil the call back system. Answer b is incorrect since it is an example of malicious code embedded in useful code. Answer c is incorrect since it might enable bypassing controls of a system through means used for debugging or maintenance. Answer d is incorrect since it is a distractor.
16. *Answer:* b).
17. *Answer:* b). Session keys are temporary keys assigned by the KDC and used for an allotted period of time as the secret key between two entities. Answer a is incorrect since it refers to asymmetric encryption that is not used in the basic Kerberos protocol. Answer c is incorrect since it is not a key, and answer d is incorrect since a token generates dynamic passwords.
18. *Answer:* b). Threats define the possible source of security policy violations, vulnerabilities describe weaknesses in the system that might be exploited by the threats, and the risk determines the probability of threats being realized. All three items must be present to meaningfully apply access control. Therefore, the other answers are incorrect.
19. *Answer:* a). Mandatory access controls use labels to determine if subjects can have access to objects, depending on the subjects' clearances. Answer b, roles, is applied in non-discretionary access control as is answer c, tasks. Answer d, identity, is used in discretionary access control.
20. *Answer:* d). Answers a and b require strict adherence to labels and clearances. Answer c is a made-up distractor.
21. *Answer:* b). Role-based access control is part of non-discretionary access control. Answers a, c and d relate to mandatory access control.
22. *Answer:* c). Reducing the amount of data to be evaluated, by definition. Answer a is incorrect since clipping levels do not relate to letters in a password. Answer b is incorrect since clipping levels in this context have nothing to do with controlling voltage levels. Answer d is incorrect since they are not used to limit call back errors.
23. *Answer:* d). A user presents an ID to the system as identification. Answer a is incorrect since presenting an ID is not an authentication act. Answer b is incorrect since a password is an authentication mechanism. Answer c is incorrect since it refers to cryptography or authentication.
24. *Answer:* a). Answer b is incorrect since it is an identification act. Answer c is incorrect since authentication can be accomplished through the use of a password. Answer d is incorrect since authentication is applied to local and remote users.
25. *Answer:* c). These items are something you know and something you have. Answer a is incorrect since, essentially,

only one factor is being used, something you know (password.) Answer b is incorrect for the same reason. Answer d is incorrect since only one biometric factor is being used.

26. *Answer: b).* The other items are made-up distractors.
27. *Answer: b).* The features extracted from the fingerprint are stored. Answer a is incorrect since the equivalent of the full fingerprint is not stored in finger scan technology. Answers c and d are incorrect since the opposite is true of finger scan technology.
28. *Answer: c).*
29. *Answer: a).*
30. *Answer: c).* The other answers are false since for a., relational databases are ideally suited to text-only information, b. and d., OODB systems have a steep learning curve and consume a large amount of system resources .

Chapter 3—Telecommunications and Network Security

1. Which of the following is NOT a type of data network? ?
- A. LAN
 - B. WAN
 - C. MAN
 - D. GAN
2. Which of the following is NOT a network cabling type? ?
- A. Twisted Pair
 - B. Token Ring
 - C. Fiber Optic
 - D. Coaxial
3. Which of the following is NOT a property of a Packet Filtering Firewall? ?
- A. Considered a first generation firewall
 - B. Uses ACLs
 - C. Operates at the Application Layer
 - D. Examines the source and destination addresses of the incoming packet
4. Which of the following is NOT a remote computing technology? ?
- A. PGP
 - B. ISDN
 - C. Wireless
 - D. xDSL

5. A firewall that performs stateful inspection of the data packet across all layers is considered a ?
- A. First generation firewall
 - B. Second generation firewall
 - C. Third generation firewall
 - D. Fourth generation firewall
6. RAID refers to the ?
- A. Redundant Arrays of Intelligent Disks
 - B. Redundant And fault tolerant Internetworking Devices
 - C. Rapid And Inexpensive Digital tape backup
 - D. Remote Administration of Internet Domains
7. Which of the following is NOT a true statement about Network Address Translation (NAT)? ?
- A. NAT is used when corporations want to use private addressing ranges for internal networks.
 - B. NAT is designed to mask the true IP addresses of internal systems.
 - C. Private addresses can easily be globally routable.
 - D. NAT translates private IP addresses to registered "real" IP addresses.
8. What does LAN stand for? ?
- A. Local Arena News
 - B. Local Area Network
 - C. Layered Addressed Network
 - D. Local Adaptive Network
9. What does CSMA stand for? ?
- A. Carrier Station Multi-port Actuator
 - B. Carrier Sense Multiple Access
 - C. Common Systems Methodology Applications
 - D. Carrier Sense Multiple Attenuation
10. Which is NOT a property of a packet-switched network? ?

- A. Packets are assigned sequence numbers
 - B. Characterized by “bursty” traffic
 - C. Connection-oriented network
 - D. Connection-less network
11. Which is NOT a layer in the OSI architecture model? ?
- A. Transport
 - B. Internet
 - C. Data Link
 - D. Session
12. Which is NOT a layer in the TCP/IP architecture model? ?
- A. Internet
 - B. Application
 - C. Host-to-host
 - D. Session
13. Which is NOT a backup method type? ?
- A. Differential
 - B. Full
 - C. Reactive
 - D. Incremental
14. What does TFTP stands for? ?
- A. Trivial File Transport Protocol
 - B. Transport For TCP/IP
 - C. Trivial File Transfer Protocol
 - D. Transport File Transfer Protocol
15. What does the Data Encapsulation in the OSI model do? ?
- A. Creates seven distinct layers
 - B. Wraps data from one layer around a data packet from an adjoining layer
 - C. Provides “best effort” delivery of a data packet
 - D. Makes the network transmission deterministic
16. What is NOT a feature of TACACS+? ?
- A. Enables two-factor authentication
 - B. Replaces older frame relay-switched networks

- C. Enables a user to change passwords
 - D. Resynchronizes security tokens
17. What is NOT true of a star-wired topology? ?
- A. Cabling termination errors can crash the entire network.
 - B. The network nodes are connected to a central LAN device.
 - C. It has more resiliency than a BUS topology.
 - D. 10BaseT Ethernet is star-wired.
18. FDDI uses what type of network topology? ?
- A. BUS
 - B. RING
 - C. STAR
 - D. MESH
19. What does the protocol ARP do? ?
- A. Takes a MAC address and finds an IP address to match it with
 - B. Sends messages to the devices regarding the health of the network
 - C. Takes an IP address and finds out what MAC address it belongs to
 - D. Facilitates file transfers
20. What does the protocol RARP do? ?
- A. Takes a MAC address and finds an IP address to match it with
 - B. Sends messages to the devices regarding the health of the network
 - C. Takes an IP address and finds out what MAC address it belongs to
 - D. Facilitates file transfers
21. What is the protocol that supports sending and receiving email called? ?
- A. SNMP
 - B. SMTP

- C. ICMP
D. RARP
22. Which of the following is NOT a VPN remote computing protocol? ?
- A. PPTP
B. L2F
C. L2TP
D. UTP
23. Which of the following is NOT a property of CSMA? ?
- A. The workstation continuously monitors the line.
B. The workstation transmits the data packet when it thinks the line is free.
C. Workstations are not permitted to transmit until they are given permission from the primary host.
D. It does not have a feature to avoid the problem of one workstation dominating the conversation.
24. Which of the following is NOT a property of Token Ring networks? ?
- A. Workstations cannot transmit until they receive a token.
B. These networks were originally designed to serve large, bandwidth-consuming applications.
C. These networks were originally designed to serve sporadic and only occasionally heavy traffic.
D. All end stations are attached to a MSAU.
25. Which is NOT a property of Fiber Optic cabling? ?
- A. Carries signals as light waves
B. Transmits at higher speeds than copper cable
C. Easier to tap than copper cabling
D. Very resistant to interference
26. Which is NOT a property of a bridge? ?

- A. Forwards the data to all other segments if the destination is not on the local segment
- B. Operates at Layer 2, the Data Link Layer
- C. Operates at Layer 3, the Network Layer
- D. Can create a broadcast storm
- 27.** Which is NOT a standard type of DSL? **?**
- A. ADSL
- B. FDSL
- C. VDSL
- D. HDSL
- 28.** Which is a property of a circuit-switched network, as opposed to a packet-switched network? **?**
- A. Physical, permanent connections exist from one point to another in a circuit-switched network.
- B. The data is broken up into packets.
- C. The data is sent to the next destination, which is based on the router's understanding of the best available route.
- D. Packets are reassembled according to their originally assigned sequence numbers
- 29.** Which is NOT a packet-switched technology? **?**
- A. SMDS
- B. T1
- C. Frame Relay
- D. X.25
- 30.** Which is NOT a remote security method? **?**
- A. VoIP
- B. Callback
- C. Caller ID
- D. Restricted Address
- 31.** What does covert channel eavesdropping refer to? **?**
- A. Using a hidden, unauthorized network connection to communicate unauthorized information

- B. Nonbusiness or personal use of the Internet
- C. Socially engineering passwords from an ISP
- D. The use of two-factor passwords
32. What does logon abuse refer to? ?
- A. Breaking into a network primarily from an external source
- B. Legitimate users accessing networked services that would normally be restricted to them
- C. Nonbusiness or personal use of the Internet
- D. Intrusions via dial-up or asynchronous external network connections
33. What is probing used for? ?
- A. To induce a user into taking an incorrect action
- B. To give an attacker a road map of the network
- C. To use up all of a target's resources
- D. To covertly listen to transmissions
34. Which is NOT a property of or issue with tape backup? ?
- A. Slow data transfer during backups and restores
- B. Server disk space utilization expands
- C. Possible that some data re-entry may need to be performed after a crash
- D. One large disk created by using several disks
35. What is a Server Cluster? ?
- A. A primary server that mirrors its data to a secondary server
- B. A group of independent servers that are managed as a single system
- C. A tape array backup implementation

- D. A group of WORM optical jukeboxes
36. In which OSI layer does the MIDI digital music protocol standard reside? ?
- A. Application Layer
B. Presentation Layer
C. Session Layer
D. Transport Layer

Answers

1. *Answer:* d) GAN does not exist. LAN stands for Local Area Network, WAN stands for Wide Area Network, and MAN stands for Metropolitan Network.
2. *Answer:* b) Token Ring. Token Ring is a LAN media access method, not a cabling type.
3. *Answer:* c). A packet filtering firewall can operate at the Network or Transport Layers.
4. *Answer:* a). PGP stands for Pretty Good Privacy, an e-mail encryption technology.
5. *Answer:* c). A stateful inspection firewall is considered a third generation firewall.
6. *Answer:* a). Redundant Arrays of Intelligent Disks. The other acronyms do not exist.
7. *Answer:* c). Private addresses are not easily routable, thereby the reason for using NAT.
8. *Answer:* b).
9. *Answer:* b). The other acronyms do not exist.
10. *Answer:* c). Packet-switched networks are considered connection-less networks, circuit-switched networks are considered connection-oriented.
11. *Answer:* b). The Internet Layer is a TCP/IP architecture model layer.
12. *Answer:* d). The Session Layer is a OSI model layer.
13. *Answer:* c) Reactive is not a backup method.
14. *Answer:* c) The other acronyms do not exist.
15. *Answer:* b) Data Encapsulation attaches information from one layer to the packet as it travels from an adjoining layer. a) The OSI layered architecture model creates seven layers. c) the TCP/IP protocol UDP provides "best effort" packet delivery, and d) a token-passing transmission scheme creates a deterministic network because it's possible to compute the maximum predictable delay.
16. *Answer:* b). TACACS+ has nothing to do with frame relay networks.
17. *Answer:* a) Cabling termination errors are an inherent issue with bus topology networks.
18. *Answer:* b). FDDI is a RING topology, like Token Ring.
19. *Answer:* c). Address Resolution Protocol starts with an IP address, then queries the network to find the MAC, or

- hardware address of the workstation it belongs to. ICMP does b), RARP does a), and FTP does d).
20. *Answer:* a). The reverse of ARP. The Reverse Address Resolution Protocol knows a MAC (Media Access Control) address and asks the RARP server to match it with an IP address.
 21. *Answer:* b). Simple Mail Transport Protocol, queues and transfers email. SNMP stands for Simple Network Management Protocol. ICMP stands for Internet Control Message Protocol. RARP stands for Reverse Address Resolution Protocol
 22. *Answer:* d). UTP stands for unshielded twisted pair wiring.
 23. *Answer:* c). The Polling transmission type uses primary and secondary hosts, and the secondary must wait for permission from the primary before transmitting.
 24. *Answer:* c). Ethernet networks were originally designed to work with more sporadic traffic than token ring networks.
 25. *Answer:* c) Fiber Optic cable is much harder to tap than copper cable.
 26. *Answer:* c). A bridge operates at Layer 2, and therefore does not use IP addressing to make routing decisions.
 27. *Answer:* b). FDSL does not exist.
 28. *Answer:* a) Permanent connections are a feature of circuit-switched networks.
 29. *Answer:* b). A T1 line is a type of leased line, which uses a dedicated, point-to-point technology.
 30. *Answer:* a) VoIP stands for Voice-Over-IP, a digital telephony technology.
 31. *Answer:* a). A Covert Channel is a connection intentionally created to transmit unauthorized information from inside a trusted network to a partner at an outside, untrusted node. c) is called Masquerading.
 32. *Answer:* b). Logon abuse entails an otherwise proper user attempting to access areas of the network that are deemed off-limits. a) is called network intrusion and d) is called a back-door attack.
 33. *Answer:* b) Probing is a procedure where the intruder runs programs that scan the network to create a network map for later intrusion. a) is spoofing, c) is the objective of a denial of service attack, and d) is passive eavesdropping.
 34. *Answer:* d). RAID level 0, striping is the process of creating a large disk out of several smaller disks.
 35. *Answer:* b). A server cluster is a group of servers that appear to be a single server to the user. a) refers to Redundant Servers.
 36. *Answer:* b). MIDI is a Presentation layer protocol.

Chapter 4—Cryptography

1. The Secure Hash Algorithm (SHA) is specified in the

?

- A. Data Encryption Standard
 B. Digital Signature Standard
 C. Digital Encryption Standard
 D. Advanced Encryption Standard
2. What does Secure Sockets Layer (SSL)/Transaction Security Layer (TSL) do? ?
- A. Implements confidentiality, authentication, and integrity above the Transport Layer
 B. Implements confidentiality, authentication, and integrity below the Transport Layer
 C. Implements only confidentiality above the Transport Layer
 D. Implements only confidentiality below the Transport Layer
3. What are MD4 and MD5? ?
- A. Symmetric encryption algorithms
 B. Asymmetric encryption algorithms
 C. Hashing algorithms
 D. Digital certificates
4. Elliptic curves, which are applied to public key cryptography, employ modular exponentiation that characterizes the ?
- A. Elliptic curve discrete logarithm problem
 B. Prime factors of very large numbers
 C. Elliptic curve modular addition
 D. Knapsack problem
5. Which algorithm is used in the Clipper Chip? ?
- A. IDEA
 B. DES
 C. SKIPJACK
 D. 3 DES
6. The hashing algorithm in the Digital Signature Standard (DSS) generates a message digest of ?
- A. 120 bits
 B. 160 bits
 C. 56 bits
 D. 130 bit

7. The protocol of the Wireless Application Protocol (WAP), which performs functions similar to SSL in the TCP/IP protocol, is called the ?
- A. Wireless Application Environment (WAE)
 - B. Wireless Session Protocol (WSP)
 - C. Wireless Transaction Protocol (WTP)
 - D. Wireless Transport Layer Security Protocol (WTLS)
8. A Security Parameter Index (SPI) and the identity of the security protocol (AH or ESP) are the components of ?
- A. SSL
 - B. IPSec
 - C. S-HTTP
 - D. SSH-2
9. When two different keys encrypt a plaintext message into the same ciphertext, this situation is known as (a) ?
- A. Public key cryptography
 - B. Cryptanalysis
 - C. Key clustering
 - D. Hashing
10. What is the result of the Exclusive Or operation, $1 \oplus 0$? ?
- A. 1
 - B. 0
 - C. Indeterminate
 - D. 10
11. A block cipher ?
- A. Encrypts by operating on a continuous data stream
 - B. Is an asymmetric key algorithm
 - C. Converts a variable-length of plaintext into a fixed length ciphertext
 - D. Breaks a message into fixed length units for encryption
12. In most security protocols that support authentication, integrity and confidentiality, ?
- A. Public key cryptography is used to create digital

signatures.

- B. Private key cryptography is used to create digital signatures.
 - C. DES is used to create digital signatures.
 - D. Digital signatures are not implemented.
13. Which of the following is an example of a symmetric key algorithm? ?
- A. Rijndael
 - B. RSA
 - C. Diffie-Hellman
 - D. Knapsack
14. Which of the following is a problem with symmetric key encryption? ?
- A. Is slower than asymmetric key encryption
 - B. Most algorithms are kept proprietary
 - C. Work factor is not a function of the key size
 - D. Secure distribution of the secret key
15. Which of the following is an example of an asymmetric key algorithm? ?
- A. IDEA
 - B. DES
 - C. 3 DES
 - D. ELLIPTIC CURVE
16. In public key cryptography ?
- A. Only the private key can encrypt and only the public key can decrypt
 - B. Only the public key can encrypt and only the private key can decrypt
 - C. The public key is used to encrypt and decrypt
 - D. If the public key encrypts, then only the private key can decrypt
17. In a hybrid cryptographic system, usually ?
- A. Public key cryptography is used for the encryption of the message.

- B. Private key cryptography is used for the encryption of the message.
- C. Neither public key nor private key cryptography is used.
- D. Digital certificates cannot be used.
18. What is the block length of the Rijndael Cipher? ?
- A. 64 bits
- B. 128 bits
- C. Variable
- D. 256 bits
19. A polyalphabetic cipher is also known as a ?
- A. One-time pad
- B. Vigenère cipher
- C. Steganography
- D. Vernam cipher
20. The classic Caesar cipher is a ?
- A. Polyalphabetic cipher
- B. Monoalphabetic cipher
- C. Transposition cipher
- D. Code group
21. In Steganography, ?
- A. Private key algorithms are used.
- B. Public key algorithms are used.
- C. Both public and private key algorithms are used.
- D. The fact that the message exists is not known.
22. What is the key length of the Rijndael Block Cipher? ?
- A. 56 or 64 bits
- B. 512 bits
- C. 128, 192, or 256 bits
- D. 512 or 1024 bits
23. In a block cipher, diffusion ?
- A. Conceals the connection between the ciphertext and plaintext
- B. Spreads the influence of a plaintext character over many

- ciphertext characters
- C. Is usually implemented by non-linear S-boxes
- D. Cannot be accomplished
24. The NIST Advanced Encryption Standard uses the ?
- A. 3 DES algorithm
- B. Rijndael algorithm
- C. DES algorithm
- D. IDEA algorithm
25. The modes of DES do NOT include ?
- A. Electronic Code Book
- B. Cipher Block Chaining
- C. Variable Block Feedback
- D. Output Feedback
26. Which of the following is true? ?
- A. The work factor of triple DES is the same as for double DES.
- B. The work factor of single DES is the same as for triple DES.
- C. The work factor of double DES is the same as for single DES.
- D. No successful attacks have been reported against double DES.
27. The Rijndael Cipher employs a round transformation that is comprised of three *layers* of distinct, invertible transformations. These transformations are also defined as uniform, which means that every bit of the State is treated the same. Which of the following is NOT one of these layers? ?
- A. The non-linear layer, which is the parallel application of S-boxes that have the optimum worst-case nonlinearity properties
- B. The linear mixing layer, which provides a guarantee of the high diffusion of multiple rounds
- C. The key addition layer, which is an Exclusive Or of the Round Key to the intermediate State
- D. The key inversion layer, which provides confusion through the

- multiple rounds
28. The Escrowed Encryption Standard describes the ?
- A. Rijndael Cipher
 - B. Clipper Chip
 - C. Fair Public Key Cryptosystem
 - D. Digital certificates
29. Enigma was ?
- A. An English project created to break German ciphers
 - B. The Japanese rotor machine used in WWII
 - C. Probably the first programmable digital computer
 - D. The German rotor machine used in WWII
30. Which of the following characteristics does a one-time pad have if used properly? ?
- A. It can be used more than once.
 - B. The key does not have to be random.
 - C. It is unbreakable.
 - D. The key has to be of greater length than the message to be encrypted.
31. The DES key is ?
- A. 128 bits
 - B. 64 bits
 - C. 56 bits
 - D. 512 bits
32. In a digitally-signed message transmission using a hash function ?
- A. The message digest is encrypted in the private key of the sender.
 - B. The message digest is encrypted in the public key of the sender.
 - C. The message is encrypted in the private key of the sender.
 - D. The message is encrypted in the public key of the sender.
33. The strength of RSA public key encryption is based on the ?
- A. Difficulty in finding logarithms

- in a finite field
- B. Difficulty of multiplying two large prime numbers
 - C. Fact that only one key is used
 - D. Difficulty in finding the prime factors of very large numbers
34. Elliptic curve cryptosystems ?
- A. Have a higher strength per bit than an RSA
 - B. Have a lower strength per bit than an RSA
 - C. Cannot be used to implement digital signatures
 - D. Cannot be used to implement encryption
35. Which of the following is NOT a key management issue? ?
- A. Key recovery
 - B. Key storage
 - C. Key change
 - D. Key exchange

Answers

1. *Answer:* b). Answer a) refers to DES; a symmetric encryption algorithm; answer c) is a distractor, there is no such term; answer d) is the Advanced Encryption Standard, which has replaced DES and is now the Rijndael algorithm.
2. *Answer:* a) by definition. Answer b) is incorrect since SSL/TLS operate above the Transport Layer; answer c is incorrect since authentication and integrity are provided also, and answer d) is incorrect since it cites only confidentiality and SSL/TLS operate above the Transport Layer.
3. *Answer:* c). Answers a) and b) are incorrect since they are general types of encryption systems and answer d) is incorrect since hashing algorithms are not digital certificates
4. *Answer:* a). Modular exponentiation in elliptic curves is the analog of the modular discrete logarithm problem. Answer b) is incorrect since prime factors are involved with RSA public key systems; answer c is incorrect since modular addition in elliptic curves is the analog of modular multiplication; and answer d is incorrect since the knapsack problem is not an elliptic curve problem.
5. *Answer:* c). Answers a), b) and d) are other symmetric key algorithms.
6. *Answer:* b).
7. *Answer:* d). SSL performs security functions in TCP/IP. The other answers refer to protocols in the WAP protocol stack, also, but their primary functions are not security.

8. *Answer: b).* The SPI, AH and/or ESP and the destination IP address are components of an IPSec Security Association (SA.) The other answers describe protocols other than IPSec.
9. *Answer: c).* Answer a) describes a type of cryptographic system using a public and a private key; answer b) is the art/science of breaking ciphers; answer d) is the conversion of a message of variable length into a fixed length message digest.
10. *Answer: a).* An XOR operation results in a 0 if the two input bits are identical and a 1 if one of the bits is a 1 and the other is a 0.
11. *Answer: d).* Answer a) describes a stream cipher; answer b) is incorrect since a block cipher applies to symmetric key algorithms; and answer c describes a hashing operation.
12. *Answer: a).* Answer b) is incorrect since private key cryptography does not create digital signatures; answer c) is incorrect since DES is a private key system and therefore, follows the same logic as in b; and answer d) is incorrect since digital signatures are implemented to obtain authentication and integrity.
13. *Answer: a).* The other answers are examples of asymmetric key systems.
14. *Answer: d).* Answer a) is incorrect since the opposite is true, answer b) is incorrect since most symmetric key algorithms are published, and answer c) is incorrect since work factor is a function of key size. The larger the key, the larger the work factor.
15. *Answer: d).* All the other answers refer to symmetric key algorithms.
16. *Answer: d).* Answers a) and b) are incorrect since, if one key encrypts, the other can decrypt and answer c) is incorrect since, if the public key encrypts, it cannot decrypt.
17. *Answer: b).* Answer a) is incorrect since public key cryptography is usually used for encryption and transmission of the secret session key. Answer c) is incorrect since both public and private key encryption are used and answer d) is incorrect since digital certificates can be used and normally, are used.
18. *Answer: c).* The other answers with fixed numbers are incorrect.
19. *Answer: b).* Answer a) is incorrect since a one-time pad uses a random key with length equal to the plaintext message and is used only once. Answer c) is the process of sending a message with no indication that a message even exists. Answer d) is incorrect since it applies to stream ciphers that are XOR'ed with a random key string.
20. *Answer: b).* It uses one alphabet shifted 3 places. Answers a) and c) are incorrect since in a, multiple alphabets are used and in c, the letters of the message are transposed. Answer d) is incorrect since code groups deal with words and phrases and ciphers deal with bits or letters.
21. *Answer: d).* The other answers are incorrect since neither of the algorithms are used.

22. *Answer: c).*
23. *Answer: b).* Answer a) defines confusion; answer c) defines how confusion is accomplished; answer d) is incorrect since it can be accomplished.
24. *Answer: b).* By definition, the others are incorrect.
25. *Answer: c).* There is no such encipherment mode.
26. *Answer: c).* The Meet-in-the-Middle attack has been successfully applied to double DES with the work factor is equivalent to that of single DES. Thus, answer d) is incorrect. Answer a) is false since the work factor of triple DES is greater than that for double DES. In triple DES, three levels of encryption and/or decryption are applied to the message. The work factor of double DES is equivalent to the work factor of single DES. Answer b) is false since the work factor of single DES is less than for triple DES. In triple DES, three levels of encryption and/or decryption are applied to the message in triple DES.
27. *Answer: d).* This answer is a distractor and does not exist.
28. *Answer: b).*
29. *Answer: d).* Answer a) describes the Ultra Project based in Bletchley Park, England, answer b) describes the Japanese Purple Machine, and answer c) refers to Colossus.
30. *Answer: c).* If the one-time-pad is used only once and its corresponding key is truly random and does not have repeating characters, it is unbreakable. Answer a) is incorrect since, if used properly, the one-time-pad should be used only once. Answer b) is incorrect since the key should be random. Answer d) is incorrect since the key has to be of the same length as the message.
31. *Answer: c).*
32. *Answer: a).* The hash function generates a message digest. The message digest is encrypted with the private key of the sender. Thus, if the message can be opened with the sender's public key that is known to all, the message must have come from the sender. The message is not encrypted with the public key since the message is usually longer than the message digest and would take more computing resources to encrypt and decrypt. Since the message digest uniquely characterizes the message, it can be used to verify the identity of the sender. Answers b) and d) will not work since a message encrypted in the public key of the sender can only be read using the private key of the sender. Since the sender is the only one who knows this key, no one else can read the message. Answer c) is incorrect since the message is not encrypted, but the message digest is encrypted
33. *Answer: d).* Answer a) applies to such public key algorithms as Diffie-Hellman and Elliptic Curve. Answer b) is incorrect since it is easy to multiply two large prime numbers. Answer c) refers to symmetric key encryption.
34. *Answer: a).* It is more difficult to compute elliptic curve discrete logarithms than conventional discrete logarithms or factoring. Smaller key sizes in the elliptic curve implementation can yield

higher levels of security. Therefore, answer b) is incorrect. Answers c) and d) are incorrect since elliptic curve cryptosystems can be used for digital signatures and encryption.

35. *Answer:* d). The other answers are key management issues, but key exchange is a function of the encryption system.

Chapter 5—Security Architecture and Models

1. What does the Bell-LaPadula model NOT allow? ?
- A. Subjects to read from a higher level of security relative to their level of security
 - B. Subjects to read from a lower level of security relative to their level of security
 - C. Subjects to write to a higher level of security relative to their level of security
 - D. Subjects to read at their same level of security
2. In the * (star) property of the Bell-LaPadula model, ?
- A. Subjects cannot read from a higher level of security relative to their level of security
 - B. Subjects cannot read from a lower level of security relative to their level of security
 - C. Subjects cannot write to a lower level of security relative to their level of security
 - D. Subjects cannot read from their same level of security
3. The Clark-Wilson model focuses on data's ?
- A. Integrity
 - B. Confidentiality
 - C. Availability
 - D. Format
4. The * (star) property of the Biba model states: ?
- A. Subjects cannot write to a lower level of integrity relative to their level of integrity
 - B. Subjects cannot write to a higher level of integrity relative to their level of integrity
 - C. Subjects cannot read from a

- lower level of integrity relative to their level of integrity
- D. Subjects cannot read from a higher level of integrity relative to their level of integrity
5. Which of the following does the Clark-Wilson model NOT involve? ?
- A. Constrained data items
- B. Transformational procedures
- C. Confidentiality items
- D. Well-formed transactions
6. The Take-Grant model ?
- A. Focuses on confidentiality
- B. Specifies the rights a subject can transfer to an object
- C. Specifies the levels of integrity
- D. Specifies the levels of availability
7. The Biba model addresses ?
- A. Data disclosure
- B. Transformation procedures
- C. Constrained data items
- D. Unauthorized modification of data
8. Mandatory access controls first appear in the Trusted Computer System Evaluation Criteria (TCSEC) at the rating of ?
- A. D
- B. C
- C. B
- D. A
9. In the access control matrix, the rows are ?
- A. Access Control Lists (ACLs)
- B. Tuples
- C. Domains
- D. Capability lists
10. Superscalar computer architecture is characterized by a ?
- A. Computer using instructions that perform many operations per instruction
- B. Computer using instructions that are simpler and require less clock cycles to execute

- C. Processor that executes one instruction at a time
- D. Processor that enables concurrent execution of multiple instructions in the same pipeline stage
11. A Trusted Computing Base (TCB) is defined as ?
- A. The total combination of protection mechanisms within a computer system that are trusted to enforce a security policy
- B. The boundary separating the trusted mechanisms from the remainder of the system
- C. A trusted path that permits a user to access resources
- D. A system that employs the necessary hardware and software assurance measures to enable processing multiple levels of classified or sensitive information to occur
12. Memory space insulated from other running processes in a multiprocessing system is part of a ?
- A. Protection domain
- B. Security perimeter
- C. Least upper bound
- D. Constrained data item
13. The boundary separating the TCB from the remainder of the system is called the ?
- A. Star property
- B. Simple security property
- C. Discretionary control boundary
- D. Security Perimeter
14. The system component that enforces access controls on an object is the ?
- A. Security perimeter
- B. Trusted domain
- C. Reference monitor
- D. Access control matrix
15. In the discretionary portion of the Bell-LaPadula mode that is based on the access matrix, how the access rights are defined and evaluated is called ?

- A. Authentication
 - B. Authorization
 - C. Identification
 - D. Validation
16. A computer system that employs the necessary hardware and software assurance measures to enable it to process multiple levels of classified or sensitive information is called a ?
- A. Closed system
 - B. Open system
 - C. Trusted system
 - D. Safe system
17. For fault-tolerance to operate, a system must be ?
- A. Capable of detecting and correcting the fault
 - B. Capable of only detecting the fault
 - C. Capable of terminating operations in a safe mode
 - D. Capable of a cold start
18. Which of the following composes the four phases of the National Information Assurance Certification and Accreditation Process (NIACAP)? ?
- A. Definition, Verification, Validation, and Confirmation
 - B. Definition, Verification, Validation, and Post Accreditation
 - C. Verification, Validation, Authentication, and Post Accreditation
 - D. Definition, Authentication, Verification, and Post Accreditation
19. What is a programmable logic device (PLD)? ?
- A. A volatile device
 - B. Random Access Memory (RAM) that contains the software to perform specific tasks
 - C. An integrated circuit with connections or internal logic gates that can be changed

- through a programming process
- D. A program resident on disk memory that executes a specific function
20. The termination of selected, non-critical processing when a hardware or software failure occurs and is detected is referred to as ?
- A. Fail safe
 - B. Fault tolerant
 - C. Fail soft
 - D. An Exception
21. Which of the following are the three types of NIACAP accreditation? ?
- A. Site, type, and location
 - B. Site, type, and system
 - C. Type, system, and location
 - D. Site, type, and general
22. Content-dependent control makes access decisions based on ?
- A. The object's data
 - B. The object's environment
 - C. The object's owner
 - D. The object's view
23. The term failover refers to ?
- A. Switching to a duplicate "hot" backup component
 - B. Terminating processing in a controlled fashion
 - C. Resiliency
 - D. A fail soft system
24. Primary storage is the ?
- A. Memory directly addressable by the CPU, which is for storage of instructions and data that are associated with the program being executed
 - B. Memory such as magnetic disks that provide non-volatile storage
 - C. Memory used in conjunction with real memory to present a CPU with a larger, apparent address space
 - D. Memory where information

must be obtained by sequentially searching from the beginning of the memory space

25. In the Common Criteria, a Protection Profile ?
- A. Specifies the mandatory protection in the product to be evaluated
 - B. Is also known as the Target of Evaluation (TOE)
 - C. Is also known as the Orange Book
 - D. Specifies the security requirements and protections of the products to be evaluated
26. Context-dependent control uses which of the following to make decisions? ?
- A. Subject or object attributes, or environmental characteristics
 - B. Data
 - C. Formal models
 - D. Operating system characteristics
27. What is a computer bus? ?
- A. A message sent around a token ring network
 - B. Secondary storage
 - C. A group of conductors for the addressing of data and control
 - D. A message in object-oriented programming
28. In a ring protection system, where is the security kernel usually located ? ?
- A. Highest ring number
 - B. Arbitrarily placed
 - C. Lowest ring number
 - D. Middle ring number
29. Increasing performance in a computer by overlapping the steps of different instructions is called? ?
- A. A reduced instruction set computer
 - B. A complex instruction set computer
 - C. Vector processing
 - D. Pipelining

30. Random access memory is ?
 A. Non-volatile
 B. Sequentially addressable
 C. Programmed by using fusible links
 D. Volatile
31. The addressing mode in which an instruction accesses a memory location whose contents are the address of the desired data is called ?
 A. Implied addressing
 B. Indexed addressing
 C. Direct addressing
 D. Indirect addressing
32. Processes are placed in a ring structure according to ?
 A. Least privilege
 B. Separation of duty
 C. Owner classification
 D. First in, first out
33. The MULTICS operating system is a classic example of ?
 A. An open system
 B. Object orientation
 C. Data base security
 D. Ring protection system
34. What are the hardware, firmware, and software elements of a Trusted Computing Base (TCB) that implement the reference monitor concept called? ?
 A. The trusted path
 B. A security kernel
 C. An Operating System (OS)
 D. A trusted computing system

Answers

1. *Answer:* a). The other options are not prohibited by the model.
2. *Answer:* c). By definition of the star property.
3. *Answer:* a). The Clark-Wilson model is an integrity model.
4. *Answer:* b).
5. *Answer:* c. Answers a, b, and d are parts of the Clark-Wilson model
6. *Answer:* b).
7. *Answer:* d). The Biba model is an integrity model. Answer a) is associated with confidentiality. Answers b) and c) are specific to the Clark-Wilson model.

8. *Answer: c).*
9. *Answer: d).* Answer a) is incorrect because the access control list is not a row in the access control matrix. Answer b) is incorrect since a tuple is a row in the table of a relational database. Answer c) is incorrect since a domain is the set of allowable values a column or attribute can take in a relational database.
10. *Answer: d).* Answer a) is the definition of a complex instruction set computer. Answer b) is the definition of a reduced instruction set computer. Answer c) is the definition of a scalar processor.
11. *Answer: a).* Answer b) is the security perimeter. Answer c) is the definition of a trusted path. Answer d) is the definition of a trusted computer system.
12. *Answer: a).*
13. *Answer: d).* Answers a) and b) deal with security models and answer c) is a distractor.
14. *Answer: c).*
15. *Answer: b).* Since authorization is concerned with how access rights are defined and how they are evaluated.
16. *Answer: c).* By definition of a trusted system. Answers a) and b) refer to open, standard information on a product as opposed to a closed or proprietary product. Answer d) is a distractor.
17. *Answer: a).* The two conditions required for a fault-tolerant system. Answer b) is a distractor. Answer c) is the definition of fail safe and answer d) refers to starting after a system shutdown.
18. *Answer: b).*
19. *Answer: c).* Answer a) is incorrect since a PLD is non-volatile. Answer b) is incorrect since random access memory is volatile memory that is not a non-volatile logic device. Answer c) is a distractor.
20. *Answer: c).*
21. *Answer: b).*
22. *Answer: a).* Answer b) is context-dependent control. Answers c) and d) are distractors.
23. *Answer: a).* Failover means switching to a hot backup system that maintains duplicate states with the primary system. Answer b) refers to fail safe and answers c) and d) refer to fail soft.
24. *Answer: a).* Answer b) refers to secondary storage. Answer c) refers to virtual memory answer d) refers to sequential memory.
25. *Answer: d).* Answer a) is a distractor. Answer b) is the product to be evaluated. Answer c) refers to TCSEC.
26. *Answer: a).* Answer b) refers to content-dependent and answers c) and d) are distractors.
27. *Answer: c).* Answer a) is a token. Answer b) refers to disk storage. Answer d) is a distractor.
28. *Answer: c).*
29. *Answer: d).*

30. *Answer: d).* RAM is volatile. The other answers are incorrect since RAM is volatile, random accessible and not programmed by fusible links.
31. *Answer: d).*
32. *Answer: a).* A process is placed in the ring that gives it the minimum privileges necessary to perform its functions.
33. *Answer: d).* Multics is based on the ring protection architecture.
34. *Answer: b).*

Chapter 6—Operations Security

1. What does IPL stand for? ?
- A. Initial Program Life cycle
 - B. Initial Program Load
 - C. Initial Post-transaction Logging
 - D. Internet Police League
2. Which of the following is NOT a use of an audit trail? ?
- A. Provides information about additions, deletions, or modifications to the data
 - B. Collects information such as passwords or infrastructure configurations
 - C. Assists the monitoring function by helping to recognize patterns of abnormal user behavior
 - D. Allows the security practitioner to trace a transaction's history
3. Why is security an issue when a system is booted into "Single-user mode"? ?
- A. The operating system is started without the security front-end loaded.
 - B. The users cannot login to the system and they will complain.
 - C. Proper forensics cannot be executed while in the single-user mode.
 - D. Backup tapes cannot be restored while in the single-user mode.
4. Which of the following examples is the best definition of Fail Secure? ?
- A. Access personnel have security clearance, but they do not have a "need-to-know."

- B. The operating system is started without the security front-end loaded.
- C. The system fails to preserve a secure state during and after a system crash.
- D. The system preserves a secure state during and after a system crash.
5. Which of the following would NOT be an example of compensating controls being implemented? ?
- A. Sensitive information requiring two authorized signatures to release
- B. A safety deposit box needing two keys to open
- C. Modifying the timing of a system resource in some measurable way to covertly transmit information
- D. Signing in or out of a traffic log and using a magnetic card to access to an operations center
6. "Separation of duties" embodies what principle? ?
- A. An operator does not know more about the system than the minimum required to do the job.
- B. Two operators are required to work in tandem to perform a task.
- C. The operators' duties are frequently rotated.
- D. The operators have different duties to prevent one person from compromising the system.
7. Which is NOT true about Covert Channel Analysis? ?
- A. It is an operational assurance requirement that is specified in the Orange book.
- B. It is required for B2 class systems in order to protect against covert storage channels.

- C. It is required for B2 class systems to protect against covert timing channels.
- D. It is required for B3 class systems to protect against both covert storage and covert timing channels.
8. An audit trail is an example of what type of control? ?
- A. Deterrent control
 - B. Preventative control
 - C. Detective control
 - D. Application control
9. Using pre-numbered forms to initiate a transaction is an example of what type of control? ?
- A. Deterrent control
 - B. Preventative control
 - C. Detective control
 - D. Application control
10. Which of the following is a reason to institute output controls? ?
- A. To preserve the integrity of the data in the system while changes are being made to the configuration
 - B. To protect the output's confidentiality
 - C. To detect irregularities in the software's operation
 - D. To recover damage after an identified system failure
11. Convert Channel Analysis, Trusted Facility Management, and Trusted Recovery are parts of which book in the TCSEC Rainbow series? ?
- A. Red Book
 - B. Orange Book
 - C. Green Book
 - D. Dark Green Book
12. How do covert timing channels convey information? ?
- A. By changing a system's stored data characteristics
 - B. By generating noise and traffic with the data

- C. By performing a covert channel analysis
- D. By modifying the timing of a system resource in some measurable way
13. Which of the following is the best example of “need-to-know”? ?
- A. An operator does not know more about the system than the minimum required to do the job.
- B. Two operators are required to work together to perform a task.
- C. The operators’ duties are frequently rotated.
- D. An operator cannot generate and verify transactions alone.
14. Which of the following is an example of “least privilege”? ?
- A. An operator does not know more about the system than the minimum required to do the job.
- B. An operator does not have more system rights than the minimum required to do the job.
- C. The operators’ duties are frequently rotated.
- D. An operator cannot generate and verify transactions alone.
15. Which of the following would be the BEST description of clipping levels? ?
- A. A baseline of user errors above which violations will be recorded
- B. A listing of every error made by users to initiate violation processing
- C. Variance detection of too many people with unrestricted access
- D. Changes a system’s stored data characteristics
16. Which of the following is NOT a proper media control? ?
- A. The data media should be

logged to provide a physical inventory control.

- B. All data storage media should be accurately marked.
- C. A proper storage environment should be provided for the media.
- D. The media that is re-used in a sensitive environment does not need sanitization.

17. Configuration management control best refers to

?

- A. The concept of “least control” in operations
- B. Ensuring that changes to the system do not unintentionally diminish security
- C. The use of privileged-entity controls for system administrator functions
- D. Implementing resource protection schemes for hardware control

18. Which of the following would NOT be considered a penetration testing technique?

?

- A. War dialing
- B. Sniffing
- C. Data manipulation
- D. Scanning

19. Inappropriate computer activities could be described as

?

- A. Computer behavior that may be grounds for a job action or dismissal
- B. Loss incurred unintentionally though the lack of operator training
- C. Theft of information or trade secrets for profit or unauthorized disclosure
- D. Data scavenging through the resources available to normal system users

20. Why are maintenance accounts a threat to operations controls?

?

- A. Maintenance personnel could slip and fall and sue the

organization.

- B. Maintenance accounts are commonly used by hackers to access network devices.
- C. Maintenance account information could be compromised if printed reports are left out in the open.
- D. Maintenance may require physical access to the system by vendors or service providers.

Answers

1. *Answer:* b). The IPL is a task performed by the operator to boot up the system. The other terms do not exist.
2. *Answer:* b). Auditing should not be used to collect user's passwords. It is used for the other three examples, however.
3. *Answer:* a). When the operator boots the system in "single-user mode," the user front-end security controls are not loaded. This mode should be used for recovery and maintenance procedures only, and all operations should be logged and audited.
4. *Answer:* d). Based on the Common Criteria, a system can be evaluated as Fail Secure if it "preserves a secure state during and after identified failures occur."
5. *Answer:* c). This is the definition for a covert timing channel. The other three are examples of compensating controls, which are a combination of technical, administrative or physical controls to enhance security.
6. *Answer:* d). "Separation of duties" means that the operators are prevented from generating and verifying transactions alone, for example. A task might be divided into different smaller tasks to accomplish this, or in the case of an operator with multiple duties, the operator makes a logical, functional job change when performing such conflicting duties. Answer a) is "need-to-know," answer b) is "dual-control", and c) is "job rotation."
7. *Answer:* c). Covert channel analysis is required to be performed for B2 level class systems to protect against covert storage channels by the Orange book. B3 systems need to be protected against both covert storage channels and covert timing channels.
8. *Answer:* c). An audit trail is a record of events to piece together what has happened and allow enforcement of individual accountability by creating a reconstruction of events. They can be used to assist in the proper implementation of the other controls, however.
9. *Answer:* b). Pre-numbered forms are an example of the general category of preventative controls. They can also be considered a type of transaction controls, and input control.

10. *Answer:* b). In addition to being used as a transaction control verification mechanism, output controls are used to ensure output, such as printed reports, are distributed securely. a), is an example of Configuration or Change control, c) is an example of Application controls, and d) is an example of Recovery controls.
11. *Answer:* b). a), the Red Book is the Trusted Network Interpretation (TNI) summary of network requirements (described in the Telecommunications and Network Security domain), c) the Green Book is the Department of Defense (DoD) *Password Management Guideline*, and d), the Dark Green Book is *The Guide to Understanding Data Remanence in Automated Information Systems*.
12. *Answer:* d) A covert timing channel alters the timing of parts of the system to enable it to be used to communicate information covertly (outside of the normal security function). Answer a), is the description of the use of a covert storage channel, b) is a technique to combat the use of covert channels, and c), is the Orange Book requirement for B3, B2, and A1 evaluated systems.
13. *Answer:* a). "Need-to-know" means the operators are working in an environment which limits their knowledge of the system, applications or data to the minimum elements that they require to perform their job. Answer b) is "dual-control," c) is "job rotation," and answer d) is "separation of duties."
14. *Answer:* b). "Least Privilege" embodies the concept that users or operators should be granted the lowest level of system access or system rights that allows them to perform their job. Answer a) is "need-to-know," c) is "job rotation," and d) is "separation of duties."
15. *Answer:* a). This is the best description of a clipping level. It's not b), as the reason for creating a clipping level is to prevent auditors from having to examine every error. The answer c), is a common use for clipping levels, but is not a definition. D) is meaningless.
16. *Answer:* d). Sanitization is the process of removing information from used data media to prevent data remanence. Different media require different types of sanitation. All the others are examples of proper media controls.
17. *Answer:* b). Configuration Management Control (and Change Control) are processes to ensure that any changes to the system are managed properly and do not inordinately affect either the availability or security of the system.
18. *Answer:* c). Data manipulation describes the corruption of data integrity to perform fraud for personal gain or other reasons. External penetration testing should not alter the data in any way. The other three are common penetration techniques.
19. *Answer:* a). While all of the activities described above are considered in the broad category of inappropriate activities, this description is used to define a narrower category of inappropriate activities. Answer b), is commonly defined as accidental loss, answer c), is considered intentionally illegal

computer activity and d), is a “keyboard attack.” A type of data scavenging attack using common tools or utilities available to the user.

20. *Answer:* b) Maintenance accounts are login accounts to systems resources, primarily networked devices. They often have the factory-set passwords which are frequently distributed through the hacker community.

Chapter 7—Applications and Systems Development

1. What is a data warehouse? ?
- A. A remote facility used for storing backup tapes
 - B. A repository of information from heterogeneous databases
 - C. A table in a relational database system
 - D. A hot backup building
2. What does normalizing data in a data warehouse mean? ?
- A. Redundant data is removed.
 - B. Numerical data is divided by a common factor.
 - C. Data is converted to a symbolic representation.
 - D. Data is restricted to a range of values.
3. What is a neural network? ?
- A. A hardware or software system that emulates the reasoning of a human expert
 - B. A collection of computers that are focused on medical applications
 - C. A series of networked PCs performing artificial intelligence tasks
 - D. A hardware or software system that emulates the functioning of biological neurons
4. A neural network learns by using various algorithms to ?
- A. Adjust the weights applied to the data
 - B. Fire the rules in knowledge base

- C. Emulate an inference engine
D. Emulate the thinking of an expert
5. The SEI Software Capability Maturity Model is based on the premise that ?
- A. Good software development is a function of the number of expert programmers in the organization.
B. The maturity of an organization's software processes cannot be measured.
C. The quality of a software product is a direct function of the quality of its associated software development and maintenance processes.
D. Software development is an art that cannot be measured by conventional means.
6. In configuration management, a configuration item is ?
- A. The version of the operating system, which is operating on the work station, that provides information security services
B. A component whose state is to be recorded and against which changes are to be progressed
C. The network architecture used by the organization
D. A series of files that contain sensitive information
7. In an object-oriented system, polymorphism denotes ?
- A. Objects of many different classes that are related by some common superclass; thus, any object denoted by this name is able to respond to some common set of operations in a different way
B. Objects of many different classes that are related by some common superclass; thus, all objects denoted by this name are able to respond to some common set of

operations in identical fashion

- C. Objects of the same class; thus, any object denoted by this name is able to respond to some common set of operations in the same way
- D. Objects of many different classes that are unrelated, but respond to some common set of operations in the same way

8. The simplistic model of software life cycle development assumes that

?

- A. Iteration will be required among the steps in the process.
- B. Each step can be completed and finalized without any effect from the later stages that may require rework.
- C. Each phase is identical to a completed milestone.
- D. Software development requires reworking and repeating some of the phases.

9. What is a method in an object-oriented system?

?

- A. The means of communication among objects
- B. A guide to programming of objects
- C. The code defining the actions that the object performs in response to a message
- D. The situation where a class inherits the behavioral characteristics of more than one parent class

10. What does the Spiral Model depict?

?

- A. A spiral that incorporates various phases of software development
- B. A spiral that models the behavior of biological neurons
- C. The operation of expert systems
- D. Information security checklists

11. In the software life cycle, verification

?

- A. Evaluates the product in

development against real world requirements

- B. Evaluates the product in development against similar products
- C. Evaluates the product in development against general baselines
- D. Evaluates the product in development against the specification

12.

In the software life cycle, validation

?

- A. Refers to the work product satisfying the real-world requirements and concepts
- B. Refers to the work product satisfying derived specifications
- C. Refers to the work product satisfying software maturity levels
- D. Refers to the work product satisfying generally accepted principles

13.

In the modified Waterfall Model

?

- A. Unlimited backward iteration is permitted.
- B. The model was reinterpreted to have phases end at project milestones.
- C. The model was reinterpreted to have phases begin at project milestones.
- D. Product verification and validation are not included.

14.

Cyclic redundancy checks, structured walk-throughs, and hash totals are examples of what type of application controls?

?

- A. Preventive security controls
- B. Preventive consistency controls
- C. Detective accuracy controls
- D. Corrective consistency controls

15.

In a system life cycle, information security controls should be

?

- A. Designed during the product

- implementation phase
- B. Implemented prior to validation
 - C. Part of the feasibility phase
 - D. Specified after the coding phase
16. The software maintenance phase controls consist of ?
- A. Request control, change control, and release control
 - B. Request control, configuration control, and change control
 - C. Change control, security control, and access control
 - D. Request control, release control, and access control
17. In configuration management, what is a software library? ?
- A. A set of versions of the component configuration items
 - B. A controlled area accessible only to approved users who are restricted to the use of an approved procedure
 - C. A repository of backup tapes
 - D. A collection of software build lists
18. What is configuration control? ?
- A. Identifying and documenting the functional and physical characteristics of each configuration item
 - B. Controlling changes to the configuration items and issuing versions of configuration items from the software library
 - C. Recording the processing of changes
 - D. Controlling the quality of the configuration management procedures
19. What is searching for data correlations in the data warehouse called? ?
- A. Data warehousing
 - B. Data mining
 - C. A data dictionary
 - D. Configuration management

20. The security term that is concerned with the same primary key existing at different classification levels in the same database is ?
- A. Polymorphism
 - B. Normalization
 - C. Inheritance
 - D. Polyinstantiation
21. What is a data dictionary? ?
- A. A database for system developers
 - B. A database of security terms
 - C. A library of objects
 - D. A validation reference source
22. Which of the following is an example of mobile code? ?
- A. Embedded code in control systems
 - B. Embedded code in PCs
 - C. Java and ActiveX code downloaded into a web browser from the World Wide Web (WWW)
 - D. Code derived following the spiral model
23. Which of the following is NOT true regarding software unit testing? ?
- A. The test data is part of the specifications.
 - B. Correct test output results should be developed and known beforehand.
 - C. Live or actual field data is recommended for use in the testing procedures.
 - D. Testing should check for out-of-range values and other bounds conditions.

Answers

1. *Answer:* b). A repository of information from heterogeneous databases. Answers a and d describe physical facilities for backup and recovery of information systems and answer c describes a relation in a relational database.
2. *Answer:* a). Removing redundant data.
3. *Answer:* d). A neural network is a hardware or software system that emulates the functioning of biological neurons. Answer a) refers to an expert system and answers b) and c) are

distractors.

4. *Answer:* a). A neural network learns by using various algorithms to adjust the weights applied to the data. Answers b), c) and d) are terminology referenced in expert systems.
5. *Answer:* c). The quality of a software product is a direct function of the quality of its associated software development and maintenance processes. Answer a) is false since the SEI Software CMM relates the production of good software to having the proper processes in place in an organization and not to expert programs or heroes. Answer b) is false since the Software CMM provides means to measure the maturity of an organization's software processes. Answer d) is false for the same reason as answer b).
6. *Answer:* b). A component whose state is to be recorded and against which changes are to be progressed. Answers a), c), and d) are incorrect by the definition of a configuration item.
7. *Answer:* a). Objects of many different classes that are related by some common superclass that are able to respond to some common set of operations in a different way. Answers b), c), and d) are incorrect by the definition of polymorphism.
8. *Answer:* b). Each step can be completed and finalized without any affect from the later stages that might require rework. Answer a) is incorrect since no iteration is allowed for in the model. Answer c) is incorrect since it applies to the modified Waterfall model. Answer d) is incorrect since no iteration or reworking is considered in the model.
9. *Answer:* c). A method in an object-oriented system is the code that defines the actions that the object performs in response to a message. Answer a) is incorrect since it defines a message. Answer b) is a distractor and answer d) refers to multiple inheritance.
10. *Answer:* a). A spiral that incorporates various phases of software development. The other answers are distractors.
11. *Answer:* d). In the software life cycle, verification evaluates the product in development against the specification. Answer a) defines validation. Answers b) and c) are distractors.
12. *Answer:* a) In the software life cycle, validation is the work product satisfying the real-world requirements and concepts. The other answers are distractors.
13. *Answer:* b). The modified Waterfall model was reinterpreted to have phases end at project milestones. Answer a) is false since unlimited backward iteration is not permitted in the modified Waterfall model. Answer c) is a distractor and answer d) is false since verification and validation are included.
14. *Answer:* c). Cyclic redundancy checks, structured walk-throughs and hash totals are examples of detective accuracy controls. The other answers do not apply by the definition of the types of controls.
15. *Answer:* c). In the system life cycle, information security controls should be part of the feasibility phase. The other answers are incorrect since the basic premise of information system security is that controls should be included in the

- earliest phases of the software life cycle and not added later in the cycle or as an afterthought.
- 16.** *Answer:* a). The software maintenance phase controls consist of request control, change control and release control by definition. The other answers are, therefore, incorrect.
- 17.** *Answer:* b). In configuration management, a software library is a controlled area accessible only to approved users who are restricted to the use of approved procedure. Answer a) is incorrect since it defines a build list. Answer c) is incorrect since it defines a backup storage facility. Answer d) is a distractor.
- 18.** *Answer:* b). Configuration control is controlling changes to the configuration items and issuing versions of configuration items from the software library. Answer a is the definition of configuration identification. Answer c is the definition of configuration status accounting and answer d is the definition of configuration audit.
- 19.** *Answer:* b). Searching for data correlations in the data warehouse is called data mining. Answer a) is incorrect since data warehousing is creating a repository of information from heterogeneous databases that is available to users for making queries. Answer c) is incorrect since a data dictionary is a database for system developers. Answer d) is incorrect since configuration management is the discipline of identifying the components of a continually evolving system for the purposes of controlling changes to those components and maintaining integrity and traceability throughout the life cycle.
- 20.** *Answer:* d). The security term that is concerned with the same primary key existing at different classification levels in the same database is polyinstantiation. Answer a) is incorrect since polymorphism is defined as objects of many different classes that are related by some common superclass; thus, any object denoted by this name is able to respond to some common set of operations in a different way. Answer b) is incorrect since normalization refers to removing redundant or incorrect data from a database. Answer c is incorrect since inheritance refers to methods from a class inherited by another subclass.
- 21.** *Answer:* a). A data dictionary is a database for system developers. Answers b), c), and d) are distractors.
- 22.** *Answer:* c). An example of mobile code is Java and ActiveX code downloaded into a web browser from the World Wide Web. Answers a), b), and d) are incorrect since they are types of code that are not related to mobile code.
- 23.** *Answer:* c), live or actual field data are NOT recommended for use in testing since they do not thoroughly test all normal and abnormal situations and the test results are not known beforehand. Answers a), b), and d), are true of testing.

Chapter 8—Business Continuity Planning/Disaster Recovery Planning

1. Which of the following is NOT one of the five disaster recovery plan testing types? ?
 - A. Simulation
 - B. Checklist
 - C. Mobile
 - D. Full Interruption
2. Why is it so important to test disaster recovery plans frequently? ?
 - A. The businesses that provide subscription services may have changed ownership.
 - B. A plan is not considered viable until a test has been performed.
 - C. Employees may get bored with the planning process.
 - D. Natural disasters can change frequently.
3. What is the purpose of the Business Impact Assessment (BIA)? ?
 - A. To create a document to be used to help understand what impact a disruptive event would have on the business.
 - B. To define a strategy to minimize the effect of disturbances and to allow for resumption of business processes.
 - C. To emphasize the organization's commitment to its employees and vendors.
 - D. To work with executive management to establish a DRP policy.
4. Which of the following is NOT considered an element of a backup alternative? ?
 - A. Electronic vaulting
 - B. Remote journaling
 - C. Warm site
 - D. Checklist
5. Which type of backup subscription service will allow a business to recover quickest? ?
 - A. A hot site
 - B. A mobile or rolling backup

service

C. A cold site

D. A warm site

6. Which of the following would best describe a “cold” backup site? ?

A. A computer facility with electrical power and HVAC, all needed applications installed and configured on the file/print servers, and enough workstations present to begin processing

B. A computer facility with electrical power and HVAC but with no workstations or servers on-site prior to the event and no applications installed

C. A computer facility with no electrical power or HVAC

D. A computer facility available with electrical power and HVAC and some file/ print servers, although the applications are not installed or configured and all of the needed workstations may not be on site or ready to begin processing

7. Which of the following is NOT considered a natural disaster? ?

A. Earthquake

B. Sabotage

C. Tsunami

D. Flood

8. What could be a major disadvantage to a “mutual aid” or “reciprocal” type of backup service agreement? ?

A. It’s free or at low cost to the organization.

B. The use of prefabricated buildings makes recovery easier.

C. In a major emergency, the site may not have the capacity to handle the operations required.

D. Annual testing by the Info Tech department is required to

- maintain the site.
9. What is considered the major disadvantage to employing a “hot” site for disaster recovery? ?
- A. Exclusivity is assured for processing at the site.
 - B. Maintaining the site is expensive.
 - C. The site is immediately available for recovery.
 - D. Annual testing is required to maintain the site.
10. When is the disaster considered to be officially over? ?
- A. When the danger has passed and the disaster has been contained.
 - B. When the organization has processing up and running at the alternate site.
 - C. When all of the elements of the business have returned to normal functioning at the primary site.
 - D. When all employees have been financially reimbursed for their expenses.
11. What is the number one priority of disaster response? ?
- A. Transaction processing
 - B. Personnel safety
 - C. Protecting the hardware
 - D. Protecting the software
12. Put the five disaster recovery testing types in their proper order, from the least extensive to the most. ?
- A. Full-interruption
 - B. Checklist
 - C. Structured walk-through
 - D. Parallel
 - E. Simulation
13. What is the difference between a “parallel” disaster recovery plan test and a “full interruption” disaster recovery plan test? ?
- A. There is no difference; both terms mean the same thing.
 - B. While a full-interruption test

tests the processing functionality of the alternate site, the parallel test actually replicates a disaster by halting production.

C. While a parallel test tests the processing functionality of the alternate site, the full-interruption test actually replicates a disaster by halting production.

D. Functional business unit representatives meet to review the plan to ensure it accurately reflects the organization's recovery strategy

14. Which of the following is NOT one of the primary goals of a BIA? ?

A. Resource requirements

B. Personnel safety

C. Criticality prioritization

D. Downtime estimation

Answers

1. *Answer:* c). Mobile. The other three are proper examples of elements of the five disaster recovery plan testing types.
2. *Answer:* b). A plan is not considered functioning and viable until a test has been performed. An untested plan sitting on a shelf is useless and might even have the reverse effect of creating a false sense of security. While the other answers, especially a), are good reasons to test, b) is the primary reason.
3. *Answer:* a). Create a document to be used to help understand what impact a disruptive event would have on the business. b), is the definition of business continuity planning.
4. *Answer:* d). A checklist is a type of disaster recovery plan test. Electronic vaulting is the batch transfer of backup data to an off-site location. Remote journaling is the parallel processing of transactions to an alternate site. A warm site is a backup processing alternative.
5. *Answer:* a). Warm and cold sites require more work after the event occurs to get them to full operating functionality. A "mobile" backup site might be useful for specific types of minor outages, but a hot site is still the main choice of backup processing site.
6. *Answer:* b). A computer facility with electrical power and HVAC, with workstations and servers available to be brought on-site when the event begins and no applications installed, is a cold site. a), is a hot site, and d), is a warm site. c), is just an empty room.

7. *Answer: b).* An easy one, although the more paranoid among us might think the others are Mother Nature's way of sabotage.
8. *Answer: c).* The site might not have the capacity to handle the operations required during a major disruptive event. While mutual aid might be a good system for sharing resources during a small or isolated outage, a major natural or other type of disaster can create serious resource contention between the two organizations.
9. *Answer: b).* The expense of maintaining the site. A hot site is commonly used for those extremely time-critical functions that the business must have up and running to continue operating, but the expense of duplicating and maintaining all of the hardware, software, and application elements is a serious resource drain to most organizations.
10. *Answer: c).* When all of the elements of the business have returned to normal functioning at the primary site. It's important to remember that a threat to continuity exists when processing is being returned to its original site after salvage and cleanup has been done.
11. *Answer: b).* The number one function of all disaster response and recovery is the protection of the safety of people, all other concerns are vital to business continuity, but secondary to personnel safety.
12. *Answer: b), c), e), d), a).*
13. *Answer: c).* A parallel test tests the processing functionality of the alternate site, whereas the full-interruption test actually replicates a disaster by halting production. Answer d) is the definition of a checklist test type.
14. *Answer: b).* Personnel safety is the primary priority of BCP and DRP, not BIA.

Chapter 9—Law, Investigation, and Ethics

1. According to the Internet Activities Board (IAB), an activity that causes which of the following is considered a violation of ethical behavior on the Internet? ?
 - A. Wasting resources
 - B. Appropriating other people's intellectual output
 - C. Using a computer to steal
 - D. Using a computer to bear false witness
2. Which of the following best defines social engineering? ?
 - A. Illegal copying of software
 - B. Gathering information from discarded manuals and printouts
 - C. Using people skills to obtain

proprietary information

- D. Destruction or alteration of data
3. Because the development of new technology usually outpaces the law, law enforcement uses which traditional laws to prosecute computer criminals? ?
- A. Malicious mischief
 - B. Embezzlement, fraud, and wiretapping
 - C. Immigration
 - D. Conspiracy and elimination of competition
4. Which of the following is NOT a category of law under the Common Law System: ?
- A. Criminal law
 - B. Civil law
 - C. Administrative/Regulatory law
 - D. Derived law
5. A trade secret ?
- A. Provides the owner with a legally enforceable right to exclude others from practicing the art covered for a specified time period
 - B. Protects "original" works of authorship
 - C. Secures and maintains the confidentiality of proprietary technical or business-related information that is adequately protected from disclosure by the owner
 - D. Is a word, name, symbol, color, sound, product shape, or device used to identify goods and to distinguish them from those made or sold by others
6. Which of the following is NOT a European Union (EU) principle? ?
- A. Data should be collected in accordance with the law.
 - B. Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is permissible.

- C. Data should be used only for the purposes for which it was collected and should be used only for reasonable period of time.
- D. Information collected about an individual cannot be disclosed to other organizations or individuals unless authorized by law or by consent of the individual

7. The Federal Sentencing Guidelines ?

- A. Hold senior corporate officers personally liable if their organizations do not comply with the law
- B. Prohibit altering, damaging, or destroying information in a federal interest computer
- C. Prohibit eavesdropping or the interception of message contents
- D. Established a category of sensitive information called Sensitive But Unclassified (SBU)

8. What does the prudent man rule require? ?

- A. Senior officials to post performance bonds for their actions
- B. Senior officials to perform their duties with the care that ordinary, prudent people would exercise under similar circumstances
- C. Senior officials to guarantee that all precautions have been taken and that no breaches of security can occur
- D. Senior officials to follow specified government standards

9. Information Warfare is ?

- A. Attacking the information infrastructure of a nation to gain military and/or economic advantages.
- B. Developing weapons systems based on artificial intelligence

- technology
- C. Generating and disseminating propaganda material
- D. Signal intelligence
10. The chain of evidence relates to ?
- A. Securing laptops to desks during an investigation
- B. DNA testing
- C. Handling and controlling evidence
- D. Making a disk image
11. The Kennedy-Kassenbaum Act is also known as ?
- A. RICO
- B. OECD
- C. HIPAA
- D. EU Directive
12. Which of the following refers to a U.S. Government program that reduces or eliminates emanations from electronic equipment? ?
- A. CLIPPER
- B. ECHELON
- C. ECHO
- D. TEMPEST
13. Imprisonment is a possible sentence under ?
- A. Civil (tort) law
- B. Criminal law
- C. Both civil and criminal law
- D. Neither civil or criminal law
14. Which one of the following conditions must be met if legal electronic monitoring of employees is conducted by an organization? ?
- A. Employees must be unaware of the monitoring activity.
- B. All employees must agree with the monitoring policy.
- C. Results of the monitoring cannot be used against the employee.
- D. The organization must have a policy stating that all employees are regularly notified that monitoring is being conducted.

15. Which of the following is a key principle in the evolution of computer crime laws in many countries? ?
- A. All members of the United Nations have agreed to uniformly define and prosecute computer crime.
 - B. Existing laws against embezzlement, fraud, and wiretapping cannot be applied to computer crime.
 - C. The definition of property was extended to include electronic information.
 - D. Unauthorized acquisition of computer-based information without the intent to resell is not a crime.
16. The concept of Due Care states that senior organizational management must ensure that ?
- A. All risks to an information system are eliminated.
 - B. Certain requirements must be fulfilled in carrying out their responsibilities to the organization.
 - C. Other management personnel are delegated the responsibility for information system security.
 - D. The cost of implementing safeguards is greater than the potential resultant losses resulting from information security breaches.
17. Liability of senior organizational officials relative to the protection of the organizations information systems is prosecutable under ?
- A. Criminal law
 - B. Civil law
 - C. International law
 - D. Financial law
18. Responsibility for handling computer crimes in the United States is assigned to ?
- A. The Federal Bureau of Investigation (FBI) and the Secret Service
 - B. The FBI only

- C. The National Security Agency (NSA)
- D. The Central Intelligence Agency (CIA)
19. In general, computer-based evidence is considered ?
- A. Conclusive
- B. Circumstantial
- C. Secondary
- D. Hearsay
20. Investigating and prosecuting computer crimes is made more difficult because ?
- A. Backups may be difficult to find.
- B. Evidence is mostly intangible.
- C. Evidence cannot be preserved.
- D. Evidence is hearsay and can never be introduced into a court of law.
21. Which of the following criteria are used to evaluate suspects in the commission of a crime? ?
- A. Motive, Intent, and Ability
- B. Means, Object, and Motive
- C. Means, Intent, and Motive
- D. Motive, Means, and Opportunity
22. 18 U.S.C. §2001 (1994) refers to ?
- A. Article 18, U.S. Code, Section 2001, 1994 edition
- B. Title 18, University of Southern California, Article 2001, 1994 edition
- C. Title 18, Section 2001 of the U.S. Code, 1994 edition
- D. Title 2001 of the U.S. Code, Section 18, 1994 edition
23. What is enticement? ?
- A. Encouraging the commission of a crime when there was initially no intent to commit a crime
- B. Assisting in the commission of a crime
- C. Luring the perpetrator to an

attractive area or presenting the perpetrator with a lucrative target after the crime has already been initiated

D. Encouraging the commission of one crime over another

24. Which of the following is NOT a computer investigation issue? ?

A. Evidence is easy to obtain.

B. The time frame for investigation is compressed.

C. An expert may be required to assist.

D. The information is intangible.

25. Conducting a search without the delay of obtaining a warrant if destruction of evidence seems imminent is possible under ?

A. Federal Sentencing Guidelines

B. Proximate Causation

C. Exigent Circumstances

D. Prudent Man Rule

Answers

1. *Answer:* a). Answers b), c), and d) are ethical considerations of other organizations.
2. *Answer:* c). Using people skills to obtain proprietary information. Answer a is software piracy; answer b) is dumpster diving; and answer d) is a violation of integrity.
3. *Answer:* b). Answer a is not a law; answer; c) is not applicable because it applies to obtaining visas and so on; and answer d) is not correct because the crimes in answer b) are more commonly used to prosecute computer crimes.
4. *Answer:* d). It is a distractor, and all of the other answers are categories under common law.
5. *Answer:* c). It defines a trade secret. Answer a) refers to a patent. Answer b) refers to a copyright. Answer d) refers to a trademark.
6. *Answer:* b). The transmission of data to locations where "equivalent" personal data protection cannot be assured is NOT permissible. The other answers are EU principles.
7. *Answer:* a). Answer b) is part of the U.S. Computer Fraud and Abuse Act. Answer c) is part of the U.S. Electronic Communications Privacy Act. Answer d) is part of the U.S. Computer Security Act.
8. *Answer:* b). Answer a) is a distractor and is not part of the prudent man rule. Answer c) is incorrect because it is not possible to guarantee that breaches of security can never occur. Answer d) is incorrect since the prudent man rule does not refer to a specific government standard but relates to what

- other prudent persons would do.
9. *Answer:* a). Answer b) is a distractor and has to do with weapon systems development. Answer c) is not applicable. Answer d) is the conventional acquisition of information from radio signals.
10. *Answer:* c). Answer a) relates to physical security; answer b) is a type of biological testing; and answer d) is part of the act of gathering evidence.
11. *Answer:* c). The others refer to other laws or guidelines.
12. *Answer:* d). Answer a) refers to the U.S. government Escrowed Encryption Standard. Answer b) refers to the large-scale monitoring of RF transmissions. Answer c) is a distractor.
13. *Answer:* b). It is the only one of the choices where imprisonment is possible.
14. *Answer:* d). Answer a) is incorrect since employees must be made aware of the monitoring if it is to be legal; answer b) is incorrect since employees do not have to agree with the policy; answer c) is incorrect since the results of monitoring might be used against the employee if the corporate policy is violated.
15. *Answer:* c). Answer a) is incorrect since all nations do not agree on the definition of computer crime and corresponding punishments. Answer b) is incorrect since the existing laws can be applied against computer crime. Answer d) is incorrect since, in some countries, possession without intent to sell is considered a crime.
16. *Answer:* b). Answer a) is incorrect since all risks to information systems cannot be eliminated; answer c) is incorrect since senior management cannot delegate its responsibility for information system security under Due Care; answer d) is incorrect since the cost of implementing safeguards should be less than or equal to the potential resulting losses relative to the exercise of Due Care.
17. *Answer:* b).
18. *Answer:* a). Making the other answers incorrect.
19. *Answer:* d). Answer a) refers to incontrovertible evidence; answer b) refers to inference from other, intermediate facts; answer c) refers to a copy of evidence or oral description of its content.
20. *Answer:* b). Answer a) is incorrect since, if backups are done, they usually can be located. Answer c) is incorrect since evidence can be preserved using the proper procedures. Answer d) is incorrect since there are exceptions to the Hearsay Rule.
21. *Answer:* d).
22. *Answer:* c).
23. *Answer:* c). The definition of enticement. Answer a) is the definition of entrapment. Answers b) and d) are distractors.
24. *Answer:* a). In many instances, evidence is difficult to obtain in computer crime investigations. Answers b), c) and d) are computer investigation issues.
25. *Answer:* c). The other answers refer to other principles,

Chapter 10—Physical Security

1. The recommended optimal relative humidity range for computer operations is ?
 - A. 10%—30%
 - B. 30%—40%
 - C. 40%—60%
 - D. 60%—80%

2. How many times should a diskette be formatted to comply with TCSEC Orange book object reuse recommendations? ?
 - A. Three
 - B. Five
 - C. Seven
 - D. Nine

3. Which of the following more closely describes the combustibles in a Class B-rated fire? ?
 - A. Paper
 - B. Gas
 - C. Liquid
 - D. Electrical

4. Which of the following is NOT the proper suppression medium for a Class B fire? ?
 - A. CO₂
 - B. Soda Acid
 - C. Halon
 - D. Water

5. What does an audit trail or access log usually NOT record? ?
 - A. How often a diskette was formatted
 - B. Who attempted access
 - C. The date and time of the access attempt
 - D. Whether the attempt was successful

6. A brownout can be defined as a ?
 - A. Prolonged power loss
 - B. Momentary low voltage
 - C. Prolonged low voltage
 - D. Momentary high voltage

7. A surge can be defined as a(n) ?
A. Prolonged high voltage
B. Initial surge of power at start
C. Momentary power loss
D. Steady interfering disturbance
8. Which is NOT a type of a fire detector? ?
A. Heat-sensing
B. Gas-discharge
C. Flame-actuated
D. Smoke-actuated
9. Which of the following is NOT considered an acceptable replacement for Halon discharge systems? ?
A. FA200
B. Inergen (IG541)
C. Halon 1301
D. Argon (IG55)
10. Which type of fire extinguishing method contains standing water in the pipe, and therefore generally does not enable a manual shutdown of systems before discharge? ?
A. Dry Pipe
B. Wet pipe
C. Preaction
D. Deluge
11. Which type of control below is NOT an example of a physical security access control? ?
A. Retinal scanner
B. Guard dog
C. Five-key programmable lock
D. Audit trail
12. Which is NOT a recommended way to dispose of unwanted used data media? ?
A. Destroying CD-ROMs
B. Formatting diskettes seven or more times
C. Shredding paper reports by cleared personnel
D. Copying new data over existing data on diskettes
13. Which of the following is an example of a "smart" card? ?
A. A drivers license
B. A bank ATM card

- C. An employee photo ID
D. A library card
14. Which is NOT an element of two-factor authentication? ?
A. Something you are
B. Something you know
C. Something you have
D. Something you ate
15. The theft of a laptop poses a threat to which tenet of the C.I.A. triad? ?
A. Confidentiality
B. Integrity
C. Availability
D. All of the above
16. Which is a benefit of a guard over an automated control? ?
A. Guards can use discriminating judgment.
B. Guards are cheaper.
C. Guards do not need training.
D. Guards do not need pre-employment screening.
17. Which is NOT considered a preventative security measure? ?
A. Fences
B. Guard
C. Audit trails
D. Preset locks
18. Which is NOT a PC security control device? ?
A. A cable lock
B. A switch control
C. A port control
D. A file cabinet lock
19. What is the recommended height of perimeter fencing to keep out casual trespassers? ?
A. 1' to 2' high
B. 3' to 4' high
C. 6' to 7' high
D. 8' to 12' high
20. Why should extensive exterior perimeter lighting of entrances or parking areas be installed? ?
A. To enable programmable locks

- to be used
- B. To create two-factor authentication
 - C. To discourage prowlers or casual intruders
 - D. To prevent data remanence
21. Which of the following is NOT a form of data erasure? ?
- A. Clearing
 - B. Remanence
 - C. Purging
 - D. Destruction
22. Which is NOT considered a physical intrusion detection method? ?
- A. Audio motion detector
 - B. Photoelectric sensor
 - C. Wave pattern motion detector
 - D. Line Supervision

Answers

1. *Answer:* c). 40% to 60% relative humidity is recommended for safe computer operations. Too low humidity can create static discharge problems, too high humidity can create condensation and electrical contact problems.
2. *Answer:* c). Most computer certification and accreditation standards recommend that diskettes be formatted seven times to prevent any possibility of data remanence.
3. *Answer:* c). Paper is described as a common combustible and is therefore rated a class A fire. An electrical fire is rated Class C. Gas is not defined as a combustible.
4. *Answer:* d). Water is not a proper suppression medium for a class B fire. The other three are commonly used.
5. *Answer:* a). How often a diskette was formatted. The other three answers are common elements of an access log or audit trail.
6. *Answer:* c). Answer a) prolonged power loss is a blackout; answer b) momentary low voltage is a sag; and d), momentary high voltage is a spike.
7. *Answer:* a). Answer b), initial surge of power at start or power on is called an inrush; c) momentary power loss is a fault; and d) a steady interfering disturbance is called noise.
8. *Answer:* b). Gas-discharge is a type of fire extinguishing system, not a fire detection system.
9. *Answer:* c). Existing installations are encouraged to replace Halon 1301 with one of the substitutes listed.
10. *Answer:* b). The other three are variations on a dry pipe discharge method, with the water not standing in the pipe until a fire is detected. The deluge method is not recommended for

computer equipment, however, due to the volume of water discharged.

11. *Answer: d).*
12. *Answer: d).* Copying new data over existing data on diskettes. While this method might overwrite the older files, if the new data file is smaller than the older data file, recoverable data might exist past the file end marker of the new file.
13. *Answer: b).* The other three cards are “dumb” cards, because it is assumed that they contain no electronics, magnetic stripes or integrated circuits.
14. *Answer: d).* An easy one.
15. *Answer: d).* Confidentiality, as the data can now be read by someone outside of a monitored environment, Availability, as the user has lost the computing ability provided by the unit, and Integrity, as the data residing on and any telecommunications from the portable are now suspect.
16. *Answer: a).* Guards can use discriminating judgment. Guards are typically more expensive than automated controls, need training as to the protection requirements of the specific site, and need to be screened and bonded.
17. *Answer: c).* Audit trails are detective, rather than preventative, as they are used to piece together the information of an intrusion or intrusion attempt after the fact.
18. *Answer: d).* A cable lock is used to attach the PC to a desk, a switch control is used to prevent powering off a unit, and a port control (such as a diskette drive lock) is used to prevent data from being downloaded from the PC.
19. *Answer: b).* 3’ to 4’ high fencing is considered minimal protection, only for restricting casual trespassers. c) and d) are better protection against intentional intruders.
20. *Answer: c).* The other answers have nothing to do with lighting.
21. *Answer: b).* Clearing refers to the overwriting of data media intended to be reused in same organization. Purging refers to degaussing or overwriting media intended to be removed from the organization. Destruction refers to completely destroying the media.
22. *Answer: d).* Line supervision is the monitoring of the alarm signaling transmission medium to detect tampering. Audio detectors monitor a room for any abnormal sound wave generation. Photoelectric sensors receive a beam of light from a light-emitting device. Wave pattern motion detectors generate a wave pattern and send an alarm if the pattern is disturbed.

Appendix D: A Process Approach to HIPAA Compliance Through a HIPAA-CMM

Summary

Addressing the *Health Insurance Portability and Accountability Act* (HIPAA) health information standards in an effective manner requires a sound, structured approach. The method of compliance with the HIPAA privacy regulations and pending Security and Electronic Signature standards should provide proper and complete coverage of the requirements of the law and should support metrics for evaluating the effectiveness of the implementation.

The major issue relative to meeting HIPAA information security requirements at this time is that there is no standard process in place to determine HIPAA compliance. This situation becomes more complicated when institutions are evaluated according to different criteria and methodologies. What is needed is a standard methodology and evaluation model that is based on proven, valid techniques that are recognized by the information security community. This paper proposes a *HIPAA-Capability Maturity Model* (HIPAA-CMM) based on such techniques. The model is based on the proven and recognized CMM framework developed initially for measuring the quality and maturity level of an organization's software development process and has been extended to systems engineering and systems security engineering.

While the Security and Electronic Signature standards regulation portions of the HIPAA implementation are still in draft form and are subject to amendment, the privacy regulation already provides that "a covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information." A review of the current draft regulation regarding security standards reveals that it codifies information system security practices that are generally accepted as best in commercial government arenas. In order to comply with the act and with the privacy regulation's requirement for "appropriate administrative, technical and physical safeguards," covered entities will have to demonstrate due diligence in implementing generally accepted best information system security practices.

The HIPAA-CMM is proposed as the standard framework for evaluating and assuring HIPAA compliance. The *process areas* (PAs) selected for the HIPAA-CMM are based on the generally accepted best practices of systems security engineering. (A PA is a defined set of related security engineering process characteristics that, when performed collectively, can achieve a defined purpose.) Thus, the use of the HIPAA-CMM will not only measure compliance with current HIPAA requirements, but with the standards that are likely to be included in the final privacy, will also measure Security and Electronic Signature standards regulation when it is issued.

The HIPAA-CMM is based on the Systems Security Engineering Capability Maturity Model[®] (SSE-CMM[®]), [SSE99]. The PAs of the SSE-CMM incorporate the technical, organizational, and best project practices of systems security engineering. As such, they provide a process-based common thread that encompasses most security-related evaluation criteria and security guidance documents. Corbett's HIPAA-CMM incorporates a specific subset of the 22 SSE-CMM PAs to address the privacy and information security portions of HIPAA. To provide the complete coverage and granularity required by the HIPAA regulations that are not addressed by the SSE-CMM, additional PAs have been developed. These PAs are HIPAA-Specific PAs (HPAs) and serve to customize the model for the HIPAA application. Because the HIPAA regulations have not been finalized as yet, the corresponding requirements have been developed based on the extant HIPAA documentation and generally accepted best security practices. The HIPAA-CMM is designed as the basis for providing the full

evaluation coverage that is necessary to address all the HIPAA information security compliance requirements.

The catalyst for the HIPAA-CMM was an initial investigation of the relationship between the SSE-CMM and other federal information security compliance standards. The questions addressed were as follows:

- How can the SSE-CMM assist in supporting the use of federal security standards and guidelines?
- How can the SSE-CMM be used to gather evidence of compliance?

In the past, SSE-CMM PA mappings to federal security standards and guidelines have been shown to be feasible and valuable in providing evidence for the evaluation of assurance mechanisms. In all such mappings, the SSE-CMM is viewed as complementary to the associated evaluation criteria and provides a structured basis for evidence gathering and assurance. The HIPAA regulations, however, require an enterprise view of an organization's privacy and security processes and procedures that is not implemented by the IT/IS evaluation mechanisms or fully covered by the SSE-CMM. Thus, there is a need for supplemental PAs to meet the proposed HIPAA information security legislative requirements. These supplemental PAs and selected SSE-CMM PAs comprise Corbett's HIPAA-CMM.

The SSE-CMM mappings that have been investigated ([FER97] and [GAL97]) were to the Common Criteria Assurance Requirements [CCP96], Defense Information Technology Security Certification and Accreditation Process (DITSCAP [DOD97]), and the Trusted Computer System Evaluation Criteria (TCSEC [DOD85]). The mappings also apply to the *National Information Assurance Certification and Accreditation Process* (NIACAP, [NST00]) because the NIACAP is an extension of the DITSCAP for non-defense government organizations. They were developed for the independent evaluation of government IT/IS and are very effective in performing that function. Also, a version of the NIACAP, the *Commercial INFOSEC Analysis Process* (CIAP), is under development for the evaluation of critical commercial systems.

Other SSE-CMM mappings have been proposed [HOP99] to ISO/IEC 13335 Information Technology — Security Techniques — Guidelines for the Management of IT Security (GMITS) — Part 2 [ISO]; the NIST Handbook [NIS95]; BS 7799 [BSI98]; and the Canadian Handbook on Information Technology Security MG-9 [CSE98].

We discuss the SSE-CMM mappings in more detail in Appendix D [of this report].

Background

The major issue relative to meeting HIPAA information security requirements at this time is that there is no standard process in place to determine HIPAA compliance. This situation becomes more complicated when institutions are evaluated according to different criteria and methodologies. What is needed is a standard methodology and evaluation model that is based on proven, valid techniques that are recognized by the information security community. The Corbett Technologies HIPAA-CMM was developed based on such techniques.

Reviews of HIPAA information security issues and *Capability Maturity Models* (CMMs) are presented in the following sections to provide a basis for developing the corresponding mappings.

HIPAA

The United States *Kennedy-Kassenbaum Health Insurance Portability and Accountability Act* (HIPAA-Public Law 104-191), effective August 21, 1996, addresses the issues of health care privacy and plan portability in the United States. With respect to privacy, the act stated, "Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit . . . detailed recommendations on standards with respect to the privacy of individually identifiable health information." The act further stated, "The recommendations . . . shall address at least the following:

- The rights that an individual who is a subject of individually identifiable health information should have
- The procedures that should be established for the exercise of such rights
- The uses and disclosures of such information that should be authorized or required"

The act then provided that if the legislation governing standards with respect to the privacy of individually identifiable health information is not enacted by "the date that is 36 months after the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act." Congress failed to act by that date, and therefore the Secretary of Health and Human Services was required to issue the privacy regulations no later than February 21, 2000. This date was not met, but the regulations were announced in December 2000 [HHS00] and included the following items:

- Coverage was extended to medical records of all forms, not only those in electronic form. This coverage includes oral and paper communications that did not exist in electronic form.
- Patient consent is required for routine disclosures of health records.
- Disclosure of full medical records for the purposes of treatment to providers is allowed.
- Protection was issued against the unauthorized use of medical records for employment purposes.

The privacy regulations were reopened for public comment for an additional period that closed on March 30, 2001. Also, the Security and Electronic Signature standards are still in draft form. The privacy regulations, however, state the following in reference to information system security requirements:

"(c) (1) Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) Implementation specification: safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart."

At the present state of the regulations, HIPAA provides the following penalties for violations:

- *General penalty for failure to comply* — each violation is \$100; maximum for all violations of an identical requirement cannot exceed \$25,000.
- *Wrongful disclosure of identifiable health information* — \$50,000, imprisonment of not more than one year, a or both.
- *Wrongful disclosure of identifiable health information under false pretenses* — \$100,000, imprisonment of not more than five years, or both.

- *Offense with intent to sell information* — \$250,000, imprisonment of not more than 10 years, or both.

Process Improvement

The basic premise of process improvement is that the quality of services produced is a direct function of the quality of the associated development and maintenance processes. The Carnegie Mellon *Software Engineering Institute* (SEI) has developed an approach to process improvement called the IDEAL model. IDEAL stands for Initiating, Diagnosing, Establishing, Acting, and Learning as defined in Table D.1 .

Table D.1: The IDEAL Model [SSE99]

I	Initiating	Laying the groundwork for a successful improvement effort.
D	Diagnosing	Determining where you are relative to where you want to be.
E	Establishing	Planning the specifics of how you will reach your destination.
A	Acting	Doing the work according to the plan.
L	Learning	Learning from the experience and improving your ability.

The goal is to establish a continuous cycle of evaluating the current status of your organization, making improvements, and repeating this cycle. The high-level steps are shown in Table D.1 .

Each of the five phases of the IDEAL approach is made up of several activities. These activities are summarized in Appendix C for application to security engineering.

The following basic principles of process change are necessary to implement a successful process improvement activity:

- Major changes must be sponsored by senior management.
- Focus on fixing the process, not assigning blame.
- Understand the current process first.
- Change is continuous.
- Improvement requires investment.
- Retaining improvement requires periodic reinforcement.

CMMs

In 1986, in collaboration with Mitre Corporation, the SEI developed a methodology for measuring the maturity of software development processes. This methodology was formalized into the CMM of Software [PAU95] [SEI95].

A CMM describes the stages through which processes progress as they are defined, implemented, and improved. Process capability is defined as the quantifiable range of expected results that can be achieved by following a process. To quote from the SSE-CMM,

“The model provides a guide for selecting process improvement strategies by determining the current capabilities of specific processes and identifying the issues most critical to quality and process improvement within a particular domain. A CMM may take the form of a reference model to be used as a guide for developing and improving a mature and defined process.”

The CMM has been applied to many environments as the framework for implementing process improvement. Table D.2 contrasts the SSE-CMM with other related efforts. Note that the SSE-CMM is the only approach that is focused on information system security engineering.

Effort	Goal	Approach	Scope
SSE-CMM	Define, improve, and assess security engineering capability	Continuous security engineering maturity model and appraisal method	Security engineering organizations
SE-CMM	Improve system or product engineering process	Continuous maturity model of systems engineering practices and appraisal method	Systems engineering organizations
SEI CMM for Software	Improve the management of software development	Staged maturity model of software engineering and management practices	Software engineering organizations
Trusted CMM	Improve the process of high integrity software development and its environment	Staged maturity model of software engineering and management practices including security	High integrity software organizations
CMMI	Combine existing process improvement models into a single	Sort, combine, and arrange process improvement	Engineering organizations

Table D.2: The SSE-CMM and Related Efforts [SSE99]

Effort	Goal	Approach	Scope
	architectural framework	nt building blocks to form tailored models	
Systems Engineering CM (EIA731)	Define, improve, and assess systems engineering capability	Continuous systems engineering maturity model and appraisal method	Systems engineering organizations
Common Criteria	Improve security by enabling reusable protection profiles for classes of technology	Set of functional and assurance requirements for security, along with an evaluation process	Information technology
CISSP	Make security professional a recognized discipline	Security body of knowledge and certification tests for security profession	Security practitioners
Assurance Frameworks	Improve security assurance by enabling a broad range of evidence	Structured approach for creating assurance arguments and efficiently producing evidence	Security engineering organizations
ISO 9001	Improve organizational quality management	Specific requirements for quality management practices	Service organizations

Table D.2: The SSE-CMM and Related Efforts [SSE99]

Effort	Goal	Approach	Scope
ISO 15504	Software process improvement and assessment	Software process improvement model and appraisal methodology	Software engineering organizations
ISO 13335	Improvement of management of information technology security	Guidance on process used to achieve and maintain appropriate levels of security for information and services	Security engineering organizations

The HIPAA-CMM is based on the SE-CMM and SSE-CMM; therefore, the SE and SSE-CMMs are described briefly in the following sections.

The Systems Engineering CMM

The SSE-CMM is based on the *Systems Engineering CMM* (SE-CMM). The eleven Project and Organizational PAs of the SSE-CMM come directly from the SE-CMM. These areas are as follows:

- PA12 — Ensure Quality
- PA13 — Manage Configuration
- PA14 — Manage Project Risk
- PA15 — Monitor and Control Technical Effort
- PA16 — Plan Technical Effort
- PA17 — Define Organization's Systems Engineering Process
- PA18 — Improve Organization's Systems Engineering Process
- PA19 — Manage Product Line Evolution
- PA20 — Manage Systems Engineering Support Environment
- PA21 — Provide Ongoing Skills and Knowledge
- PA22 — Coordinate with Suppliers

The SE-CMM [BAT94] describes the essential elements of an organization's systems engineering process that must exist in order to ensure good systems engineering. It also provides a reference to compare existing systems engineering practices against the essential systems engineering elements described in the model. The definition of systems engineering on which the SE-CMM is based is defined as the selective application of scientific and engineering efforts to:

- Transform an operational need into a description of the system configuration that best satisfies the operational need according to the measures of effectiveness.

- Integrate related technical parameters and ensure compatibility of all physical, functional, and technical program interfaces in a manner that optimizes the total system definition and design.
- Integrate the efforts of all engineering disciplines and specialties into the total engineering effort.

Similarly, a system is defined as follows:

- An integrated composite of people, products, and processes that provide a capability to satisfy a need or objective.
- An assembly of things or parts forming a complex or unitary whole; a collection of components organized to accomplish a specific function or set of functions.
- An interacting combination of elements that are viewed in relation to function.

The SSE-CMM

The SSE-CMM takes a process-based approach to information systems security and is based on the SE-CMM. The methodology and metrics of the SE-CMM are duplicated in the SSE-CMM in that they provide a reference for comparing existing the best systems security engineering practices against the essential systems security engineering elements described in the model. The SSE-CMM is the primary element of the proposed HIPAA-CMM.

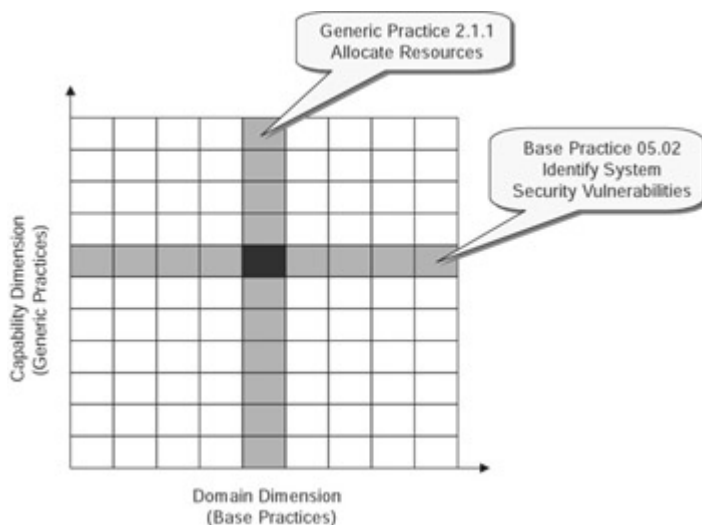


Figure D.1: The capability and domain dimensions of the SSE-CMM [SSE99].

The SSE-CMM defines two dimensions that are used to measure the capability of an organization to perform specific activities. These dimensions are *domain* and *capability*. The domain dimension consists of all of the practices that collectively define security engineering. These practices are called *base practices* (BPs). The capability dimension represents practices that indicate process management and institutionalization capability. These practices are called *generic practices* (GPs) because they apply across a wide range of domains. The GPs represent activities that should be performed as part of performing BPs. The relationship between BPs and GPs is given in Figure D.1, illustrating the evaluation of allocating resources in order to support the BP with identifying system security vulnerabilities.

For the domain dimension, the SSE-CMM specifies 11 security engineering PAs and 11 organizational and project-related PAs, each of which are comprised of BPs. BPs are mandatory characteristics that must exist within an implemented security engineering process before an organization can claim satisfaction in a given PA. The 22 PAs and their corresponding BPs incorporate the best practices of systems security engineering. The PAs are as follows:

- Technical
 - PA01 Administer Security Controls
 - PA02 Assess Impact
 - PA03 Assess Security Risk
 - PA04 Assess Threat
 - PA05 Assess Vulnerability
 - PA06 Build Assurance Argument
 - PA07 Coordinate Security
 - PA08 Monitor Security Posture
 - PA09 Provide Security Input
 - PA10 Specify Security Needs
 - PA11 Verify and Validate Security
- Project and Organizational Practices
 - PA12 — Ensure Quality
 - PA13 — Manage Configuration
 - PA14 — Manage Project Risk
 - PA15 — Monitor and Control Technical Effort
 - PA16 — Plan Technical Effort
 - PA17 — Define Organization's Systems Engineering Process
 - PA18 — Improve Organization's Systems Engineering Process
 - PA19 — Manage Product Line Evolution
 - PA20 — Manage Systems Engineering Support Environment
 - PA21 — Provide Ongoing Skills and Knowledge
 - PA22 — Coordinate with Suppliers

The GPs are ordered in degrees of maturity and are grouped to form and distinguish among five levels of security engineering maturity. The attributes of these five levels are as follows [SSE99]:

- Level 1
 - BPs are Performed
- Level 2
 - 2.1 Planning Performance
 - 2.2 Disciplined Performance
 - 2.3 Verifying Performance
 - 2.4 Tracking Performance
- Level 3
 - 3.1 Defining a Standard Process
 - 3.2 Perform the Defined Process
 - 3.3 Coordinate the Process
- Level 4
 - 4.1 Establishing Measurable Quality Goals
 - 4.2 Objectively Managing Performance
- Level 5
 - 5.1 Improving Organizational Capability
 - 5.2 Improving Process Effectiveness

The corresponding descriptions of the five levels are given as follows [SSE99]:

Level 1, “Performed Informally.” Focuses on whether an organization or project performs a process that incorporates the BPs. A statement characterizing this level would be, “You have to do it before you can manage it.”

Level 2, “Planned and Tracked.” Focuses on project-level definition, planning, and performance issues. A statement characterizing this level would be, “Understand what’s happening with the project before defining organization-wide processes.”

Level 3, “Well Defined.” Focuses on disciplined tailoring from defined processes at the organization level. A statement characterizing this level would be, “Use the best of what you’ve learned from your projects to create organization-wide processes.”

Level 4, “Quantitatively Controlled.” Focuses on measurements being tied to the business goals of the organization. Although it is essential to begin collecting and using basic project measures early, the measurement and use of data is not expected organization-wide until the higher levels have been achieved. Statements characterizing this level would be, “You can’t measure it until you know what ‘it’ is” and “Managing with measurement is only meaningful when you’re measuring the right things.”

Level 5, “Continuously Improving.” Gains leverage from all of the management practice improvements seen in the earlier levels, then emphasizes the cultural shifts that will sustain the gains made. A statement characterizing this level would be, “A culture of continuous improvement requires a foundation of sound management practice, defined processes, and measurable goals.”

The HIPAA-CMM uses the GPs, capability levels, and a major subset of the PAs of the SSE-CMM to evaluate HIPAA information security compliance. Remediation of the areas of weakness or noncompliance can then be addressed with confidence in a cost-effective manner.

HIPAA Security Requirements Mappings to PAs

Ideally, there would be a one-to-one mapping of all HIPAA information security requirements to the SSE-CMM PAs. There are, in fact, such mappings, but these mappings do not complete HIPAA compliance coverage based on the present state of the HIPAA regulations and the corresponding generally accepted best information security practices. Obviously, where the HIPAA requirements are process-oriented, there is a better mapping to the SSE-CMM PAs. The other HIPAA privacy regulations require more granularity and coverage of information security issues than the PAs of the SSE-CMM provide. These additional requirements are met by using the *HIPAA-specific PAs* (HPAs) as defined in this document.

In reviewing the HIPAA assurance requirements based on the extant privacy regulations, the draft Security and Electronic Signature standards, and the corresponding best information security practices, the following PAs from the SSE-CMM were selected. These PAs address a subset of the HIPAA requirements:

- Technical
 - PA01 Administer Security Controls
 - PA02 Assess Impact
 - PA03 Assess Security Risk
 - PA04 Assess Threat
 - PA05 Assess Vulnerability
 - PA06 Build Assurance Argument
 - PA07 Coordinate Security
 - PA08 Monitor Security Posture
 - PA09 Provide Security Input

- PA10 Specify Security Needs
- PA11 Verify and Validate Security
- Project and Organizational Practices
 - PA12 — Ensure Quality
 - PA13 — Manage Configuration
 - PA14 — Manage Project Risk
 - PA15 — Monitor and Control Technical Effort
 - PA17 — Define Organization’s Systems Engineering Process
 - PA21 — Provide Ongoing Skills and Knowledge
 - PA22 — Coordinate with Suppliers

The selected SSE-CMM PAs are detailed in Appendix A of this document.

To complete the coverage of evaluation of HIPAA compliance, newly defined PAs that are tailored to the remaining HIPAA requirements are needed. These HPAs are developed and described in the next section and are also included in Appendix A of this document.

The capability dimension of the SSE-CMM with its GPs will be used for the HIPAA-CMM model and its PAs.

Figure D.2 illustrates the combining of complementary SSE-CMM and HPAs to develop the HIPAA-CMM and to implement continuous process improvement.

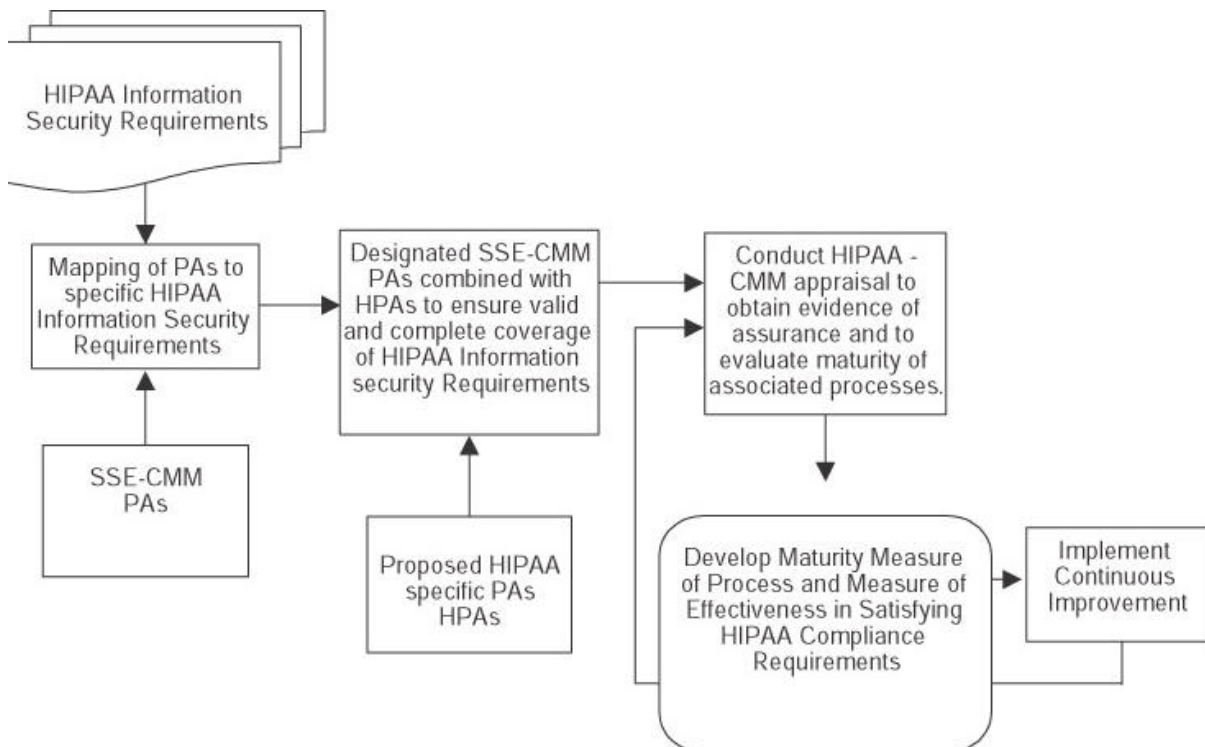


Figure D.2: HIPAA-CMM structure and use.

HPAs

Based on an analysis of the HIPAA privacy regulations and the draft Security and Electronic Signature standards, the following five categories of HIPAA requirements

based on best information security practices could not be directly matched to PAs of the SSE-CMM:

- Establishing and designating responsibility for ensuring that policies and procedures are followed relative to the release of individually identifiable patient healthcare information and establishing recourse for violations of these policies.
- Development of disaster recovery and business continuity plans for all relevant networks and systems.
- Establishing patient health care information protection, validation, and authentication through logical controls and protecting the confidentiality and data integrity of exchanged information with external entities.
- Establishing personnel information security policies and procedures.
- Addressing physical security requirements for information systems protection, including theft, fire, and other hazards.

Therefore, in order to complete the required coverage of the HIPAA compliance requirements, five PAs with corresponding BPs are needed. These HPAs incorporate the generally accepted best security engineering practices and are focused on the five identified HIPAA categories that could not be met by PAs of the SSE-CMM. The goals of the HPAs map to the HIPAA requirements, and the BPs provide guidance on the specific actions to take in order to confirm that the goals are accomplished.

The HPAs are listed as follows and are detailed with their base practices in Appendix A, Section A.2 of this document:

- HPA 01 Administer Patient Health Care Information Controls
- HPA 02 Develop Disaster Recovery and Business Continuity Plans For All Relevant Networks And Systems
- HPA 03 Establish Patient Health Care Information Security Controls
- HPA 04 Evolve Personnel Information Security Policies and Procedures
- HPA 05 Administer Physical Security Controls
- Defining and Using the HIPAA-CMM

The HIPAA information security requirements based on the extant HIPAA regulations and draft standards have been developed by using the generally accepted best information security practices. These requirements are best estimates at this time and are summarized in Tables D.3, D.4, and D.5.

HIPAA Mappings

The HIPAA security requirement mappings to SSE-CMM and the HPAs are also provided in [Tables D.3](#), [D.4](#), and [D.5](#). The listed PAs ensure that the processes are in place to evaluate the application of the specific assurance mechanisms required by the HIPAA legislation. A complete listing of the HIPAA-CMM PAs is given in Appendix A.

HIPAA Information Security Requirements	SSE-CMM Mapping	HPAs
1. Adopt written policies and procedures for the receipt, storage, processing, and distribution of information.	PA 01, 17, 22.	
2. Designate a Privacy Officer who is responsible for ensuring that the policies and procedures are followed and for the release of individually	PA 07, 10	HPA 01

Table D.3: Administrative Procedures

HIPAA Information Security Requirements	SSE-CMM Mapping	HPAs
identifiable patient healthcare information.		
3. Establish a security certification process that determines the degree to which the system, application, or network meets security requirements.	PA 11, 12	
4. Develop disaster recovery and business continuity plans for all relevant networks and systems.	PA 02, 03, 04, 05, 06, 14.	HPA 02
5. Train employees to ensure that they understand the new privacy protection procedures.	PA 21	
6. Establish contracts with all business partners protecting confidentiality and data integrity of exchanged information.	PA 22	HPA 03
7. Implement personnel security, including clearance policies and procedures.	PA 01, 09	HPA 04
8 .Develop and implement system auditing policies and procedures.	PA 01, 06, 08, 12,	13, 15
9. Establish boundaries on use and release of individual medical records.	PA 01, 06, 10, 11	HPA 01.
10. Ensure that patient consent is obtained prior to the release of medical information and that the consent is not coerced.	PA 01, 10	HPA 01.
11. Provide patients with education on the privacy protection accorded to them.	PA 01, 10	HPA 01
12. Ensure patients access to their medical records.	PA 01, 10	HPA 01
13. Establish patient recourse and penalties for violations of security policies and procedures.	PA 01, 10, 11	HPA 01.
14. Establish procedures for processing terminated personnel to prevent violation of information security policies and procedures.	PA 01, 21	HPA 04.

Table D.4: Technological Security Safeguards

HIPAA Information Security Requirements	SSE-CMM Mapping	HPAs
1. Implement encryption and/or access controls to prevent and detect unauthorized intrusions into the system and network.	PA 01, 10, 22	HPA 03.
2. Implement identification and authentication mechanisms for access to the system and network.	PA 01, 11, 13	HPA 03
3. Ensure that sensitive information is altered or destroyed by authorized personnel only and that these activities are logged.	PA 01, 06, 11	HPA 03
4. Establish means for message non-repudiation and authentication.	PA 01, 06, 11	HPA 03
5. Establish means to preserve integrity of messages or means to detect modification of a message.	PA 01, 06, 11	HPA 03
6. Establish and implement log-on and log-off procedures to protect against unauthorized access to workstations and systems off.	PA 01, 08, 11	HPA 03

Table D.5: Physical Security Measures

HIPAA Information Security Requirements	SSE-CMM Mapping	HPAs
1. Develop policies and procedures for handling, storage, and disposal of magnetic media and for object reuse.	PA 01, 06	HPA 05.
2. Protect computer systems and related buildings and equipment from fire and other hazards.	PA 01, 02, 03, 04, 05, 08, 11	HPA 05
3. Use physical controls to limit access to computer systems and facilities to authorized personnel.	PA 01, 03, 07, 11	HPA 05.
4. Physically secure workstations and laptops.	PA 01, 03, 11	HPA 05

Using the HIPAA-CMM

Conducting an appraisal by using the mappings defined in the tables provides the means to measure the quality of the processes in place to meet the HIPAA information security-related regulation requirements. To provide meaningful results, the question of, “What capability level ensures compliance?” has to be answered. The standard proposed in this approach is that *for all the HIPAA-CMM PAs, the Level 2 GPs as*

defined in the SSE-CMM have to be achieved for minimum HIPAA information security-related compliance. For the compliance to remain in place over the long term and be considered an element of continuous process improvement, the Level 3 GPs must be obtained as a minimum.

As noted in Figure D.2, the appraisal results are used to implement continuous improvement of the information security processes.

Conclusion

A HIPAA-CMM and assessment methodology is being developed as a standard for evaluating HIPAA compliance. With appropriate guidance and use of the SSE-CMM PAs and the defined HPAs to achieve the additional granularity and coverage as required, the proposed HIPAA-CMM provides a formal, repeatable, and consistent methodology to assess an organization's HIPAA compliance. This approach will identify areas of strong compliance, marginal compliance, and lack of compliance and will provide a consistent basis for defining remediation means. Inherently, the HIPAA-CMM also serves as a tool for implementing continuous improvement and for evaluating the effectiveness of the improvement

References

[BAT94] Bate, Roger; Garcia, Suzanne et. al, "A Systems Engineering Capability Maturity Model Version 1.0," SEI, 1994.

[BSI98] British Standards Institute, United Kingdom, "Information Security Management, British Standard 7799," 1998.

[CCP96] Common Criteria Project; "Common Criteria for Information Technology Security Evaluation, v1.0," January 1996.

[CSE98] Communications Security Establishment, Government of Canada, "Canadian Handbook on Information Technology Security MG-9," 1998.

[CUR95] Curtis, Bill; Hefley, William; and Miller, Sally, "The People Capability Maturity Model," SEI, 1995.

[DOD85] Department of Defense, "Department of Defense Trusted Computer System Evaluation Criteria," DoD 5200.28-STD, December 1985.

[DOD97] Department of Defense; "Department of Defense Information Technology Security Certification and Accreditation Process," 1997.

[NST00] National Security Telecommunications and Information Systems Security Committee; "National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP)," April 2000.

[FER97] Ferraiolo, Karen; Gallagher, Lisa; Thompson, Victoria; "Final Report Contract Number 50-DKNCB-7-90099, Process-Based Assurance Product Suite," December 1997.

[GAL97] Ferraiolo, Karen; Gallagher, Lisa; Thompson, Victoria; "Building a Case for Assurance from Process," December 1999.

[HHS00] HHS; "HHS Fact Sheet," December 2000.

[HOP99] Hopkinson, John; "The Relationship Between the SSE-CMM and IT Security Guidance Documentation," 1999.

[HUM89] Humphrey, Watts; "Managing the Software Process," 1989.

[ISO] ISO; "ISO/IEC 13335 Information Technology — Security Techniques — Guidelines for the Management of IT Security — Part 1: Concepts and Models, Part 2: Managing and Planning, Part 3: Management Techniques, Part 4: Baseline Control, and Part 5: Safeguards for External Connections."

[NIS95] National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, "An Introduction to Computer Security"; The NIST Handbook, 1995.

[PAU95] SEI, "The Capability Maturity Model: Guidelines for Improving the Software Process," Addison Wesley, 1995.

[SEI95] SEI, "The Capability Maturity Model," 1995.

[SSE99] "The Systems Security Engineering Capability Maturity Model v2.0," 1999.

Appendix A — HIPAA-CMM PA Overview

(Comprised of PAs from the SSE-CMM v2.0 and the HPAs)

Appendix A—HIPAA-CMM PA Overview

(Comprised of Pas from the SSE-CMMv2.0 and the HPAs)

A.1 SSE-CMM

PA 01	
Administer Security Controls	
Goal 1	Security controls are properly configured and used.
BP.01.01	Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.
BP.01.02	Manage the configuration of system security controls.
BP.01.03	Manage security awareness, training, and education programs for all users and administrators.
BP.01.04	Manage periodic maintenance and administration of security services and control mechanisms.

PA 02	
Assess Impact	
Goal 1	The security impacts of risks to the system are identified and characterized.
BP.02.01	Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system.
BP.02.02	Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system.
BP.02.03	Select the impact metric to be used for this assessment.
BP.02.04	Identify the relationship between the selected metrics for this assessment and metric conversion factors if required.
BP.02.05	Identify and characterize impacts.
BP.02.06	Monitor ongoing changes in the impacts.
PA 03	
Assess Security Risk	
Goal 1	An understanding of the security risk associated with operating the system within a defined environment is achieved.
Goal 2	Risks are prioritized according to a defined methodology.
BP.03.01	Select the methods, techniques, and criteria by which security risks for the system in a defined environment are analyzed, assessed, and compared.
BP.03.02	Identify threat/vulnerability/impact triples (exposures).
BP.03.03	Assess the risk associated with the occurrence of an exposure.
BP.03.04	Assess the total uncertainty associated with the risk for the exposure.
BP.03.05	Order the risks by priority.
BP.03.06	Monitor ongoing changes in the risk

PA 03	
Assess Security Risk	
	spectrum and changes to their characteristics.
PA 04	
Assess Threat	
Goal 1	Threats to the security of the system are identified and characterized.
BP.04.01	Identify applicable threats arising from a natural source.
BP.04.02	Identify applicable threats arising from man-made sources, either accidental or deliberate.
BP.04.03	Identify appropriate units of measure, and applicable ranges, in a specified environment.
BP.04.04	Assess capability and motivation of threat agent for threats arising from manmade sources.
BP.04.05	Assess the likelihood of an occurrence of a threat event.
BP.04.06	Monitor ongoing changes in the threat spectrum and changes to their characteristics.
PA 05	
Assess Vulnerability	
Goal 1	An understanding of system security vulnerabilities within a defined environment is achieved.
BP.05.01	Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized.
BP.05.02	Identify system security vulnerabilities.
BP.05.03	Gather data related to the properties of the vulnerabilities.
BP.05.04	Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations

PA 05	
Assess Vulnerability	
	of specific vulnerabilities.
BP.05.05	Monitor changes in applicable vulnerabilities and to their characteristics.
PA 06	
Build Assurance Agreement	
Goal 1	The work products and processes clearly provide the evidence that the customer's security needs have been met.
BP.06.01	Identify the security assurance objectives.
BP.06.02	Define a security assurance strategy to address all assurance objectives.
BP.06.03	Identify and control security assurance evidence.
BP.06.04	Perform analysis of security assurance evidence.
BP.06.05	Provide a security assurance argument that demonstrates the customer's security needs are met.
PA 07	
Coordinate Security	
Goal 1	All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions.
Goal 2	Decisions and recommendations related to security are communicated and coordinated.
BP.07.01	Define security engineering coordination objectives and relationships.
BP.07.02	Identify coordination mechanisms for security engineering.
BP.07.03	Facilitate security engineering coordination.

PA 07	
Coordinate Security	
BP.07.04	Use the identified mechanisms to coordinate decisions and recommendations related to security.
PA 08	
Monitor Security Posture	
Goal 1	Both internal and external security-related events are detected and tracked.
Goal 2	Incidents are responded to in accordance with policy.
Goal 3	Changes to the operational security posture are identified and handled in accordance with the security objectives.
BP.08.01	Analyze event records to determine the cause of an event, how it proceeded, and likely future events.
BP.08.02	Monitor changes in threats, vulnerabilities, impacts, risks, and environment.
BP.08.03	Identify security-relevant incidents.
BP.08.04	Monitor the performance and functional effectiveness of security safeguards.
BP.08.05	Review the security posture of the system to identify necessary changes.
BP.08.06	Manage the response to security-relevant incidents.
BP.08.07	Ensure that the artifacts related to security monitoring are suitably protected.
PA 09	
Provide Security Input	
Goal 1	All system issues are reviewed for security implications and are resolved in accordance with security goals.
Goal 2	All members of the project team have an understanding of security so they can perform their functions.

PA 09	
Provide Security Input	
Goal 3	The solution reflects the security input provided.
BP.09.01	Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.
BP.09.02	Determine the security constraints and considerations needed to make informed engineering choices.
BP.09.03	Identify alternative solutions to security-related engineering problems.
BP.09.04	Analyze and prioritize engineering alternatives using security constraints and considerations.
BP.09.05	Provide security-related guidance to the other engineering groups.
BP.09.06	Provide security-related guidance to operational system users and administrators.
PA 10	
Specific Security Needs	
Goal 1	A common understanding of security needs is reached between all parties, including the customer.
BP.10.01	Gain an understanding of the customer's security needs.
BP.10.02	Identify the laws, policies, standards, external influences, and constraints that govern the system.
BP.10.03	Identify the purpose of the system in order to determine the security context.
BP.10.04	Capture a high-level security-oriented view of the system operation.
BP.10.05	Capture high-level goals that define the security of the system.
BP.10.06	Define a consistent set of statements that define the protection to be implemented in the system.

PA 10	
Specific Security Needs	
BP.10.07	Obtain agreement that the specified security meets the customer's needs.
PA 11	
Verify and Validate Security	
Goal 1	Solutions meet security requirements.
Goal 2	Solutions meet the customer's operational security needs.
BP.11.01	Identify the solution to be verified and validated.
BP.11.02	Define the approach and level of rigor for verifying and validating each solution.
BP.11.03	Verify that the solution implements the requirements associated with the previous level of abstraction.
BP.11.04	Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs.
BP.11.05	Capture the verification and validation results for the other engineering groups.

Project and Organizational PA Overview

The project and organizational PA category groups together those PAs that are primarily concerned with improving project and organizational capability.

PA 12	
Ensure Quality	
Goal 1	Process quality is defined and measured.
Goal 2	Expected work product quality is achieved.
BP.12.01	Monitor conformance to the defined process.
BP.12.02	Measure work product quality.

PA 12	
Ensure Quality	
BP.12.03	Measure quality of the process.
BP.12.04	Analyze quality measurements.
BP.12.05	Obtain participation.
BP.12.06	Initiate quality improvement activities.
BP.12.07	Detect need for corrective actions.
PA 13	
Manage Configurations	
Goal 1	Control over work product configurations is maintained.
BP.13.01	Establish configuration management methodology.
BP.13.02	Identify configuration units.
BP.13.03	Maintain work product baselines.
BP.13.04	Control changes.
BP.13.05	Communicate configuration status.
PA 14	
Manage Project Risk	
Goal 1	Risks to the program are identified, understood, and mitigated.
BP.14.01	Develop a risk-management approach.
BP.14.02	Identify risks.
BP.14.03	Assess risks.
BP.14.04	Review your risk assessment.
BP.14.05	Execute risk mitigation.
BP.14.06	Track risk mitigation.
PA 15	
Monitor and Control Technical Effort	
Goal 1	The technical effort is monitored and controlled.
BP.15.01	Direct the technical effort.

PA 15	
Monitor and Control Technical Effort	
BP.15.02	Track project resources.
BP.15.03	Track technical parameters.
BP.15.04	Review project performance.
BP.15.05	Analyze project issues.
BP.15.06	Take corrective action.
PA 17	
Define Organization's Security Engineering Process	
Goal 1	A standard systems engineering process is defined for the organization.
BP.17.01	Establish process goals.
BP.17.02	Collect process assets.
BP.17.03	Develop the organization's security engineering process.
BP.17.04	Define tailoring guidelines.
PA 21	
Provide Ongoing Skills and Knowledge	
Goal 1	The organization has the skills necessary to achieve project and organizational objectives.
BP.21.01	Identify training needs.
BP.21.02	Select mode of knowledge or skill acquisition.
BP.21.03	Assure availability of skill and knowledge.
BP.21.04	Prepare training materials.
BP.21.05	Train personnel.
BP.21.06	Assess training effectiveness.
BP.21.07	Maintain training records.
BP.21.08	Maintain training materials.
PA 22	
Coordinate with Suppliers	

PA 22

Coordinate with Suppliers	
Goal 1	Effective suppliers are selected and used.
BP.22.01	Identify systems components or services.
BP.22.02	Identify competent suppliers or vendors.
BP.22.03	Choose suppliers or vendors.
BP.22.04	Provide expectations.
BP.22.05	Maintain communications.

A.2 HPAs

HPA 01	
Administer Patient Health Care Information Controls	
Goal 1	Privacy officer is designated with required authority and responsibility.
Goal 2	Limitations and guidance on the use and disclosure of individual medical information are established.
BP 01.01	Designate a privacy officer who is responsible for enforcing policies and procedures and for the release of individually identifiable patient healthcare information.
BP 01.02	Establish boundaries on individual medical records' use and release.
BP 01.03	Establish recourse for violations of policies on use and release of individual medical records.
BP 01.04	Provide patients with education on the privacy protection accorded to them.
BP 01.05	Establish patient recourse and penalties for violations of security policies and procedures.
BP 01.06	Ensure patient access to their individual medical records.
HPA 02	

Develop Disaster Recovery And Business Continuity Plans For All Relevant Networks And Systems	
Goal 1	Business Continuity Plan is developed and institutionalized.
Goal 2	Disaster Recovery Plan is developed and institutionalized.
BP 02.01	Establish Disaster Recovery Plan (Evaluate this process using supplementary information from SSE-CMM PAs 02, 03, 04 and 05).
BP 02.02	Establish Business Continuity Plan (Evaluate this process using supplementary information from SSE-CMM PAs 02, 03, 04, and 05).
BP 02.03	Institutionalize Disaster Recovery Plan.
BP 02.04	Institutionalize Business Continuity Plan.
HPA 03	
Establish Patient Health Care Information Security Controls	
Goal 1	Individual patient health care information is protected from unauthorized disclosure and modification.
Goal 2	Authentication and non-repudiation are established for external and internal patient health care information exchange.
BP 03.01	Provide encryption to preserve privacy of transmitted or stored patient health care information.
BP 03.02	Provide identification and authentication mechanisms for access to the system and network.
BP 03.03	Manage the destruction or alteration of sensitive information, including logging of these activities.
BP 03.04	Provide means for message non-repudiation and authentication.
BP 03.05	Preserve the integrity of messages and provide means to detect modification of messages.

HPA 03	
Establish Patient Health Care Information Security Controls	
BP 03.06	Provide log-on and log-off procedures to protect against unauthorized access to workstations and systems.
BP 03.07	Protect the confidentiality and data integrity of exchanged information with partners through appropriate contracts (evaluate in conjunction with PA 22 of the SSE-CMM).
HPA 04	
Evolve Personnel Information Security Policies and Procedures	
Goal 1	Personnel security controls are properly defined, administered, and used.
BP 04.01	Provide means and methods for processing terminated personnel to prevent violation of information security policies and procedures.
BP 04.02	Manage personnel security issues, including clearance policies and procedures.
HPA 05	
Administer Physical Security Controls	
Goal 1	Physical security controls are properly administered and used.
BP 05.01	Establish policies and procedures for handling, storage, and disposal of magnetic media and for object reuse.
BP 05.02	Provide means and methods to protect computer systems and related buildings and equipment from fire and other hazards.
BP 05.03	Provide physical controls to limit access to computer systems and facilities to authorized personnel.
BP 05.04	Provide for physical security of workstations and laptops.

Appendix B — Glossary (SSE-CMM v2.0)

Accountability

The property that ensures that the actions of an entity can be traced uniquely to the entity [ISO 7498-2; 1988].

Accreditation

A formal declaration by a designated approving authority that a system is approved to operate in a particular security mode by using a prescribed set of safeguards.

Assessment

An appraisal by a trained team of professionals to determine the state of an organization's current process, to determine the high-priority, process-related issues facing an organization, and to obtain the organizational support for process improvement.

Asset

Anything that has value to the organization [ISO 13335-1: 1996].

Assurance

The degree of confidence that security needs are satisfied [NIST94].

Assurance Argument

A set of structured assurance claims supported by evidence and reasoning that demonstrate clearly how assurance needs have been satisfied.

Assurance Claim

An assertion or supporting assertion that a system meets a security need. Claims address both direct threats (for example, system data are protected from attacks by outsiders) and indirect threats (for example, system code has minimal flaws).

Assurance Evidence

Data on which a judgment or conclusion about an assurance claim can be based. The evidence might consist of observations, test results, analysis results, and appraisals providing support for the associated claims.

Authenticity

The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems, and information [ISO 13335-1:1996].

Availability

The property of being accessible and useable upon demand by an authorized entity [ISO 7498-2: 1988].

Baseline

A specification or product that has been formally reviewed and agreed upon that thereafter serves as the basis for further development and that can be changed only through formal change control procedures [IEEE-STD-610].

Certification

Comprehensive evaluation of security features and other safeguards of an AIS to establish the extent to which the design and implementation meet a set of specified security requirements.

Confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO 7498-2:1988].

Consistency

The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component [IEEE-STD-610].

Correctness

A property of a representation of a system or product such that it accurately reflects the specified security requirements for that system or product.

Customer

The individual or organization that is responsible for accepting the product and authorizing payment to the service/development organization.

Data Integrity

The property that data has not been altered or destroyed in an unauthorized manner [ISO 7498-2:1988].

Effectiveness

A property of a system or product representing how well it provides security in the context of its proposed or actual operational use.

Engineering Group

A collection of individuals (both managers and technical staff) who are responsible for project or organizational activities related to a particular engineering discipline (for example, hardware, software, software configuration management, software quality assurance, systems, system test, and system security).

Evidence

Directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfies a specified requirement.

Group

The collection of departments, managers, and individuals who have responsibility for a set of tasks or activities. The size can vary from a single individual assigned part-time, to several part-time individuals assigned from different departments, to several dedicated full-time individuals.

Integrity

See data integrity and system integrity.

Maintenance

The process of modifying a system or component after delivery in order to correct flaws, improve performance or other attributes, or to adapt to a changed environment [IEEE-STD-610].

Methodology

A collection of methods, procedures, and standards that define an integrated synthesis of engineering approaches to the development of a product or system.

Objective

Non-biased.

Penetration Profile

A delineation of the activities that are required to effect a penetration.

Privacy

The right of an individual or entity to control the acquisition, storage, and dissemination of information about the individual or entity.

Procedure

A written description of a course of action to be taken in order to perform a given task [IEEE-STD-610].

Process

A sequence of steps performed for a given purpose [IEEE-STD-620].

Reliability

The property of consistent behavior and results [IEEE 13335-1:1996].

Residual Risk

The risk that remains after safeguards have been implemented [IEEE 13335-1:1996].

Risk

The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets [IEEE 13335-1:1996].

Risk Analysis

The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards [IEEE 13335-1:1996].

Risk Management

The process of assessing and quantifying risk and establishing an acceptable level of risk for the organization [IEEE 13335-1:1996].

Security

The preservation of confidentiality, integrity, availability, and authenticity of information; protection from intrusion or compromise of information that will cause harm to the organization.

Security Engineering

Security engineering is an evolving discipline. As such, a precise definition with community consensus does not exist today. Some generalizations are possible, however. Some goals of security engineering are to:

- Gain an understanding of the security risks associated with an enterprise.
- Establish a balanced set of security needs in accordance with identified risks.
- Transform security needs into security guidance to be integrated into the activities of other disciplines employed on a project and into descriptions of a system configuration or operation.
- Establish confidence or assurance in the correctness and effectiveness of security mechanisms.
- Determine that operational impacts due to residual security vulnerabilities in a system or its operation are tolerable (acceptable risks).
- Integrate the efforts of all engineering disciplines and specialties into a combined understanding of the trustworthiness of a system.

Security Policy

Rules, directives, and practices that govern how assets, including sensitive information, are managed, protected, and distributed within an organization and its systems.

Security Related Requirements

Requirements that have a direct effect on the secure operation of a system or enforce conformance to a specified security policy.

Signature Authority

Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

System

A collection of components organized to accomplish a specific function or set of functions [IEEE-STD-610]; a system can include many products; a product can be the system.

Threat Capabilities

Intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or a system.

Validation

The process of assessing a system to determine whether it satisfies the specified requirements.

Verification

The process of assessing a system to determine whether the work products of a given development phase satisfy the conditions imposed at the start of that phase.

Vulnerability

Includes a weakness of an asset or group of assets that can be exploited by a threat [IEEE 13335-1:1996].

Work Product

Output of a process.

Appendix C

The Ideal Approach to Process Improvement

The Carnegie Mellon *Software Engineering Institute* (SEI) has developed an approach to process improvement called IDEAL, which stands for Initiating, Diagnosing, Establishing, Acting, and Learning.

The goal is to establish a continuous cycle of evaluating the current status of your organization, making improvements, and repeating this process. The high-level steps are described as follows and appear in Table D.1.

I	Initiating	Laying the groundwork for a successful improvement effort
D	Diagnosing	Determining where you are relative to where you want to be
E	Establishing	Planning the specifics of how you will reach your destination
A	Acting	Doing the work according to the plan

L	Learning	Learning from the experience and improving your ability
---	----------	---

The Initiating Phase

Embarking upon a security engineering process improvement effort should be handled in the same manner in which all new projects within an organization are approached. One must become familiar with the project's objectives and means for their accomplishment, develop a business case for the implementation, gain the approval and confidence of management, and develop a method for the project's implementation.

Effective and continuous support of the effort throughout its lifetime is essential for successful process improvement. Sponsorship involves not only making available the financial resources necessary to continue the process but also requires personal attention from management to the project.

After the relationship between the proposed effort and business goals has been established and key sponsors have given their commitment, a mechanism for the project's implementation must be established.

The Diagnosing Phase

In order to perform process development/improvement activities, it is imperative that an understanding of where organization's current and desired future state of process maturity be established. These parameters form the basis of the organization's process improvement action plan.

Performing a gap analysis emphasizes the differences between the current and desired states of the organization's processes and reveals additional information or findings about the organization. Grouped according to area of interest, these findings form the basis of recommendations for how to improve the organization.

The Establishing Phase

In this phase, a detailed plan of action based on the goals of the effort and the recommendations developed during the diagnosing phase is developed. In addition, the plan must take into consideration any possible constraints, such as resource limitations, which might limit the scope of the improvement effort. Priorities along with specific outputs and responsibilities are also put forth in the plan.

Time constraints, available resources, organizational priorities, and other factors might not allow for all of the goals to be realized or recommendations implemented during a single instance of the process improvement lifecycle. Therefore, the organization must establish priorities for its improvement effort.

As a result of the organization characterization defined in the diagnosing phase and established priorities, the scope of the process improvement effort might be different from that developed in the initiating phase. The develop approach step requires that the redefined objectives and recommendations be mapped to potential strategies for accomplishing the desired outcomes.

At this point, all of the data, approaches, recommendations, and priorities are brought together in the form of a detailed action plan. Included in the plan are the allocation of responsibilities, resources, and specific tasks, tracking tools to be used, and

established deadlines and milestones. The plan should also include contingency plans and coping strategies for any unforeseen problems.

The Acting Phase

This phase is the implementation phase and requires the greatest level of effort of all the phases both in terms of resources and time. Achieving the goals of the organization might require multiple parallel cycles within the acting phase in order to address all of the desired improvements and priorities.

Solutions, or improvement steps, for each problem area are developed based on available information on the issue and resources for implementation. At this stage, the solutions are 'best guess' efforts of a technical working group.

The first step in designing processes that will meet the business needs of an enterprise is to understand the business, product, and organizational context that will be present when the process is being implemented. Some questions that need to be answered before process design include the following:

- How is security engineering practiced within the organization?
- What life cycle will be used as a framework for this process?
- How is the organization structured to support projects?
- How are support functions handled (for example, by the project or by the organization)?
- What are the management and practitioner roles used in this organization?
- How critical are these processes to organizational success?

Because first attempts at generating solutions rarely succeed, all solutions must be tested before they are implemented across an organization. How an organization chooses to test its solutions is dependent upon the nature of the area of interest, the proposed solution, and the resources of the organization.

Using information collected during testing, potential solutions should be modified to reflect new knowledge about the solution. The importance of the processes under focus as well as the complexity of the proposed improvements will dictate the degree of testing and refinement proposed solutions must undergo before being considered acceptable for implementation throughout the organization.

Once a proposed improved process has been accepted, it must be implemented beyond the test group. Depending upon the nature and degree to which a process is being improved, the implementation stage might require significant time and resources. Implementation can occur in a variety of ways depending upon the organization's goals.

The Learning Phase

The learning phase is both the final stage of the initial process improvement cycle and the initial phase of the next process improvement effort. Here the entire process improvement effort is evaluated in terms of goal realization and how future improvements can be instituted more efficiently. This phase is only as constructive as the detail of records kept throughout the process and the ability of participants to make recommendations.

Determining the success of process improvement requires analyzing the final results in light of the established goals and objectives. It also requires evaluating the efficiency of

the effort and determining where further enhancements to the process are required. These lessons learned are then collected, summarized, and documented.

Based on the analysis of the improvement effort itself, the lessons learned are translated into recommendations for improving subsequent improvement efforts. These recommendations should be promulgated outside those guiding the improvement effort for incorporation in this and other improvement efforts.

Appendix D — SSE-CMM MAPPINGS, General Considerations

This mapping of process-based mechanisms (SSE-CMM) to assurance-based mechanisms (Common Criteria, DITSCAP, TCSEC) has been addressed by [GAL97] and [FER97] and produced the following general conclusions:

- Although there is a significant overlap between the SSE-CMM PAs and the assurance-based activities, there is not always a complete one-to-one mapping.
- The SSE-CMM may not provide the level of granularity required to directly address all specific assurance requirements.
- The SSE-CMM can be used to develop assurance arguments and product assurance evidence if applied with appropriate guidance.
- In most cases, the PAs of the SSE-CMM correspond well with the processes of the traditional assurance methods.
- The processes defined in the SSE-CMM are considered to contribute to the development of assurance arguments by integrators, product developers, evaluators, and manufacturers.
- With the appropriate guidance, tailoring, and evidence gathering, it was demonstrated that the results of an SSE-CMM assessment could support important aspects of traditional assurance-based mechanisms.
- The SSE-CMM can be viewed as a common thread that logically links traditional assurance methods.

In a similar vein, Hopkinson [HOP99] has proposed mappings to ISO/IEC 13335 Information Technology — Security Techniques — Guidelines for the Management of IT Security (GMITS) — Part 2 [ISO]; the NIST Handbook [NIS95]; BS 7799 [BSI98]; and the Canadian Handbook on Information Technology Security MG-9 [CSE98].

In all of the referenced mappings and the HIPAA mappings developed in this paper, the SSE-CMM is complementary to the associated evaluation criteria and provides a structured basis for evidence gathering and assurance. For specific assurance areas in HIPAA requiring more granularity than provided by the SSE-CMM, however, additional BPs must be applied.

As stated in [GAL97], “For the evaluators and certifiers, the SSE-CMM can provide direct evidence regarding process claims, as well as a uniform method to evaluate claims and evidence, thus contributing to the normalization of the evaluation/certification process — making the process more defined and repeatable and less intuitive. Ultimately, this direct benefit can be measured in terms of cost/schedule savings to evaluation and certification efforts.”

Therefore, for assurance-based security mechanisms such as required by HIPAA, the SSE-CMM can provide a basis to develop a structured framework for the following:

- Ensuring the appropriate processes corresponding to the required assurance mechanisms are in place
- Evidence gathering to support assurance claims

- Ensuring complete coverage of required regulations or standards
- Measuring the present information security posture
- Evaluating effectiveness of remediation efforts
- Ensuring repeatability of the appraisal process
- Continuous improvement of the security processes

Appendix E: The NSA InfoSec Assessment Methodology

As a result of Presidential Decision Directive #63, forming the National Infrastructure Protection Center, the National Security Agency's *Information Systems Security Organization* (ISSO) instituted a program intended to improve the overall level of security protection of America's computing infrastructure. To help achieve this goal, the ISSO designed the *InfoSec Assessment Methodology* (IAM) and implemented a training course focused on private, commercial business security providers. Because the ISSO itself focuses solely on auditing those parts of the computing infrastructure that are considered critical to the government, it implemented a training and certification process for security practitioners in the private sector with the intention that those practitioners would incorporate the IAM into their repertoire of security auditing procedures. The IAM certification courses are conducted a few times each year. A security practitioner has to satisfy a fairly stringent experience requirement to be considered for the training.

History of the NIPC

Excerpted from www.nipc.gov

February 26, 1998, the Department of Justice and the *Federal Bureau of Investigation* (FBI) created the *National Infrastructure Protection Center* (NIPC) at FBI Headquarters in Washington, D.C. The center is a joint government and private-sector partnership that includes representatives from the relevant agencies of federal, state, and local government. The concept for the NIPC grew out of recommendations of the President's Commission on Critical Infrastructure Protection and from the government's experiences in dealing with illegal intrusions into government and private-sector computer systems over the years.

May 22, 1998, President Clinton announced two new directives (*see below*) designed to strengthen the Nation's defenses against terrorism and other unconventional threats: *Presidential Decision Directives* (PDD) 62 and 63. PDD-62 highlights the growing range of unconventional threats that we face, including "cyber terrorism" and chemical, radiological, and biological weapons, and creates a new and more systematic approach to defending against these attacks. PDD-63 focuses specifically on protecting the Nation's critical infrastructures from both physical and cyber attacks.

These attacks might come from foreign governments, foreign and domestic terrorist organizations, or foreign and domestic criminal organizations. The NIPC is part of the broader framework of government efforts established by PDD-63. Under the PDD, the NIPC serves as the national focal point for threat assessment, warning, investigation, and responses to attacks on the critical infrastructures. A significant part of its mission involves establishing mechanisms to increase the sharing of vulnerability and threat information between the government and private industry.

About the ISSO

Excerpted in its entirety from NSA INFOSEC Page — About the ISSO — Delivering IA Solutions for Cyber Systems, Revised November 2, 1999.

In order to enable our customers to protect and defend cyber systems, the NSA develops and supports a variety of products and services. We also conduct ongoing research to aid in the development of next generation solutions. Our IA solutions must encompass a wide range of voice, data, and video applications extending across networked, tactical, and satellite systems. IA solutions include the technologies, specifications and criteria, products, product configurations, tools, standards, and

operational doctrine and support activities that are needed to implement the protect, detect and report, and respond elements of cyber defense.

The Information Assurance Framework Forum, developed in a collaborative effort by NSA solution architects, customers with requirements, component vendors, and commercial integrators, guides our solution development. It finds the right solution for environments ranging from outer space to the office or foxhole. Our framework provides top-level guidance in addition to the specification of essential security features and assurances for the security products. It brings producers and consumers together before products are built so that products that better meet our customers' needs will be built.

The internationally recognized *Common Criteria* (CC) employs standardized terms to describe the security functionality and assurance of consumers' requirements and manufacturers' products. CC-based Protection Profiles specify what consumers need at both the system and component level in order to fulfill their mission. CC-based Security Targets describe how specific products meet consumers' requirements.

These IA solutions take maximum advantage of commercial components, using NSA developed products and services to fill gaps in areas that are not satisfied by commercial offerings. *Commercial, off-the-shelf* (COTS) products include security products (for example, a firewall) or security-enabled or enhanced *information technology* (IT) products (for example, an e-mail application or secure cellular telephone). Our solutions include technologies and tools that are necessary for a layered defense, in-depth strategy, and tools for defensive information operations such as intrusion detection, automated data reduction, and modeling/simulation tools.

The NSA constantly works with its government and industry partners to facilitate emerging technology, taking the lead in problems not addressed by industry.

The InfoSec Assessment Methodology

Excerpted from NSA INFOSEC Page — INFOSEC Assessment Methodology (IAM); revised February 28, 2001. Information and registration materials can be found at <http://www.nsa.gov/isso/iam/index.htm>.

The National Security Agency, a national leader in Information Assurance, is offering a limited number of *Information Systems Security* (INFOSEC) *Assessment Methodology* (IAM) classes to facilitate the transfer of government-developed technology into the private sector. The IAM course was originally developed by NSA to train United States *Department of Defense* (DoD) organizations to perform their own INFOSEC assessments. NSA has developed specialized knowledge with regard to information systems security assessments through its completion of INFOSEC assessments for its U.S. Government customers over the past 15 years.

Description

The IAM is a two-day course for experienced Information Systems Security analysts who conduct, or are interested in conducting, INFOSEC assessments of U.S. Government information systems. The course teaches NSA's INFOSEC assessment process, a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

Prerequisites

- a. U.S. citizenship
- b. Five years of demonstrated experience in the field of INFOSEC, COMSEC, or computer security, with two of the five years of experience

directly involved in analyzing computer system/network vulnerabilities and security risks.

NSA Certificate of Course Completion: To qualify for an IAM certificate of completion, students must attend all of the two-day class; demonstrate an understanding of the IAM through group exercises and class discussions; and obtain a passing grade (at least 70 percent) on the IAM test.

Short Outline of the IAM Process

In brief, the IAM process is a high-level security assessment not unlike a subset of the Systems Security Engineering Capability Maturity Model (see Appendix D). More specifically, it is a Level I assessment — a non-intrusive, standardized baseline analysis of the InfoSec posture of an automated system. A Level II assessment commonly defines a more hands-on evaluation of the security systems (both Level I and Level II are considered “cooperative”). A Level III evaluation is a “red team” assessment (possibly non-cooperative).

The IAM process will also provide recommendations for the elimination or mitigation of the vulnerability. The IAM is considered a qualitative risk analysis process because it assigns ordinality to the risks that are identified (high/medium/low), rather than a hard cost/benefit ratio to the results.

The IAM is conducted in three phases:

1. *Pre-assessment phase* — The assessment team defines the customer’s needs and begins to identify the system, its boundaries, and the criticality of the information and begins to write the assessment plan. This phase normally takes about two to four weeks.
2. *On-site phase*— Explore and confirm the conclusions made during phase I, gather data and documentation, conduct interviews, and provide an initial analysis. This phase takes about one to two weeks.
3. *Post-assessment phase* — Finalize the analysis and prepare and distribute the report and recommendations. This phase can take anywhere from two to eight weeks.

The heart of the IAM is the creation of the Organizational Criticality Matrix. In this chart, all relevant automated systems are assigned impact attributes (high, medium, or low) based on their estimated effect on Confidentiality, Integrity, and Availability, and criticality to the organization. Other elements can be added to the matrix, such as Non-repudiation or Authentication, but the basic three tenets of InfoSec (that we have been drilling into the reader throughout the book) must remain.

While this type of Level I assessment might be thought to be too high-level, (in other words, not relevant to day-to-day security issues), it is remarkable how many organizations really do not know or do not take the time to determine how critical one system is in relation to another (and more importantly, how critical the system is to the viability of the enterprise). A Level I assessment is fundamental to the design and implementation of a sound organization security architecture.

PDD#63

Excerpts from the National Infrastructure Protection Center’s (NIPC) white paper: “The Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998.”

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances, have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors and that protect both domestic and international security. Because of our military strength, future enemies, whether nations, groups or individuals, might seek to harm us in non-traditional ways, including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure, and information systems might be capable of significantly harming both our military power and our economy.

II. The President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability — and no later than five years from the day the President signed Presidential Decision Directive 63, the United States shall have achieved and shall maintain the capability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of the following:

- The Federal Government to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and to deliver minimum essential public services
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services
- Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.

IV. A Public-Private Partnership to Reduce Vulnerability

Because the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private

sector. To succeed, this partnership must be genuine, mutual, and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector. Together, these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- Assessing the vulnerabilities of the sector to cyber or physical attacks
- Recommending a plan to eliminate significant vulnerabilities
- Proposing a system for identifying and preventing attempted major attacks
- Developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with the Federal Emergency Management Agency (FEMA) as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans with a particular focus on interdependencies.

V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, President Clinton wants those involved to be mindful of the following general principles and concerns:

We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.

The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.

Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.

The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.

The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained.

Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.

The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.

The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors. We must focus on preventative measures as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.

Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

VI. Structure and Organization

The Federal Government shall be organized for the purposes of this endeavor around four components:

Lead Agencies for Sector Liaison

For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. Government department that will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection (and, in particular, in recommending components of the National Infrastructure Assurance Plan). Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.

Lead Agencies for Special Functions

There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, and law enforcement). For each of those special functions, there shall be a Lead Agency that will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.

Interagency Coordination

The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies including the National

Economic Council, will meet to coordinate the implementation of this directive under the auspices of a *Critical Infrastructure Coordination Group* (CICG) chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by and report to the President through the Assistant to the President for National Security Affairs, who shall ensure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum, and the National Security and Telecommunications and Information System Security Committee.

National Infrastructure Assurance Council

On the recommendation of the Lead Agencies, the National Economic Council, and the National Coordinator, the President will appoint a panel of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency *Chief Information Officer* (CIO) shall be responsible for information assurance. Every department and agency shall appoint a *Chief Infrastructure Assurance Officer* (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO might be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.

No later than 180 days from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The *Critical Infrastructure Coordination Group* (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure.

VIII. Tasks

Within 180 days, the Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks:

Vulnerability Analyses

For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment followed by periodic updates. As appropriate,

these assessments shall also include the determination of the minimum essential infrastructure in each sector.

Remedial Plan

Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities, and funding.

Warning

A national center to warn of significant infrastructure attacks will be established immediately. As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.

Response

A system for responding to a significant infrastructure attack while it is underway will be established, with the goal of isolating and minimizing damage.

Reconstitution

For varying levels of successful infrastructure attacks, we shall have a system to rapidly reconstitute minimum required capabilities.

Education and Awareness

There shall be Vulnerability Awareness and Education Programs within both the government and the private sector in order to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.

Research and Development

Federally sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private-sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.

Intelligence

The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include (but not be limited to) the foreign cyber/information warfare threat.

International Cooperation

There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations, and multi-national corporations.

Legislative and Budgetary Requirements

There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the director of the *Office of Management and Budget* (OMB).

IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to the President and to the heads of departments and agencies through the Assistant to the President for National Security Affairs. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan,

and additional policy, legislative, and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition, following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.

Appendix F: The Case for Ethical Hacking

Overview

The purpose of this appendix is to acquaint the security practitioner with the issues involved with the procedure known as “ethical hacking.” The process of testing the network infrastructure by employing external penetration testing has been around for quite a while, but very recently the importance of this procedure has dramatically increased due to the global nature of the Internet and the fact that most corporations do not have a physically isolated network perimeter anymore.

External penetration testing is called many different things, including the following:

- Ethical hacking
- Penetration testing
- Vulnerability assessment (although external penetration testing is really only just a part of a full vulnerability assessment; see the BCP/DRP domain)
- Internet security testing
- Web site testing
- Red teaming

The majority of security professionals agree that external network perimeter testing is a vital part of implementing a fully balanced security process, and it is commonly used to augment the audit and security methodologies we have discussed in the book. What we will describe as follows is the proper way in which *Ethical Hacking* (EH) should be employed in the enterprise.

We will examine three fundamental concepts of EH:

1. *Rationale*. Why EH should be employed and its benefits.
2. *Roles and responsibilities*. How to determine who should perform the testing and the reasons for the choice.
3. *Implementation*. How to maximize the testing quality and minimize the risk by using best practices.

Rationale

Today, organizations face global risks once their computing infrastructures are externally exposed. This situation is most commonly due to e-commerce and the Internet. EH can be a strong weapon in the information security professional’s arsenal to help mitigate that risk. No matter how extensive and layered the security architecture is constructed, the organization does not know the real potential for external intrusion until the perimeter defenses are realistically tested.

To ensure security, systems should be ethically hacked. EH is important because of the risks that organizations face and the similarity of Internet systems to all other systems. Web sites and their underlying systems face an ongoing and increasing risk from external penetration. Security gaps can result from either simple system changes or advances in hacker technology. A successful attack is costly, resource- and time-consuming, and embarrassing to the credibility of the organization.

The only way to know whether the organization’s Web sites, associated services, IP addresses, and underlying systems are secure is to test them. Web sites are similar to all other systems: when they are changed or when they are expected to handle external changes (in other words, advances in hacker technology), they should be tested. This

situation is similar to the tenets of configuration and change control, which require a full testing process prior to and after implementation.

Roles and Responsibilities

Determining who should perform the testing is a critical step in the EH process. Points to consider when making the choice between internal and external hacking teams could include the following:

- *Maximizing cost effectiveness.* Which choice will ensure the lowest cost for the greatest benefit?
- *Assuring thorough testing.* How thorough will the testing need to be in order to guarantee the minimum risk?
- *Avoiding potential risks.* What risk will the production systems incur as a direct result of the testing? Also, what legal or compliance liability will the organization be exposed to during the testing?
- *Assuring full reporting.* How complete and non-partisan will the final report be?

To ensure this cost effectiveness, the efficient use of staff, a lack of corporate bias, and full and complete reporting, the EH should be performed by an independent outside firm that has proven integrity.

Using an external penetration service firm rather than internal corporate resources has quantitative and qualitative advantages:

1. *Greater bang for the buck.* Firms that specialize in EH can afford the ongoing research and development, systems development, and maintenance that is needed to operate state-of-the-art proprietary and open source testing tools and techniques. It is not cost-effective for a single firm, even a firm that has many subsidiaries and Web sites, to fund such an effort.
2. *More effective use of staff.* Internal system security departments have a limited amount of time and a limited budget. By outsourcing Web security testing, a firm's internal system security team increases the time it spends on closing and preventing security gaps (in other words, implementing remediation to the vulnerabilities that are found in the testing report).
3. *Lack of corporate bias.* External ethical hackers are more effective than internal penetration testers because the external penetration service firm is not influenced by any previous system security decisions, knowledge of the current system environment, or future system security plans.
4. *Full reporting.* An employee who is functioning as a penetration tester might be reluctant to fully report security gaps. This person might believe that presenting any bad news would be bad for his career by showing how poor the security was designed or implemented. Or, perhaps he might feel that he has created the vulnerabilities identified, inadvertently through ignorance or incompetence, or that there might be vulnerabilities intentionally created by people known to him (the worst scenario). Conversely, career advancement and professional recognition at external penetration service firms is dependent upon identifying security gaps.

Ex-Hackers or Not?

So you are convinced to begin looking for a firm to begin the EH. Before you start, let's add a cautionary note on selecting the right external firm. The same care and due diligence should take place when evaluating external ethical hackers as would take place when evaluating any other vendor (quality, cost, dependability, references, and

so on). In addition, there are two points that are somewhat unique to ethical hacking that should also be considered: integrity and independence.

Integrity. Ethics matter. Do not use an ethical hacking firm that hires or subcontracts to ex-hackers or others who have criminal records. Some of the largest consulting firms, some of the “big five” auditing firms, and some system security boutiques hire hackers who have criminal records. Your firm might not want to invite them into your systems. Check on your potential vendors’ hiring and subcontracting policies. By using a firm that does not employ ex-hackers, an entire subset of risks can be avoided. Also, many security certification organizations require the signing of ethical statements as a condition of receiving their certification (the CISSP program, for example).

Independence. Use ethical hackers who do not sell auditing, consulting, hardware, software, firewall, hosting, and/or networking services. A firm that conducts EH but that also provides security solutions or remediation has an inherent conflict of interest. It is unlikely that an EH firm will report a security vulnerability if its advice or products do not provide the needed protection or if some of its colleagues were responsible for previously securing the Web site. Full reporting of security gaps is dependent upon avoiding this conflict of interest.

Implementation

The following best practices should be utilized by the ethical hackers:

Test Remotely

By testing remotely, the ethical hacking firm emulates the hackers’ approach more realistically. Also, the firm being tested avoids the security risks associated with having consultants on-site.

Testing remotely also releases the client organization from several responsibilities, including providing the following:

- Advance preparation by the staff
- Allotting staff or resource time to assist during the test
- Configuration changes required to production systems during any phase of the test
- Actual system down time
- Facilities space (as is required for an on-site auditing team)

Test Transparently

Security vulnerabilities (in other words, the ability to cause a denial of service, gain root access to key systems, alter Web pages, and so on) can be and should be identified without doing any alteration (or at worst, real damage) to the organization’s systems. EH should not involve writing to or modifying the target systems or reducing the target’s network response time.

An important component of testing transparently is the need to test for security gaps during network traffic peaks. Certain security gaps (in other words, those associated with the processing of fragmented packets) are more likely to appear during peak traffic, so the ethical hackers need to be able to test during these periods without reducing network response time.

Use the Right Testing Tools, and Use Them Correctly

Ethical hackers should use both open source and proprietary testing tools. There are currently more than 20 excellent open-source testing tools that each have different strengths; using every one has definite benefits.

The ethical hackers should modify and optimize each of the open source tools prior to each use. This optimization should be done at the operating system, configuration, and (if applicable) application level. Each tool's test results will vary depending upon which operating system it is run and how the machine is configured. Application-level modifications should include both adding code (enhancing testing) and disabling code (preventing damage). All of these modifications should take place prior to the ethical hacking attempt.

Open-Source Testing Tools

The following tools (with modification) are excellent for ethical hacking:

- authforce
- cgichk.pl
- cheops
- dnswalk
- ess (the Echo scanner)
- ftpcheck.pl
- fts-rvscan
- hunt
- nessus
- nlog
- nmap
- nperf
- nsat
- rascan
- relaychk.pl
- Saint
- SARA
- sbscan
- scanssh
- snmpscan
- snort
- whisker

Test Each Month, Not Once or Twice a Year

EH performed on an ongoing routine schedule is the only way to know whether new security gaps have appeared in your network. Any change to the computing infrastructure, no matter how insignificant, can create new vulnerabilities. Also, hacker technology continues to advance quickly, and hackers do not try to penetrate systems just once or twice a year. As a countermeasure, EH should be conducted each month.

Test at Varying and Random Times Each Month

Some security vulnerabilities are more likely to appear when network traffic is light (for example, predictable TCP sequence numbers), and some are more likely to appear

when network traffic is heavy (for example, fragmented packet security gaps). In addition, system changes and enhancements occur at different times throughout any given month.

In order to test these varying conditions, EH should be conducted at all different times:

- Weekdays and weekends
- Days and nights
- Holidays and non-holidays

Summary

We have described the three main points of EH:

1. Its position of importance in the implementation of a well-rounded security policy.
2. Why an ethical, external firm should be engaged for the task.
3. Why best practices should be employed during the test to guarantee the greatest cost effectiveness and risk mitigation level.

Whatever you choose to call it, ethical hacking is a cornerstone of the trusted, secure computing infrastructure. When properly executed, ethical hacking can provide the level of security required to conduct business securely and efficiently on the Internet and maintain the three main tenets of information systems security: confidentiality, integrity, and availability.

Written by Ken Brandt with Russell Dean Vines. Ken Brandt (kbrandt@tigertesting.com) is a Managing Director and co-founder of Tiger Testing, a firm that specializes exclusively in ethical hacking.

Appendix G: The Common Criteria

The excerpts below are reproduced without alteration from <http://csrc.nist.gov/cc>. It's important for the reader to note the link between the *Common Criteria* (CC) and its official ISO clone, the *International Standard* (IS) 15408. The CC is becoming a global standard, so the CISSP candidate may be required to know that IS15408 and CC are commonly applied synonymously.

Common Criteria: Launching the International Standard

The Common Criteria (CC) for *Information Technology* (IT) Security Evaluation is the new standard for specifying and evaluating the security features of computer products and systems. The CC is intended to replace previous security criteria used in North America and Europe with a standard that can be used everywhere in the world.

Developing the CC has been a five-year international project involving NIST and the *National Security Agency* (NSA), on behalf of the United States, and security organizations in Canada, France, Germany, the Netherlands, and the United Kingdom. They have worked in close cooperation with the International Standards Organization (ISO).

In the United States, the new international standard CC has formed the basis for the *National Information Assurance Partnership* (NIAP), a joint activity of NIST and NSA to establish an IT product security evaluation program supported by a number of accredited, independent testing laboratories. The main goals of NIAP are to establish cost-effective evaluation of security-capable IT products and to promote the wide availability of tested products to federal agencies and others, thus playing a crucial role in helping to protect the U.S. information infrastructure.

Note A glossary at the end of this appendix defines key terms used throughout the document.

Purpose of CC

The CC will be used as the basis for evaluation of the security properties of IT products and systems. By using such a common criteria base, a wider audience may find the results of an IT security evaluation meaningful. The CC permits comparability among the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and the assurance measures applied to them during a security evaluation.

The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them must meet. The evaluation results may help consumers determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

The CC supports the development of standardized sets of well understood IT product security requirements by user communities in the form of *Protection Profiles* (PPs) for use in procurements and advice to manufacturers. Manufacturers can use similar sets of CC-based requirements to describe the security capabilities of their products. These are called *Security Targets* (STs), which can then be used as the basis for security evaluations of those products. Security evaluations are formalized testing and analytic processes that use the CC to determine whether IT products have been correctly developed to specification and whether they are effective in countering the security problems as claimed. Users can integrate evaluated IT products into their systems with increased confidence that their claimed security features will operate as intended.

Earlier Security Criteria Work

The CC represents the outcome of a long series of efforts to develop criteria for the security evaluation of IT products and systems that can be broadly useful within the international community. In the early 1980s, NSA developed the *Trusted Computer System Evaluation Criteria* (TCSEC or “Orange Book”). NSA has used the TCSEC extensively since then in its IT security product evaluation program.

In the succeeding decade, various countries initiated the development of evaluation criteria that built upon the concepts of the TCSEC but were more flexible and adaptable to the evolving nature of IT.

In Europe, the European Commission published the *Information Technology Security Evaluation Criteria* (ITSEC) in 1991 after joint development by France, Germany, the Netherlands, and the United Kingdom.

In Canada, the *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC) were published in early 1993 as a combination of the ITSEC and TCSEC approaches.

In the United States, NIST and NSA jointly developed the draft *Federal Criteria for Information Technology Security* (FC) version 1.0, which was also published in early 1993 as a second approach to combining North American and European concepts for evaluation criteria.

Work began in 1990 in ISO to develop an international standard evaluation criteria for general use. The new criteria were to be responsive to the need for mutual recognition of standardized security evaluation results in a global IT market. This task was assigned to the *Joint Technical Committee 1 — Information Technology* (JTC1), subcommittee 27 — Security Techniques (SC27), *Working Group 3 — Security Criteria* (WG3).

Development of the Common Criteria

In June 1993, the seven organizations responsible for all the North American and European security criteria (listed at end of bulletin) pooled their efforts to align their separate criteria into a single set of widely useful international IT security criteria. This joint multi-national activity, named the CC Project, sought to resolve the conceptual and technical differences among the source criteria. The results were to be delivered to WG3 as a contribution to the international standard criteria under development.

The CC Project sponsoring organizations formed the *CC Editorial Board* (CCEB) to develop the CC. They established a formal cooperative liaison with WG3 and contributed several early versions of the CC to WG3’s work, which were in turn influenced by WG3 experts’ interaction. Beginning in 1994, WG3 adopted these versions as successive working drafts of the ISO criteria.

Version 1.0 of the CC was completed in January 1996 and distributed by ISO in April 1996 as a *Committee Draft* (CD). The CC Project used this version to perform a number of trial evaluations. A widespread public review of the document was also conducted.

The *CC Implementation Board* (CCIB) extensively revised the CC based on the results of trial use, public review, and interaction with ISO. Working closely with WG3, the CCIB completed CC version 2.0 in April 1998, and it was sent out by ISO for balloting as a Final Committee Draft. In October 1998, WG3 slightly revised the document and approved it as Final Draft International Standard 15408, for final balloting in the winter of 1998. The document is expected to become IS 15408 in early 1999 without further change. For historical and continuity purposes, ISO has accepted the continued use of the term “*Common Criteria*” (CC) within the document, while recognizing that the official ISO name for the new IS 15408 is “*Evaluation Criteria for Information Technology Security*.”

CC Project Sponsoring Organizations

The seven European and North American governmental organizations provided nearly all of the effort that went into developing the CC from its inception to its completion. These organizations are also “evaluation authorities,” managing product security evaluation programs for their respective national governments. They have committed themselves to replacing their respective evaluation criteria with the new IS 15408. Their goal is mutual recognition of each other’s security product evaluation results, permitting a wider global market for good IT security products.

Interim Mutual Recognition

In April 1996, NIST in cooperation with NSA published a bulletin called “Guidance on the Selection of Low Level Assurance Evaluated Products.” The bulletin recommended TCSEC Class C2 - “Controlled Access Protection” as an acceptable minimum set of security criteria for general use in low-threat environments. The bulletin also publicly acknowledged that the Canadian CTCPEC and the European ITSEC contained similar requirements.

The NIST bulletin recognized that, while full equivalency among these three criteria was not easy to establish, enough similarities existed to recommend the use of low-level assurance products evaluated under any of them. The bulletin also noted that equivalency should cease to be an issue once the CC is adopted and implemented by the participating countries.

With the advent of CC version 2.0 and its ISO counterpart, IS 15408, supported by the CC-based Mutual Recognition Arrangement signed by these countries in October 1998 (see end of bulletin), equivalency is no longer an issue.

Three Parts of the CC

Part 1 — Introduction and General Model

Part 1 introduces the CC. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also defines constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. These constructs are called *Protection Profiles* (PPs), *Security Targets* (STs), and packages and are described in a later section. In addition, Part 1 describes the usefulness of each part of the CC in terms of each of the target audiences.

Part 2 — Security Functional Requirements

Part 2 contains a catalog of well-defined and understood security functional requirements that are intended to be used as a standard way of expressing the security requirements for IT products and systems. The catalog is organized into classes, families, and components:

- Classes are high-level groupings of families of requirements, all sharing a common security focus (e.g., identification and authentication).
- Families are lower-level groupings of requirement components all sharing specific security objectives but differing in rigor or emphasis (e.g., user authentication).
- Components are the lowest selectable requirements that may be included in PPs, STs, or packages (e.g., unforgeable user authentication).

Part 2 also includes an extensive annex of application notes for applying the material that it contains. While it is possible to explicitly state functional requirements not included in the Part 2 catalog in building CC-based constructs (PPs, STs, and

packages), that course is not advised unless it is clearly not practical to use Part 2 components. Using functional requirements not part of the catalog could jeopardize widespread acceptance of the result.

Part 3 — Security Assurance Requirements

Part 3 contains a catalog that establishes a set of assurance components that can be used as a standard way of expressing the assurance requirements for IT products and systems. The Part 3 catalog is organized into the same class — family — component structure as Part 2. Part 3 also defines evaluation criteria for PPs and STs. Part 3 presents the seven *Evaluation Assurance Levels* (EALs), which are predefined packages of assurance components that make up the CC scale for rating confidence in the security of IT products and systems.

The EALs have been developed with the goal of preserving the concepts of assurance drawn from the source criteria (TCSEC, ITSEC, and CTCPEC) so that results of previous evaluations remain relevant. For example, EALs levels 2-7 are generally equivalent to the assurance portions of the TCSEC C2-A1 scale. Note, however, that this equivalency should be used with caution as the levels do not derive assurance in the same manner, and exact mappings do not exist.

As with Part 2, it is possible but not necessarily advisable to explicitly state assurance requirements not from Part 3 or to augment EAL packages with additional Part 3 components. Mutual recognition of product evaluation results is based largely on the EAL, so use of unique combinations of assurance requirements could jeopardize international acceptance of products evaluated against them.

Key Concepts

The CC defines three useful constructs for putting IT security requirements from Parts 2 and 3 together: the PP, the ST, and the Package. The CC has been developed around the central notion of using in these constructs, wherever possible, the security requirements in Parts 2 and 3 of the CC, which represent a well-known and understood domain.

Protection Profile

The PP is an implementation-independent statement of security needs for a set of IT security products that could be built. The PP contains a set of security requirements, preferably taken from the catalogs in Parts 2 and 3, which should include an EAL. A PP is intended to be a reusable definition of product security requirements that are known to be useful and effective.

A PP could be developed by user communities, IT product developers, or other parties interested in defining such a common set of requirements. A PP gives consumers a means of referring to a specific set of security needs and communicating them to manufacturers. The PP also helps future product evaluation against those needs.

The PP contains the following items:

- PP introduction — identification and overview information, which allows users to identify PPs useful to them.
- Target of evaluation (TOE) description — description of the IT product and its purpose, not necessarily from a security perspective.
- TOE security environment-description of the security aspects of the environment in which the product is intended to be used and the manner in which it is expected to be employed. This statement includes the following:

- Assumptions about the security aspects of the product's expected usage and operating environment, such as value of assets and limitations of use. Assumptions also describe the environment's physical, personnel, and connectivity aspects.
- Threats against which the product or its supporting environment must specifically provide protection.
- Organizational security policies or rules with which the product must comply. These can be any explicit statements of IT security needs that the product must meet.
- Security objectives — a high-level statement of what the product and its environment are intended to accomplish in covering the threats, policies, and assumptions.
- IT security requirements — the detailed statement of IT security functional and assurance requirements that the product and its operating environment must satisfy to meet the objectives.
- Application notes — additional supporting information that may be useful for the construction, evaluation, or use of the product.
- Rationale — the evidence describing how the PP is complete and cohesive and how a product built against it would be effective in meeting the objectives.

Security Target

An ST is a statement of security claims for a particular IT security product or system. The ST parallels the structure of the PP, though it has additional elements that include product-specific detailed information. The ST contains a set of security requirements for the product or system, which may be made by reference to a PP, directly by reference to CC functional or assurance components, or stated explicitly. An ST is the basis for agreement among all parties as to what security the product or system offers, and therefore the basis for its security evaluation. The ST contains a summary specification, which defines the specific measures taken in the product or system to meet the security requirements.

Package

An intermediate combination of security requirement components is termed a *package*. The package permits the expression of a set of either functional or assurance requirements that meet some particular need, expressed as a set of security objectives. A package is intended to be reusable and to define requirements that are known to be useful and effective in meeting the identified objectives. A package may be used in the construction of more complex packages or PPs and STs. The seven *evaluation assurance levels* (EALs) contained in Part 3 are predefined assurance packages.

Target of Evaluation

The TOE is an IT product or system to be evaluated, the security characteristics of which are described in specific terms by a corresponding ST, or in more general terms by a PP. In CC philosophy, it is important that a product or system be evaluated against the specific set of criteria expressed in the ST. This evaluation consists of rigorous analysis and testing performed by an accredited, independent laboratory. The scope of a TOE evaluation is set by the EAL and other requirements specified in the ST. Part of this process is an evaluation of the ST itself, to ensure that it is correct, complete, and internally consistent and can be used as the baseline for the TOE evaluation.

Uses of the CC

The CC is used in two general ways:

1. As a standardized way to describe security requirements, e.g., PPs and STs for IT products and systems
2. As a sound technical basis for evaluating the security features of these products and systems

The following hypothetical scenarios describe these two uses.

Describing Security Requirements

In a typical PP development scenario, a community of users (e.g., a banking consortium) will determine that a standardized set of security capabilities should be used in software or hardware on their systems. They will begin to construct a PP to express those common requirements. They will first identify the type of product or products envisioned and the general IT features needed. They will then consider the environment in which it will operate — in particular identifying the security problems and challenges that must be addressed. That activity is, in essence, a risk analysis and leads to a statement of general needs or security objectives to be met both by the product and by its environment.

Security objectives are transformed by use of the CC Part 2 catalog into a set of coherent and mutually supportive IT security functional requirements statements. Based on the desired level of confidence in the security of products to be built, an EAL from Part 3 is assigned. (Note that the higher the EAL, the greater the burden on the product developer, and consequently the more time and money needed to bring the product to complete availability.)

The outcome of the process just described is a PP. It is desirable that the PP be submitted to an independent testing laboratory for evaluation, to ensure that it is correct, complete, and internally consistent. The PP may then be entered into a central registry for use by the community to communicate the product security needs to manufacturers, either informally or by incorporation into procurement documents.

The preceding scenario involving a user community is only one possible approach to developing a PP, although it is the most commonly expected approach. It is also possible for one or several manufacturers to develop a PP that incorporates the features of their products, as a means of communication with potential users, ensuring interoperability via standardization or for other purposes.

Evaluating Product Security

In a typical product evaluation scenario, a manufacturer identifies a market niche for an IT product with security capability. This niche may be represented by a PP incorporating the product desires of a group of users and potential customers. The manufacturer builds the product, following the PP-specified functional requirements from CC Part 2 and the developer assurance requirements in the EAL from Part 3. Once the product is built, the manufacturer prepares an ST, which in the simplest case makes a claim of compliance with a particular PP — thereby covering the functional and assurance requirements for the product. The manufacturer also develops as part of the ST a summary specification of the ways that the product's features meet these requirements. The manufacturer then submits the ST, the product, and accompanying documentation to an accredited, independent testing laboratory for evaluation.

The laboratory evaluates the ST, to determine that it is a sound baseline for evaluation of the product and that any claims of PP compliance are supportable. The laboratory then proceeds to evaluate the product and its documentation against the ST. If the product passes evaluation, it can be submitted to an evaluation authority for validation of the evaluation results.

While definitely preferable, it is not necessary for a product to claim compliance with a PP. In the absence of PP claims, the ST is prepared in a process similar to that described for the PP. The evaluation of the ST and then the corresponding product can proceed as before, but no PP compliance claims will be examined.

Validating The Results

An integral part of the CC-based process, as described in its Part 1, is the independent validation of evaluation results in order to ensure that a product's evaluation was conducted properly. An evaluation authority is a body that implements the CC for a specific community, responsible for setting the standards and monitoring the quality of evaluations conducted by testing laboratories within that community. Each of the CC partners is an evaluation authority for the government of its respective country. NIST and NSA work together as a single U.S. authority, as described below. The evaluation authority is responsible for overseeing all evaluations in its jurisdiction, qualitatively reviewing the results, and certifying or validating the findings.

The term "validation" is used in the U.S. for this process, while the other CC partners use "certification," but the process is the same. Upon validation of a successful product evaluation, the product is awarded a CC certificate and is added to an official validated products list available to the public.

Evaluating Installed Systems

Another way that the CC process can be used is to evaluate installed systems for such purposes as system certification and accreditation programs used in several federal agencies. The organization responsible for certifying a system's secure operation could develop an ST describing the system architecture, its functions and operational environment, and the security features it embodies. An independent entity, such as an accredited testing laboratory, could then perform an on-site evaluation of the system against the ST, providing a report to support a request for accreditation.

CC Evaluation Programs

Numerous organizations throughout the world are now implementing the CC, including all of the CC project partners (listed below), as well as other European Union nations, Australia, New Zealand, Japan, Korea, and parts of the former Soviet Union. It is expected that this number will grow significantly as soon as the CC is formally published as International Standard 15408 in early 1999.

In the U.S., NIST and NSA jointly operate the *National Information Assurance Partnership* (NIAP). NIAP is a broadly based program that operates principally as the CC-based evaluation authority for the federal government. NIAP is dedicated to demonstrating the value of independent testing and validation as a measure of security and trust in IT products. Through its efforts, NIAP fosters the establishment and accreditation of commercial IT product security testing laboratories in the U.S.

The Goal of Mutual Recognition

On October 5, 1998, six of the seven CC project partners officially signed a *Mutual Recognition Arrangement* (MRA). The purpose of the MRA is to bring about an

international situation in which IT products and PPs that earn a CC certificate can be procured and used in different jurisdictions without the need for them to be evaluated and certified/validated more than once. By recognizing the results of each other's evaluations, products evaluated in one MRA member nation can be accepted in the other member nations. It is anticipated that, as other nations develop high quality IT product security evaluation programs, they too may seek to join the MRA. This path is open to other evaluation authorities upon demonstration that they can fulfill the stringent technical and procedural conditions for mutual recognition laid down in the MRA.

As product evaluations can be costly and time-consuming, both manufacturers and users have welcomed the MRA breakthrough. The anticipated outcome is a "level playing field" for multi-national IT product manufacturers, leading to a much wider availability of useful IT security products to secure the global information infrastructure.

These two factors have been the major goal of the CC project from its inception and have been the driving force and vision that empowered the ISO criteria activity as well. The joint development of the CC has created an environment of mutual respect among the partners, and the CC itself has formed the technical basis for mutual recognition, both of which were necessary for the inception of the MRA.

Glossary

The following key terms used in this appendix are adapted from CC definitions.

Assurance

grounds for confidence that an IT product or system meets its security objectives.

Evaluation

assessment of an IT product or system against defined security functional and assurance criteria, performed by a combination of testing and analytic techniques.

Evaluation Assurance Level (EAL)

one of seven increasingly rigorous packages of assurance requirements from CC Part 3. Each numbered package represents a point on the CCs predefined assurance scale. An EAL can be considered a level of confidence in the security functions of an IT product or system.

Package

a reusable set of either functional or assurance components (e.g., an EAL), combined together to satisfy a set of identified security objectives.

Product

IT software, firmware and/or hardware, providing functions designed for use or incorporation within a multiplicity of systems.

Protection Profile (PP)

an implementation-independent set of security functional and assurance requirements for a category of IT products that meet specific consumer needs.

Security Functional Requirements

requirements, preferably from CC Part 2, that when taken together specify the security behavior of an IT product or system.

Security Objective

A statement of intent to counter specified threats and/or satisfy specified organizational security policies and assumptions.

Security Target (ST)

a set of security functional and assurance requirements and specifications to be used as the basis for evaluation of an identified product or system.

System

a specific IT installation, with a particular purpose and operational environment.

Target of Evaluation (TOE)

another name for an IT product or system described in a PP or ST. The TOE is the entity that is subject to security evaluation.

For More Information

References:

NIST CSL Bulletin, April 1996

Common Criteria for IT Security v.2.0

ISO FDIS 15408, Parts 1-2-3

Common Criteria Mutual Recognition Arrangement, October 1998

Web sites:

Common Criteria Project: <http://csrc.nist.gov/cc>

NIAP: <http://niap.nist.gov>

CC Project Organizations:

- **CANADA:**

Communications Security Establishment

E-mail: criteria@cse-cst.gc.ca

WWW: www.cse-cst.gc.ca/cse/english/cc.html

- **FRANCE**

Service Central de la Securite, des Systemes d'Information (SCSSI)

E-mail: ssi20@calva.net

- **GERMANY:**

Bundesamt für Sicherheit in der Informationstechnik (BSI)

German Information Security Agency (GISA)

E-mail: cc@bsi.de

WWW: www.bsi.bund.de

- **ETHERLANDS:**

Netherlands National Communications Security Agency

E-mail: criteria@nlncsa.minbuza.nl

WWW: www.tno.nl/instit/fel/refs/cc.html

- **UNITED KINGDOM:**

Communications-Electronics Security Group

E-mail: criteria@cesg.gov.uk

WWW: www.cesg.gov.uk/cchtml

- **UNITED STATES — NIST:**

National Institute of Standards and Technology

E-mail: criteria@nist.gov

WWW: <http://csrc.nist.gov/cc>

- UNITED STATES — NSA:

National Security Agency

E-mail: common_criteria@radium.ncsc.mil

WWW: www.radium.ncsc.mil/tpep/

Appendix H: References for Further Study

This appendix contains a listing of the references we used for the compilation of the book, some additional references that may be useful to you, and the URLs of Web sites that have good information for study or general security information. We used almost all of these publications when researching for this text, and many of them you should read to study for the exam. We have listed them in what we consider to be priority order, from the most relevant to the CISSP candidate, to the least. In some cases, newer editions of the reference books are available.

Books

Handbook of Information Security Management, 1999

Micki Krause and Harold F. Tipton, eds.
CRC Press/Auerbach Publications, 1999

Implementing IPSec

Elizabeth Kaufman and Andrew Newman
John Wiley & Sons, 1999

Computer Security Basics

Deborah Russell and G. T. Gangemi, CISSP
O'Reilly & Associates, 1992

Communication Systems and Networks (Second Edition)

Ray Horak

M&T Books, 2000

Practical Unix & Internet Security

Simson Garfinkel and Gene Spafford
O'Reilly & Associates, 1996

Applied Cryptography (Second Edition)

Bruce Schneier

John Wiley & Sons, 1996

Secrets and Lies: Digital Security in a Networked World

Bruce Schneier

John Wiley & Sons, 2000

Virtual LANs

Marina Smith

McGraw-Hill, 1997

Fighting Computer Crime

Donn B. Parker

John Wiley & Sons, 1998

Information Security Policies Made Easy

Charles C. Wood

Baseline Software, 1999

Cryptography and Network Security (Second Edition)

William Stallings

Prentice Hall Inc., 1999

The NCSA Guide to Enterprise Security

Michel E. Kabay

McGraw-Hill, 1996

Computer Security Handbook, Third Edition

Arthur E. Hutt, Seymour Bosworth, and Douglas B. Hoyt

John Wiley & Sons, 1995

Information Warfare and Security

Dorothy Denning

Addison-Wesley, 1999

Internet Besieged

Dorothy Denning

Addison-Wesley, 1998

Computer Security
Dieter Gollmann
John Wiley & Sons, 1999

Java Security
Scott Oaks
O'Reilly and Associates, 1998

Network Intrusion Detection
Stephen Northcutt
New Riders Publishing, 1999

Defending Your Digital Assets
Randall K. Nichols, Daniel J. Ryan, and Julie J. C. H. Ryan
McGraw-Hill, 1999

Hacker Proof
Lars Klarder
Jamsa Press, 1997

Hacking Exposed
Stuart McClure, Joel Scambray, and George Kurtz
Osborne/McGraw Hill, 1999

Intrusion Detection
Terry Escamilla
John Wiley & Sons, 1998

Designing Network Security
Merike Kaeo
Cisco Press, 1999

Mastering Network Security
Chris Brenton
SYBEX, 1999

Maximum Security (Second edition)
SAMs/Macmillan, 1998

Web Commerce Technology Handbook
Daniel Minoli and Emma Minoli
McGraw-Hill, 1998

Secure Computing: Threats and Safeguards
Rita C. Summers
McGraw-Hill, 1997

Network Security Fundamentals
Peter Norton, Mike Stockman
SAMs/Macmillan, 2000

Virtual Private Networks (Second edition)
Charlie Scott, Paul Wolfe, Mike Erwin, and Andy Oram (editor)
O'Reilly and Associates, 1998

Web Security
Amrit Tiwana
Butterworth-Heinemann, 1999

Web Security and Commerce
Simson Garfinkel and Gene Spafford
O'Reilly and Associates, 1997

Web Security Sourcebook
Aviel D. Rubin, Daniel Geer, Marcus J. Ranum
John Wiley & Sons, 1997

CISSP Examination Textbooks, Volume 1: Theory
SRV Professional Publications, 2000
www.srvbooks.com

The International Handbook of Computer Security
Jae K. Shim, Anique A. Qureshi, Joel G. Siegel
Amacom, 2000

Web Sites

The Web sites are of interest to the CISSP candidate, either directly, as in the case of the (ISC)², or indirectly, as a resource for more info on InfoSec.

InfoSec and Government Information Sites

www.isc2.org (This site is the headquarters of the CISSP program, your main contact for the CISSP certification process.)

www.intiss.com/intisslinks.html (This site has a lot of great links for every domain of InfoSec.)

www.issa-intl.org

csrc.nist.gov/cc

www.nipc.gov

www.icsa.net

www.cerias.purdue.edu/coast/coast.html

www.alw.nih.gov/Security/security.html

www.cse.ucsd.edu/users/bsy/sec.html

www.cerberus-isc.com/resources.html

www.gocsi.com

www.nsa.gov

www.nist.gov

www.nswc.navy.mil/ISSEC/CID

www.cerias.purdue.edu/

www.sans.org/giactc.htm

www.isalliance.org

www.securityportal.com

www.fedcirc.gov

www.cert.org

www.ciac.org/ciac

www.info-sec.com/ciao/63factsheet.html

www.fbi.gov/nipc/welcome.htm

www.asisonline.org

www.bsa.org

www.eff.org

www.fbi.gov/scitech.htm

www.first.org

www.hert.org

www.htcia.org

www.usenix.org

www.ntbugtrak.com

www.nsi.org/compsec.html

www.boran.com/security

xforce.iss.net

www.itpolicy.gsa.gov

www.nswc.navy.mil/ISSEC

www.dda-ltd.co.uk/bs7799.html

Information Security Products, Services, and Training

www.checkpoint.com

www.cisco.com

www.rdvgroup.com

www.altdata.com

www.corbett-tech.com

www.strozassociates.com

www.tigertesting.com
www.misti.com
www.securify.com
www.kroll-ogara.com
www.verisign.com
www.rsasecurity.com
www.securecomputing.com
www.atomictangerine.com
www.infosecnews.com

Hacker Sites

Be careful of these sites, they may bite! Please take precautions before visiting these sites. Also, many of these sites come and go frequently, they may not be there by the time you read this.

rootshell.com/beta/news.html
www.hackers.com
www.l0pht.com
www.thecodex.com
www.defcon.org
www.lordsomer.com
www.2600.com
www.phrack.com
www.cultdeadcow.com
www.hfactorx.org
www.digicrime.com
www.hideaway.net
www.hackernews.com
www.crimeonline.org
www.technotronic.com
www.happyhacker.org
www.webfringe.com/host/

Appendix I: British Standard 7799

British Standard (BS) 7799 provides managers with guidance and a Code of Practice which will enable them to create a secure environment in which to manage their company information.

BS 7799 is supported by an accreditation scheme which enables companies to demonstrate their own level of Information Security Management by open audit and UKAS certification.

BS 7799 requires that company management address ten specific areas:

1. Security policy.
2. Security Organization.
3. Assets, classification and control.
4. Personnel security.
5. Physical and environmental security.
6. Computer and network management.
7. System access control.
8. System development controls.
9. Business continuity planning.
10. Compliance and auditing

List of Figures

Chapter 1: Security Management Practices

Figure 1.1: The C.I.A. triad.

Figure 1.2: Threat versus likelihood matrix.

Figure 1.3: Policy hierarchy.

Chapter 2: Access Control Systems

Figure 2.1: Crossover Error Rate (CER).

Chapter 3: Telecommunications and Network Security

Figure 3.1: The C.I.A. triad.

Figure 3.2: Redundant servers.

Figure 3.3: Server clustering.

Figure 3.4: The OSI seven-layer reference model.

Figure 3.5: The TCP/IP layered model.

Figure 3.6: An application proxy service firewall.

Figure 3.7: A packet-filtering boundary router.

Figure 3.8: A screened-host firewall.

Figure 3.9: A dual-homed firewall.

Figure 3.10: A screened-subnet with a DMZ.

Figure 3.11: Network Address Translation (NAT).

Figure 3.12: Example of a Cisco VPN.

Figure 3.13: Data networking components.

Figure 3.14: Local Area Networks (LANs).

Figure 3.15: Examples of analog and digital signals.

Figure 3.16: Cabling types.

Figure 3.17: A BUS topology.

Figure 3.18: A RING topology.

Figure 3.19: A STAR topology.

Figure 3.20: A TREE topology.

Figure 3.21: A MESH topology.

Figure 3.22: An Ethernet segment.

Figure 3.23: A repeater or hub.

Figure 3.24: A bridged network.

Figure 3.25: A switched network.

Figure 3.26: A routed network.

Figure 3.27: A LAN extender.

Figure 3.28: Shared Internet access with WAN and LAN devices.

Chapter 4: Cryptography

Figure 4.1: Exclusive Or encipherment and decipherment.

Figure 4.2: Encipherment process using Keystream with an XOR operation.

Figure 4.3: Link Encryption.

Figure 4.4: A Spartan Scytale.

Figure 4.5: Caesar C3 substitution cipher.

Figure 4.6: Cipher disks.

Figure 4.7: Jefferson disks. *(Courtesy of the National Cryptologic Museum)*

Figure 4.8: The Hagelin Machine.

Figure 4.9: Herbert Yardley's Black Chamber. *(Courtesy of the National Cryptologic Museum)*

Figure 4.10: Enigma Machine. *(Courtesy of the National Cryptologic Museum)*

Figure 4.11: An Enigma rotor.

Figure 4.12: An illustration of Enigma rotor connections.

Figure 4.13: American SIGABA "Big Machine." *(Courtesy of National Cryptographic Museum)*

Figure 4.14: Polyalphabetic Substitution.

Figure 4.15: A columnar transposition cipher.
Figure 4.16: A Vernam machine.
Figure 4.17: A symmetric (secret) key cryptographic system.
Figure 4.18: Cipher block chaining.
Figure 4.19: DES Cipher Feedback operation.
Figure 4.20: DES Output Feedback operations.
Figure 4.21: A transaction with digital certificates.
Figure 4.22: A Clipper Chip block diagram.
Figure 4.23: A PGP Web of Trust.

Chapter 5: Security Architecture and Models

Figure 5.1: A computer bus.
Figure 5.2: A computer memory hierarchy.
Figure 5.3: A typical machine cycle.
Figure 5.4: Instruction pipelining.
Figure 5.5: Very-Long Instruction Word (VLIW) processing.
Figure 5.6: Protection rings.
Figure 5.7: Example of an access matrix.
Figure 5.8: Take-Grant model illustration.
Figure 5.9: State transitions defined by the function f with an input X .
Figure 5.10: The Bell-LaPadula Simple Security and $*$ properties.
Figure 5.11: The Biba model axioms.
Figure 5.12: An Information Flow Model.

Chapter 7: Applications and Systems Development

Figure 7.1: Simplistic software development model.
Figure 7.2: The Waterfall model.
Figure 7.3: A modified Waterfall model incorporating V&V.
Figure 7.4: The Spiral Model.
Figure 7.5: Security life cycle components.
Figure 7.6: The IDEAL model.
Figure 7.7: A single layer artificial neural network.

Appendix D: A Process Approach to HIPAA Compliance Through a HIPAA-CMM

Figure D.1: The capability and domain dimensions of the SSE-CMM [SSE99].
Figure D.2: HIPAA-CMM structure and use.

List of Tables

Chapter 1: Security Management Practices

- Table 1.1: A Simple Private/Commercial Sector Information Classification Scheme
- Table 1.2: Roles and Responsibilities
- Table 1.3: Risk Analysis Formulas
- Table 1.4: Simple Exposure Rating Level Scale
- Table 1.5: Quantitative vs. Qualitative RA

Chapter 2: Access Control Systems

- Table 2.1: Kerberos Items and Symbols
- Table 2.2: PARTS Relation
- Table 2.3: ELECTRICAL ITEMS Relation

Chapter 3: Telecommunications and Network Security

- Table 3.1: RAID Level Descriptions
- Table 3.2: Tape Format Technology Comparison
- Table 3.3: TNI Evaluation Classes
- Table 3.4: TCP vs. UDP Protocols
- Table 3.5: Analog versus Digital Technologies
- Table 3.6: Circuit Switching versus Packet Switching

Chapter 4: Cryptography

- Table 4.1: Exclusive OR (XOR)
- Table 4.2: Equivalent Strengths of Asymmetric and Symmetric Key Sizes

Chapter 6: Operations Security

- Table 6.1: Covert Channel Classes
- Table 6.2: Trusted Facility Management Classes
- Table 6.3: Configuration Management Classes

Chapter 7: Applications and Systems Development

- Table 7.1: Application Control Types

Chapter 8: Business Continuity Planning and Disaster Recovery Planning

- Table 8.1: BCP Department Involvement
- Table 8.2: Disaster Recovery Plan Testing Types

Chapter 10: Physical Security

- Table 10.1: Electrical Power Definitions
- Table 10.2: Static Charge Damage
- Table 10.3: Fire Classes and Suppression Mediums
- Table 10.4: Heat Damage Temperatures
- Table 10.5: Fencing Height Requirements
- Table 10.6: Dumb, Smart, and Smarter Cards

Appendix D: A Process Approach to HIPAA Compliance Through a HIPAA-CMM

- Table D.1: The IDEAL Model [SSE99]
- Table D.2: The SSE-CMM and Related Efforts [SSE99]
- Table D.3: Administrative Procedures
- Table D.4: Technological Security Safeguards
- Table D.5: Physical Security Measures

- PA 01
- PA 02
- PA 03
- PA 04
- PA 05
- PA 06
- PA 07
- PA 08
- PA 09
- PA 10

PA 11
PA 12
PA 13
PA 14
PA 15
PA 17
PA 21
PA 22
HPA 01
HPA 02
HPA 03
HPA 04
HPA 05

List of Sidebars

Introduction

One-stop, up-to-date preparation

Chapter 1: Security Management Practices

Open View

Senior Management Commitment

Automated Risk Analysis Products

Back Doors

The Need for User Security Training

Chapter 3: Telecommunications and Network Security

Hardware vs. Software RAID

Backup Method Example

Saving Configuration Files and Trivial File Transfer Protocol

TNI Issues

Layered Models

Data Encapsulation

Connection-Oriented versus Connection-less Network Services

Network Address Translation

Asynchronous versus Synchronous Communications

A Word about Network Architectures

Dueling Ethernets

Broadcasts

Virtual Circuits

Chapter 6: Operations Security

The System Administrator's Many Hats

Due Care and the Internet Community

Transparency of Controls

Restricting Hardware Instructions

Media Librarian

Independent Testing

Electronic Audit Trails

Chapter 8: Business Continuity Planning and Disaster Recovery Planning

So What Is the Difference?

The FCPA

The Criticality Survey

The Information Technology Department

Disaster Recovery Plan Software Tools

Plan Viability

When Is a Disaster Over?

Chapter 10: Physical Security

Check Your Carpets!

What Are Those Three Things Again?

Diskette Storage Tips

The Joy of Dumpster Diving

Walk-Through Security List

Appendix F: The Case for Ethical Hacking

Open-Source Testing Tools