Introdução à Criptografia

João Luiz Pereira Marciano

Sumário

Introdução

O uso disseminado de transações financeiras em modo digital tem aumentado enormemente nos últimos tempos. Segundo estimativas, o Brasil movimentou no ano de 2001 o equivalente a US$ 6 Bilhões em transações digitais (*e-business*), enquanto, no mundo esta cifra teria atingido a ordem de US$600 Bilhões. Espera-se que este volume atinja a ordem de US$6 Trilhões no ano de 2005 (deve-se observar que esta estimativa é anterior à nova derrocada dos mercados globais, associada às fraudes observadas em mega-corporações norte-americanas, mas este é um assunto bem diverso). No contexto mundial, o Brasil é o sexto em Internet Banking, a sétima maior indústria de software e o décimo oitavo em e-Gov (transações e atendimento por entidades governamentais aos seus cidadãos), segundo pesquisa de 2001 realizada pela Fundação Getúlio Vargas. Ainda segundo esta pesquisa, 9 milhões de brasileiros têm acesso à Internet (cerca de 20% da população do país), sendo que 15% deste total, ou seja, 1,35 milhão de pessoas, realizam compras online.

De qualquer modo, a necessidade de segurança é premente, e já atinge o usuário comum, embora nem sempre de maneira adequada. Se é verdade que existem sempre pelo menos das formas de se fazer qualquer coisa, uma correta e uma errada, no que diz respeito à segurança as formas erradas são muito mais numerosas que as corretas, e muitas vezes são justamente as primeiras a serem escolhidas. Por mais cruel que possa parecer, é essencial ter em mente que é virtualmente impossível assegurar-se a completa segurança de um sistema computacional, mas sempre é possível demonstrar-se sua fragilidade: basta encontrar uma vulnerabilidade.

Isto não é dito para trazer desânimo aos que lêem estas páginas. Pelo contrário, o constante desafio é o maior motivador dos que se dedicam às atividades de segurança. É preferível ter-se consciência da eventual fragilidade dos sistemas com os quais se trabalha, do que acreditar cegamente na "segurança 100%" apregoada por fabricantes e vendedores de muitos produtos.

Neste sentido, a criptografia se insere como um dos mecanismos de apoio às atividades de segurança. Ao longo das páginas seguintes, alguns conceitos serão apresentados, e tentar-se-á apresentar ao leitor um panorama do status atual dos sistemas criptográficos em uso comercial, além de padrões propostos para utilização futura.

A bibliografia sobre este tema é vasta, e apresentam-se alguns livros, autores e sites que podem enriquecer o conteúdo deste texto – nem de longe passa pela mente do autor dissecar este assunto neste material. O objetivo é, antes de tudo, provocar a curiosidade dos leitores para o fascinante mundo da segurança digital.

Histórico

Para um perfeito entendimento dos assuntos a serem abordados, deve-se introduzir uma conceituação dos principais temas associados à segurança digital. São eles:

a) **Cifragem ou encriptação**: ação de produzir o embaralhamento de um determinado conteúdo, via de regra com o uso de uma chave;
b) **Decifragem ou decriptação**: ação de reverter a cifragem, obtendo o conteúdo original;
c) **Cifra**: algoritmo criptográfico;
d) **Criptologia** (do grego kriptós = escondido, oculto; lógos = estudo, ciência): é a ciência que se ocupa do estudo dos processos e técnicas de escrita em código, e sua correspondente inversão;
e) **Criptografia** (kriptós; graphein = escrita): ocupa-se dos procedimentos de escrita em código, através de cifragem;
f) **Criptoanálise** (kriptós; análysis = decomposição, exame, estudo pormenorizado): estudo da obtenção do conteúdo decifrado, a partir do cifrado, sem o uso da chave, o estudo de obtenção da chave. Uma tentativa de criptoanálise é chamada ataque.

A criptografia, ao contrário do que muitos pensam, não é recente. Pelo contrário, há registros de sua utilização ainda na Roma antiga, à época de Júlio César, com o uso de substituição de letras na mensagem transmitida (este método será melhor discutido adiante). Posteriormente, ao longo da história, vários outros exemplos formam observados, notadamente na Primeira Guerra e na Segunda Guerra mundiais, aqui já com o uso de máquinas de cifragem (rotores). O uso de criptografia por software teve uma explosão no período da Guerra Fria, que opôs as duas potências (União Soviética e Estados Unidos). Como pode-se observar, o uso da criptografia esteve sempre muito associado a aplicações militares, até a ampla disseminação dos serviços em redes digitais, a partir da década de setenta do século XX.

Formas básicas de criptografia

Criptografia de chave simétrica

De maneira geral, dados que podem ser lidos sem o uso de quaisquer medidas de segurança são chamados "texto pleno". O resultado da encriptação de texto pleno gera o chamado texto cifrado, ou encriptado. Por sua vez, o processo reverso, a decriptação, é o processo pelo qual a partir do texto cifrado obtém-se de volta o texto pleno. Esquematicamente, tem-se:

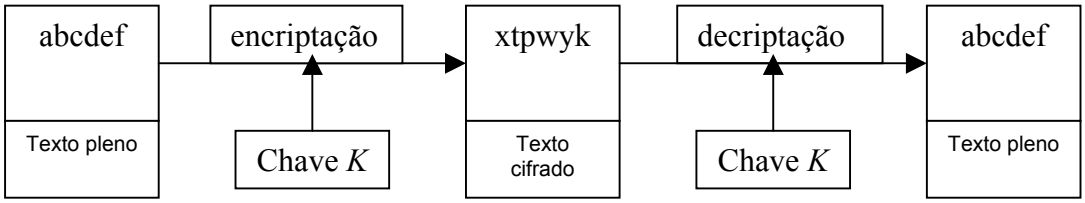

Figura 1 – criptografia de chave simétrica

Na criptografia convencional, também chamada criptografia de chave secreta ou de chave simétrica, uma mesma chave é utilizada tanto no processo de encriptação quanto no processo de decriptação. Um exemplo amplamente difundido desta modalidade é o algoritmo DES *(Data Encription Standard*) e suas variações, bastante utilizado pelo governo norte-americano e outros setores públicos ou privados ao redor do globo.

A criptografia de chaves simétricas apresenta diversas vantagens, entre as quais a velocidade de geração e processamento das chaves. Entretanto, ela apresenta a desvantagem de não se adequar a modelos onde é necessária a distribuição de chaves. Considere-se o exemplo de uma aplicação na qual deve-se distribuir chaves para um número elevado de participantes. Definindo-se um par de chaves entre cada dupla de interlocutores, tem-se que o número de chaves N, para n participantes, é de

$$N = \frac{n*(n-1)}{2}$$

Num caso onde houvesse a necessidade de 1000 interlocutores realizarem o intercâmbio de dados encriptados, vê-se que a quantidade de chaves atingiria a ordem de meio milhão de itens a serem gerados, gerenciados e distribuídos. Assim, o problema da distribuição de chaves mostra-se extremamente importante.

Criptografia de chave pública

Os problemas da distribuição de chaves são resolvidos pela criptografia de chaves públicas, que é um esquema assimétrico que usa um par de chaves para o tratamento dos dados: uma chave para a encriptação, e uma outra chave para a decriptação. A chave, dita pública, é difundida para o mundo, real ou virtual, enquanto a chave privada é mantida sob absoluto sigilo. Deste modo, qualquer pessoa que tenha conhecimento de uma determinada chave pública pode enviar dados para o detentor da respectiva chave privada, com a garantia de que somente este detentor poderá ler os dados enviados: dados encriptados com uma das chaves só podem ser decriptados com a chave correspondente do mesmo par.

Para garantir o sigilo, deve ser computacionalmente impossível, ou ao menos extremamente improvável, a obtenção da chave privada a partir da chave pública. Assim, a formulação e a utilização de algoritmos robustos torna-se imperativa.

Esquematicamente:

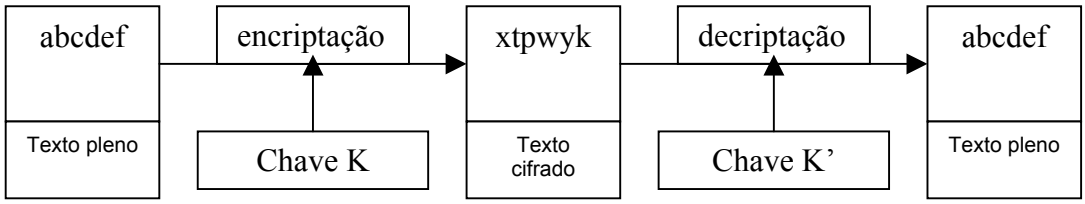

Figura 2 – Criptografia de chave pública

Uma preocupação constante no uso de sistemas criptográficos de chaves públicas é que as chaves privadas sejam do conhecimento apenas do seu proprietário. Num ambiente de redes e servidores públicos, ataques do *tipo "man-in-the-middle*" são uma ameaça potencial. Neste tipo de ataque, o atacante pode tentar introduzir uma chave copiada com o nome e identificação do usuário pelo qual pretende se passar. Assim, os dados cifrados enviados ao usuário legítimo também serão vistos pelo atacante.

Nota-se, então, a necessidade de garantir-se que a chave pública com a qual se cifra dados é de fato a chave pública do legítimo destinatário, e não uma fraude. No caso de pessoas próximas, pode-se fazer a entrega de chaves pessoalmente. Mas o que se pode fazer em ambientes de redes amplas, ou quando é necessário tratar com pessoas e entidades as quais nunca se viu antes, como no caso do comércio eletrônico?

Para simplificar esta tarefa, os certificados digitais estabelecem que uma determinada chave pública pertence de fato a uma pessoa, equipamento ou serviço, ou instituição.

Um certificado é uma forma de credencial. Analogias no mundo real são a carteira de motorista, a carteira de identidade e o passaporte. Cada um destes documentos tem alguma informação identificando seu portador, e alguma garantia de que alguém mais confirmou esta identificação. Nos exemplos citados, esta garantia é de tal teor que uma outra pessoa poderia personificar o real detentor de um destes documentos, estando de posse dele.

Um certificado digital é um conjunto de dados que funciona de forma semelhante a um certificado do mundo físico. Ele envolve informações incluídas junto à chave pública, que ajudam a outros a verificarem que a chave ali contida é genuína ou válida. Deste modo, os certificados digitais são usados para demover tentativas de substituir-se uma chave pública por outra.

Resumidamente, um certificado digital compõe-se de três partes:

- Uma chave pública;
- Informações de certificação (como nome, ID de usuário, etc.);
- Uma ou mais assinaturas digitais.

O propósito da assinatura digital num certificado é o de assegurar que a informação contida no certificado foi atestada por alguma outra pessoa ou entidade.

Mais adiante, um capítulo deste texto será totalmente dedicado à certificação digital.

Serviços providos pela criptografia

Quais os objetivos pretendidos ao se implementar criptografia? Em que medida estes objetivos são de fato alcançados? A criptografia é de fato eficiente?

A fim de se obter respostas objetivas a estas questões, fundamentais no processo de segurança da informação, deve-se conhecer alguns requisitos básicos que a criptografia é capaz de proporcionar, bem como deve-se conhecer as facilidades que ela não é capaz de introduzir.

Basicamente, a criptografia introduz as seguintes facilidades:

- **Confidencialidade**: garantia de sigilo, atesta que o conteúdo criptografado somente será lido por quem de direito;
- **Autenticação**: deve ser possível ao destinatário de uma mensagem garantir que o seu emissor é de fato quem diz ser;
- **Integridade**: deve ser possível ao destinatário de uma mensagem garantir que ela não foi modificada em trânsito; um intruso não deve ser capaz de substituir uma mensagem legítima por uma falsa;
- **Não repúdio, ou irretratabilidade**: o emissor de uma mensagem não pode ser capaz de negar que a enviou (esta forma, por vezes, é chamada de não repúdio do emissor; fala-se também o não repúdio do receptor).

Estes são requisitos vitais para a interação no mundo digital, que encontram contrapartida no mundo analógico. Infelizmente, a passagem de um mundo para outro nem sempre é simples.

Criptoanálise

Como já se viu, a criptoanálise ocupa-se da tentativa de obtenção do texto pleno de uma mensagem sem acesso à chave. Uma criptoanálise bem sucedida pode recuperar o texto pleno ou a chave, ou ambos. Pode, ainda, detectar eventual fragilidade que possa levar àqueles resultados. A perda da chave através de métodos não-criptoanalíticos é chamada comprometimento.

Uma asserção fundamental em criptoanálise, enunciada por Kerckhoffs no século XIX, é que o segredo deve residir inteiramente na chave. Outra asserção é de que o atacante possui detalhes do algoritmo criptográfico e de sua implementação (naturalmente, pode-se desenvolver algoritmos próprios, mas é sensato admitir que o atacante sempre pode obter aqueles detalhes através da análise).

Existem basicamente quatro tipos de ataques criptoanalíticos, vistos a seguir.

Ataque de texto cifrado

O criptoanalista possui o texto cifrado de várias mensagens, todas cifradas com o mesmo algoritmo. O seu trabalho é recuperar o texto pleno de tantas mensagens quanto possível, ou, o que seria melhor ainda, deduzir a chave (ou chaves) usada para encriptar aquelas mensagens, a fim de decriptar outras mensagens cifradas com a mesma chave. Esquematicamente:

Sejam C = texto cifrado; E_k = encriptação com a chave k; P = texto pleno.

Dado: $C_1 = E_k(P_1)$, $C_2 = E_k(P_2)$, ..., $C_i=E_k(P_i)$
Deduza: Ou P_1, P_2, ..., P_i, ou k, ou um algoritmo para inferir P_{i+1} a partir de $C_{i+1}=E_k(P_{i+1})$.

Ataque de texto pleno conhecido

O criptoanalista possui não somente o texto cifrado de várias mensagens, mas também ao texto pleno das mensagens correspondentes. Seu trabalho é deduzir a chave usada para encriptação ou um algoritmo para decriptar quaisquer novas mensagem criptografadas com a mesma chave.

Dado: P_1, $C_1 = E_k(P_1)$, P_2, $C_2 = E_k(P_2)$, ..., P_i, $C_i=E_k(P_i)$
Deduza: Ou k, ou um algoritmo para inferir P_{i+1} a partir de $C_{i+1}=E_k(P_{i+1})$.

Ataque de texto pleno escolhido

O criptoanalista não só tem acesso ao texto pleno e cifrado de várias mensagens, como ainda pode escolher o texto pleno a ser cifrado. Seu trabalho é deduzir a chave, ou um algoritmo para decriptar quaisquer novas mensagens encriptadas com a mesma chave.

Dado: P_1, $C_1 = E_k(P_1)$, P_2, $C_2 = E_k(P_2)$, ..., P_i, $C_i = E_k(P_i)$, onde o criptoanalista pode escolher P_1, P_2, ... , P_i
Deduza: Ou k, ou um algoritmo para inferir P_{i+1} a partir de $C_{i+1}=E_k(_{Pi+1})$.

Ataque adaptativo de texto pleno escolhido

Este é um caso especial do ataque de texto pleno escolhido. O criptoanalista não só pode escolher o texto pleno a ser cifrado, mas pode ainda modificar sua escolha baseado nos resultados da encriptação anterior. Num ataque de texto pleno escolhido, ele pode estar limitado à escolha de um único bloco de texto pleno a ser cifrado. Num ataque adaptativo de texto pleno escolhido, ele pode escolher um bloco de texto pleno a partir do anterior, e assim por diante.

Outras formas de ataque

Naturalmente, as formas de ataque não estão limitadas à modalidades digitais. A engenharia social, por exemplo, tem contribuído enormemente para o comprometimento de sistemas completos de segurança.

Fraude, chantagem, ameaças, furto, roubo e muitos outros, também são formas de se obter, indiretamente, acesso a segredos computacionais. Como se vê, o quesito digital é apenas uma das facetas da segurança, como um todo.

Segurança de algoritmos

Diferentes algoritmos possuem diferentes graus de segurança. Isto varia conforme o grau de dificuldade em quebrá-los. Se o custo requerido para quebrar um algoritmo é maior que o valor dos dados encriptados por ele, provavelmente ele estará seguro. Se o tempo requerido para quebrar um algoritmo é maior que o tempo durante o qual os dados encriptados devem permanecer em segredo, provavelmente ele estará seguro. O mesmo pode-se dizer no caso da quantidade de informação necessária para quebrar o algoritmo, em contrapartida aos dados encriptados por ele.

Diz-se "provavelmente" porque sempre há uma chance de novos progressos na criptoanálise. Por outro lado, o valor da maior parte das informações decresce ao longo do tempo. É importante que o valor dos dados permaneça inferior ao custo da quebra da segurança que os protege.

Lars Knudsen classificou as seguintes categorias de quebra de um algoritmo, em ordem decrescente de severidade:

- **Quebra total**: um criptoanalista obtém a chave k, de tal forma que $D_k(C) = P$.
- **Dedução global**: um criptoanalista encontra um determinado algoritmo, A, equivalente a $D_k(C)$, sem conhecer k.
- **Dedução local**: um criptoanalista encontra o texto pleno de um texto cifrado interceptado.
- **Dedução de informação**: um criptoanalista obtém alguma informação sobre a chave ou sobre o texto pleno. Esta informação pode ser resumir a alguns bits da chave, alguma informação sobre a forma do texto pleno, e assim por diante.

Um algoritmo é dito **incondicionalmente seguro** se, não importando quanto texto cifrado que um criptoanalista possua, não há jamais informação suficiente para recuperar o texto pleno. Com efeito, somente o método conhecido como "one-time pad" é incondicionalmente seguro, dados recursos infinitos ao criptoanalista. Todos os outros criptosistemas são

vulneráveis a um ataque de texto cifrado, pela tentativa de gerar-se uma a uma as possíveis chaves, e analisando-se se o texto pleno gerado faz sentido. Isto é chamado **ataque por força bruta**.

A criptografia está naturalmente relacionada a criptosistemas que não se possa quebrar. Um algoritmo é chamado **computacionalmente seguro** (ou **forte**) se ele não puder ser quebrado com recursos disponíveis, presentes ou futuros. O que se entende por "recursos disponíveis" está aberto à interpretação...

A complexidade de um ataque pode ser medida de diferentes formas:

a) **Complexidade de dados**: a quantidade de dados necessária como entrada para a quebra;
b) **Complexidade de processamento**: o tempo necessário para realizar o ataque;
c) **Requisitos de armazenamento**: o montante de memória necessário para o ataque.

Via de regra, a complexidade de um ataque é tomada como sendo o menor dentre estes três fatores. Alguns ataques envolvem um equilíbrio entre as três complexidades: um ataque mais rápido pode ser possível às expensas de um requisito maior de armazenamento.

A complexidade é expressa em ordens de magnitude. Assim, por exemplo, se um algoritmo tem complexidade de processamento de 2^{128}, então 2^{128} operações serão requeridas para quebrá-lo. Neste caso, possuindo-se capacidade computacional para executar um milhão de operações por segundo em cada processador e com o uso de um milhão de processadores, levar-se-á um tempo de aproximadamente 10^{19} anos para a determinação da chave. Isto é, um bilhão de vezes a idade do universo.

Enquanto a complexidade de um ataque é constante (até que os criptoanalistas encontrem um ataque melhor, é claro), a capacidade computacional é constante aumentada. Nem é preciso lembrar a lei de Moore[1]. Alguns ataques são perfeitos para a utilização de máquinas paralelas. Afirmar que um algoritmo é seguro apenas porque ele não pode ser quebrado com os recursos atuais é, no mínimo, arriscado. Bons criptosistemas são projetados tendo em vista o poder computacional previsto em anos no futuro.

Cifras de substituição e de transposição

Antes do surgimento dos computadores, a criptografia consistia na aplicação de algoritmos baseados em caracteres. Diferentes algoritmos substituíam caracteres, ou transpunham caracteres a fim de gerar o texto cifrado, muitas vezes as duas coisas.

Cifras de substituição

Uma cifra de substituição é aquela na qual cada caracter no texto pleno é substituído por outro caracter no texto cifrado. O destinatário da mensagem inverte a substituição no texto cifrado para recuperar o texto pleno.

[1] Gordon Moore, um dos fundadores da Intel, afirmou certa vez que a capacidade dos processadores dobra, em média, a cada dezoito meses. Embora haja limites físicos para a integração de componentes, novas tecnologias estão sendo pesquisadas a fim de proporcionar poder computacional cada vez maior.

Na criptografia clássica, há quatro tipos de cifras de substituição:

a) **Cifra monoalfabética** ou de substituição simples, na qual cada caracter no texto pleno é substituído por um caracter correspondente no texto cifrado; é usada em jogos recreativos e passatempos de jornais;
b) **Cifra de substituição homofônica**: análoga à anterior, exceto pelo fato de que um único caracter no texto pleno pode ser mapeado para vários caracteres no texto cifrado. Por exemplo, "A" pode corresponder a 5, 13, 25 ou 56, e "B" pode corresponder a 7, 19, 31, ou 42, etc.;
c) **Cifra de substituição poligrâmica**: blocos de caracteres são cifrados em grupos. Por exemplo, "ABA" pode corresponder a "RTQ", "ABB" a "SLL", etc.;
d) **Cifra de substituição polialfabética**: feita de múltiplas substituições simples. Por exemplo, pode haver cinco substituições simples usadas; a utilizada varia conforme a posição do caracter no texto pleno.

A famosa cifra de César é uma substituição simples (cada caracter é substituído pelo que está, por exemplo, três posições depois, módulo 26 ("A" por "D", "B" por "E", ..., "W" por "Z", "X" por "A", "Z" por "C").

ROT13 é uma cifra de substituição usada em sistemas UNIX. Nesta cifra, "A" é substituído por "N", "B" por "O", e assim por diante: cada letra sofre uma rotação de treze posições.

Encriptando-se um arquivo duas vezes com ROT13 produz o arquivo original. ROT13 não é usado para segurança, mas para omitir texto ofensivo, soluções de quebra-cabeças, etc.

Cifras de substituição simples não omitem a freqüência original dos caracteres no texto, podendo ser facilmente quebradas.

Cifras de substituição homofônica foram usadas por volta do ano 1401 pelo Duque de Mântua. São mais complicadas de quebrar que as simples, mas, como também não omitem detalhes estatísticos, um programa de computador requer alguns segundos para ter sucesso.

Cifras de substituição poligrâmica, nas quais grupos de letras são cifradas juntas, foram usadas pelo exército inglês na Primeira Guerra mundial.

Cifras de substituição polialfabética foram criadas por Leon Battista em 1568. A cifra de Vigenére, publicada pela primeira vez em 1586 é um outro exemplo. Embora quebradas por programas computacionais sem muita complexidade, vários produtos ainda usam cifras desta forma. Estas cifras possuem múltiplas chaves de uma letra, cada uma das quais é usada para encriptar uma letra do texto pleno. A primeira chave encripta a primeira letra, a segunda chave encripta a segunda letra, e assim por diante. Se houver vinte chaves de uma letra, então cada vigésima letra será encriptada com a mesma chave. Este número é chamado **período** da chave.

Cifras de transposição

Numa cifra de transposição, o texto pleno continua o mesmo, mas a ordem dos caracteres é modificada. Numa **cifra de transposição simples colunar**, o texto pleno é escrito horizontalmente numa área de largura fixa, e o texto cifrado é lido verticalmente. A decriptação

consiste em escrever o texto cifrado verticalmente numa área de largura igual, e ler o texto horizontalmente. Veja a figura 3:

Texto pleno: O RATO ROEU A ROUPA DO REI DE ROMA

O	R	A	T	O
R	O	E	U	A
R	O	U	P	A
D	O	R	E	I
D	E	R	O	M
A				

Texto cifrado: ORRDDAROOOEAEURRTUPEOOAAIM

Figura 3 – exemplo de cifra de transposição simples colunar

Mais uma vez, como as letras do texto cifrado são as mesmas do texto pleno, o conhecimento estatístico das letras do alfabeto dá uma ótima pista sobre a transposição usada. Existem outras ainda mais complexas, mas a maioria é computacionalmente quebrável.

One-time pad

Existe uma esquema criptográfico de segurança comprovada: ***one-time pad***, criada em 1917 pelo Major Joseph Mauborgne e pelo pesquisador da AT&T Gilbert Vernam. Uma cifra one-time pad consiste num grande conjunto de chaves de letras não repetidas, geradas randomicamente, ajuntadas como num bloco de papel (*pad*, em inglês). Em sua forma original, era uma fita de papel usada por operadores de teletipo. O emissor usa cada letra da chave para encriptar exatamente um caracter do texto pleno. A encriptação é a adição módulo 26 do caracter do texto pleno com o caracter da chave.

Cada letra da chave é usada apenas uma vez, para somente uma mensagem. O emissor encripta a mensagem e então destrói as páginas usadas do bloco ou a seção usada da fita do teletipo. O receptor tem um bloco igual e usa cada chave por vez para decriptar cada letra do texto cifrado, após o que destrói o bloco ou a seção da fita usada. A cada nova mensagem, gera-se uma nova seqüência de chaves. Por exemplo, se a mensagem for:

ONETIMEPAD

e a seqüência de chaves gerada for

TBFRGFARFM

então o texto cifrado é

IPKLPSFHGQ

por que

O + T mod 26 = I
N + B mod 26 = P
E + F mod 26 = K, etc.

Assumindo-se que um atacante não tenha acesso à one-time pad usada para encriptar a mensagem, este esquema é perfeitamente seguro. Um texto cifrado dado pode corresponder a qualquer texto pleno de igual tamanho.

Uma vez que cada seqüência da chave é da mesma probabilidade (pela geração randômica), um atacante não tem informação com a qual possa criptoanalisar o texto cifrado. A seqüência da chave poderia ser

POYYAEAAZX

que resultaria no texto pleno

SALMONEGGS

Ou poderia ser

BXFGBMTMXM

que produziria o texto pleno

GREENFLUID

O fundamental, aqui, é que a seqüência de letras da chave dever ser gerada randomicamente. Qualquer ataque contra este sistema será feito contra o método de geração as letras da chave. A geração realmente randômica de valores computacionais é muito mais complexa que o que pode parecer à primeira vista. Outro detalhe importante é que a mesma chave jamais pode ser usada mais de uma vez. Computacionalmente, usa-se o método de XOR para cifragem e decifragem.

Há outros problemas: como os bits da chave devem ser randômicos e jamais usados duas vezes, a chave deve ser do tamanho do texto pleno. Além disso, deve-se possuir duas cópias da chave, uma no emissor e outra no receptor. Isto complica ainda mais a questão do tráfego e destruição das chaves já utilizadas. Além disso, one-time pad não provê autenticidade.

O uso de one-time pad no mundo atual está praticamente restrito a canais super-seguros de baixa largura de banda, mas pesquisa-se sua utilização numa gama maior de aplicações.

Protocolos criptográficos

Um **protocolo** é uma série de passos que envolvem dois ou mais participantes, e que tem como objetivo desempenhar uma tarefa determinada. Por uma "série de passos", depreende-se que o protocolo possui uma seqüência, do princípio ao fim, sendo que cada passo deve ser dado em sua vez. "Envolvendo dois ou mais participantes" implica que a colaboração é fundamental para a execução do protocolo, e , por fim, a tarefa a ser executada é conhecida e bem definida para todos os participantes.

Embora pareça evidente, vale a pena explicitar as características básicas de um protocolo:

- Todos os participantes no protocolo devem conhecê-lo e seus passos previamente;
- Todos os participantes devem concordar em segui-lo;
- O protocolo deve ser inequívoco, ou seja, livre de ambigüidades;
- O protocolo deve ser completo: deve haver uma ação específica para cada situação possível.

Um **protocolo criptográfico** é um protocolo que faz uso de criptografia para a sua execução, e, via de regra, isto mais que apenas sigilo. Os participantes podem desejar compartilhar segredo para o cálculo de um valor, gerar em conjunto um valor randômico, convencer-se mutuamente sobre suas identidades, ou assinar um contrato de forma simultânea. Em todos estes casos, deseja-se prevenir ou detectar trapaças ou a tentativa de intrusões. Uma regra essencial aos protocolos criptográficos é a seguinte:

"Não deve ser possível fazer ou aprender nada além do que está especificado no protocolo" [SCH 96].

Como se verá, isto é muito mais fácil de dizer do que de implementar.

Protocolos arbitrados

Um árbitro é uma terceira parte desinteressada, confiável, utilizada a fim de se completar um protocolo. Isto significa que esta terceira parte é totalmente isenta quanto aos participantes do protocolo, e que todas aquelas partes confiam e aceitam o seu julgamento. Como se vê, árbitros são fundamentais a fim de se completar protocolos entre partes que não possuem confiança mútua.

Exemplos do mundo real seriam bancos, tabeliães, etc.

No mundo virtual, há alguns problemas:

- É mais fácil confiar numa parte neutra quando se pode vê-la;
- O árbitro é um gargalo na implementação de protocolos de larga escala, uma vez que ele deve interferir em todas as transações. O aumento do número de árbitros pode acelerar esta mediação, mas aumentará o custo envolvido;
- Uma vez que todos na rede devem confiar no árbitro, ele representa um ponto vulnerável a quem desejar subverter esta confiança.

Protocolos adjudicados

Diferentemente do protocolo arbitrado, onde em cada passo a ação do árbitro é essencial, no protocolo adjudicado a ação do mediador é requerida apenas em caso de disputa. Sua intervenção visa a determinar se o protocolo foi executado de forma leal.

No mundo real, juízes são adjudicadores profissionais. As partes A e B podem iniciar uma ação, por exemplo, um contrato, sem a intervenção de um juiz, que não verá o contrato até que uma das partes, ou ambas, faça uma argüição ao adjudicador.

Assim, o protocolo pode executar da seguinte forma:

Parte não adjudicada:

1. A e B negociam os termos do contrato;
2. A assina o contrato;
3. B assina o contrato.

Parte adjudicada (em caso de disputa):

4. A e B se apresentam ao juiz;
5. A apresenta a sua evidência;
6. B apresenta a sua evidência;
7. O juiz decide em face das evidências.

Protocolos auto-reforçados

Esta é a melhor forma de protocolo. Nenhum árbitro ou adjudicador é necessário: o próprio protocolo se encarrega de garantir o correto comportamento dos participantes. Se uma das partes tenta trapacear, automaticamente a outra detecta esta tentativa e o protocolo se interrompe.

Ataques contra protocolos

Ataques contra protocolos podem ser passivos ou ativos.

Num ataque **passivo**, um indivíduo externo à execução do protocolo pode tentar obter informação, de parte ou todo o protocolo, a fim se beneficiar. Um exemplo disto é o ataque de texto cifrado, visto anteriormente. Estes ataques podem ser bem dificeis de se detectar.

De outra forma, um atacante pode tentar subverter o protocolo a seu favor. Ele pode tentar se passar por outra pessoa, introduzir novas mensagens no protocolo, remover mensagens existentes, alterar conteúdo de mensagens existentes, repetir mensagens anteriores, etc. Estes são ataques **ativos**. A forma destes ataques pode variar conforme várias condições, mas observe que o atacante é um dos participantes do protocolo.

Comunicação com o uso de criptografia simétrica

Como duas entidades se comunicam de forma segura, numa rede aberta e considerada um ambiente hostil? Encriptando sua comunicação, decerto.

Vejamos o que deve acontecer para que A possa enviar uma mensagem para B, de forma segura:

1. A e B entram em acordo quanto ao criptosistema a ser usado;
2. A e B combinam a chave a ser usada;
3. A toma sua mensagem em texto pleno, e a encripta usando o algoritmo e a chave combinados, criando um texto cifrado;
4. A envia o texto cifrado para B;
5. B decripta o texto cifrado com o mesmo algoritmo e chave e o lê.

O que um atacante poderia fazer, estando entre A e B? De posse da mensagem transmitida no passo 4, poderia realizar criptoanálise sobre ele – um ataque de texto cifrado, conforme já foi visto. Há algoritmos com robustez suficiente para dar a este atacante trabalho por bilhões de anos.

Se ele for esperto, pode ter aceso também aos passos 1 e 2. Assim, pode decriptar a mensagem obtida no passo 4 tanto quanto B.

Um bom algoritmo é aquele em que toda a segurança é inerente ao conhecimento da chave, e nenhuma segurança é inerente ao conhecimento do algoritmo [SCH 96]. Eis porque a gerência de chaves é tão importante em criptografia. Com um algoritmo simétrico, A e B podem realizar o passo 1 em público, mas devem realizar o passo 2 e forma totalmente secreta. As chaves devem permanecer em segredo antes, durante e depois do protocolo – tanto quanto a mensagem deva permanecer em segredo. A criptografia de chaves públicas trata este roblema de outra forma, como se verá adiante.

Um atacante ativo pode tentar ainda outras coisas. Ele pode tentar interromper a comunicação no passo 4, de forma tal a impedir que A e B se comuniquem. Pode ainda interceptar as mensagens de A e substituí-las pelas suas. Se ele conhecer a chave, pode inserir suas mensagens como se fossem as de A.

Além disso, os próprios participantes A e B podem disseminar a chave ou mesmo a mensagem em texto pleno. Naturalmente, a confiança entre os participantes é fundamental num protocolo.

Resumidamente, sistemas simétricos têm os seguintes problemas:

- As chaves devem ser distribuídas em sigilo. O seu valor corresponde ao valor das mensagens cifradas com elas, já que o conhecimento da chave leva ao conhecimento das mensagens. Numa rede aberta, esta tarefa de distribuição é extremamente dificultada;
- Se uma chave é comprometida (roubada, deduzida, extorquida, revelada, etc.), o atacante pode decriptar todo o tráfego trocado com aquela chave. Pode ainda se fazer passar por uma das partes e produzir falsas mensagens para enganar a outra parte;

- Como já foi dito antes, assumindo-se que cada par de participantes possui uma chave, p número de chaves cresce rapidamente. *n* usuários requerem *n(n-1)/2* chaves.

Funções One-way

Uma função one-way é uma função de cálculo computacional fácil, mas de inversão extremamente difícil. Dito de outra forma, dado *x* é fácil calcular *f(x)*, mas dado *f(x)* deve ser computacionalmente inviável realizar o cálculo de *x*.

Sua aplicação é largamente utilizada em criptografia, mas com um acréscimo: uma chave. Com o uso da chave, torna-se fácil realizar a reversão da função one-way.

Funções de hash one-way

Uma função de hash one-way posui vários nomes, no contexto da criptografia: ela ser chamada de função de compressão, função de contração, sinopse da mensagem (*message digest*), checksum criptográfico, etc. Não importa a nomenclatura usada, funções de hash one-way são essenciais na construção da criptografia moderna.

As funções de hash são conhecidas dos projetistas de algoritmos há muito tempo. Entre outras propriedades, elas tomam um string de entrada de tamanho variável (chamado pré-imagem), e o convertem num string de saída de tamanho fixo, chamado valor de hash.

Uma função de hash one-way é uma função de hash que trabalha numa direção: é fácil computar um valor de hash de uma pré-imagem, mas é muito difícil gerar uma pré-imagem dado um valor de hash. Além disso, uma boa função de hash one-way é livre de colisões: não se deve ter duas pré-imagens com o mesmo valor de hash.

Algumas propriedades essenciais à funções de hash one-way são:

- A função de hash é pública, não havendo segredo no processo;
- A saída não deve ser dependente da entrada;
- Matematicamente, uma mudança de um bit na pré-imagem gera, em média, mudanças em metade dos bits da saída [SCH 96];
- Dado um valor de hash, é computacionalmente impraticável encontrar a pré-imagem que gerou aquele valor.

Eis um exemplo: caso você queira verificar se alguém possui determinado arquivo (que você também possui), mas não quer que ele o envie a você, peça a ele que envie o hash do arquivo – se ele enviar o hash correto, provavelmente possui o arquivo (lembre-se, há outras condições não consideradas aqui).

Códigos de autenticação de mensagens

Um código de autenticação de mensagem (do inglês *message authentication code* – ***MAC***), é uma função de hash one-way com a adição de uma chave secreta. O valor de hash é uma função tanto da pré-imagem quanto da chave – somente quem possui a chave pode obter a pré-imagem.

Comunicação com o uso de criptografia de chaves públicas

Em 1976, Whitfield Diffie e Martin Hellman apresentaram o conceito de criptografia de chaves públicas. Eles usaram duas chaves diferentes – uma pública e uma privada, sendo computacionalmente inviável, como já vimos, deduzir-se a chave privada a partir da chave publica.

Eis um exemplo:

1. A e B concordam quanto ao criptosistema de chave pública;
2. B envia a A a sua chave pública;
3. A encripta sua mensagem usando a chave pública de B;
4. A envia a mensagem a B;
5. B decripta a mensagem de A com sua chave privada.

Observe que a criptografia de chave pública soluciona o problema de gerenciamento de chaves: sem arranjo prévio quanto à chave, A pode enviar sua mensagem para B. Um atacante pode obter a mensagem, mas sem a chave privada de B não poderá abri-la.

De forma mais comum, vários usuários podem combinar o uso de um criptosistema de chave pública. As chaves públicas são, então, postadas num repositório (um banco de dados, ou um diretório de uso comum).

Agora, o protocolo é ainda mais fácil:

1. A obtém a chave pública de B a partir do banco ou diretório;
2. A encripta sua mensagem e a envia a B;
3. B decripta a mensagem de A com sua chave privada.

Assinaturas digitais

Assinaturas manuais têm sido usadas há muito tempo como prova de autenticidade ou de concordância com o conteúdo de um documento. Eis algumas de suas características, que levam uma assinatura a ter valor legal:

- A assinatura é autêntica – a assinatura convence o recebedor do documento que o assinante deliberadamente assinou o documento;
- A assinatura não é passível de fraude – é uma prova de que o autor, e não outra pessoa, deliberadamente assinou o documento;
- Não é reutilizável – a assinatura é parte do documento; uma pessoa inescrupulosa não pode remover a assinatura de um documento e colocá-la em outro;
- O documento assinado não é alterável – uma vez assinado, ele não pode ser alterado;
- A assinatura não pode ser repudiada – o assinante não pode alegar que não assinou o documento.

Na verdade, nenhuma das afirmações acima é completamente verdadeira. Contudo, convivemos com os problemas decorrentes da crença nestas caractarísticas.

No mundo digital, é fácil imaginar que os problemas são ainda maiores.

Assinando documentos com sistemas simétricos e um árbitro

A deseja assinar uma mensagem digital e enviá-la a B. Com a ajuda de um árbitro e um criptosistema simétrico, isto é possível.

O árbitro, digamos, T, pode se comunicar com A e B (e quem mais desejar assinar um documento digital). T compartilha uma chave secreta com A, K_A, e uma chave secreta diferente K_B, com B. Estas chaves foram estabelecidas antes do início do protocolo e podem ser usadas múltiplas vezes para múltiplas assinaturas.

1. A encripta sua mensagem para B com K_A e envia para T;
2. T decripta a mensagem com K_A;
3. T toma a mensagem decriptada junto com uma declaração de que a recebeu de A e encripta o conjunto com K_B;
4. T envia o conjunto criptografado para B;
5. B decripta o conjunto com K_B. Ele agora pode ler a mensagem e ter a certificação de T de que ela veio de A.

Mantidas as condições de confiança, o protocolo acima possui as características de uma assinatura conforme vistas antes.

Este protocolo funciona, mas consome tempo excessivo de T, além de ele ter de posuir uma chave única para todos os participantes. Além disso, T deve ser completamente seguro – algo extremamente difícil em termos práticos.

Assinando documentos com criptografia de chaves públicas

Há algoritmos de chave pública que podem ser usados para assinaturas digitais. Em alguns deles, como RSA (Rivest-Shamir-Adleman), tanto a chave pública como a privada podem ser usadas para encriptação. O protocolo básico é simples:

1. A encripta o documento com sua chave privada, assinando-o;
2. A envia o documento assinado para B;
3. B decripta o documento com a chave pública de A, e assim verifica a assinatura.

Este protocolo é muito melhor que o anterior. Não a necessidade de um árbitro para assinar ou verificar assinaturas – ele é necessário para atestar que a chave pública de A pertence de fato a A. Caso B não consiga executar o passo 3, ele sabe que a assinatura não é válida.

Além disso, este protocolo corresponde às características anteriores.

Assinando documentos com selos temporais

No exemplo anterior, B pode reutilizar a mensagem assinada por A. E se for uma ordem de pagamento?

Para impedir a reutilização, assinaturas digitais possuem selos temporais (*time stamping*). A cada vez que o documento digitalmente assinado é apresentado, confere-se o selo temporal nele colocado para saber se ele já não foi (e se poderia ser) apresentado.

Assinando documentos com criptografia de chaves públicas e funções hash one-way

Para efeitos práticos, algoritmos de chave pública são ineficientes para assinar documentos longos. Para poupar tempo, protocolos de assinatura digital são freqüentemente utilizados com funções de hash one-way. Ao invés de assinar um documento, A assina o hash do documento. Neste protocolo, tanto a função de hash como o algoritmo de assinatura digital são acordados antecipadamente:

A produz um hash one-way de um documento;
A encripta o hash com sua chave privada, assinando-o;
A envia o documento e o hash assinado para B;
B produz o hash one-way do documento enviado por A. Decripta o hash assinado por A com a chave pública deste, e compara o hash produzido com aquele assinado.

A velocidade é grandemente aumentada e, uma vez que as chances de dois documentos diferentes terem o mesmo hash de, digamos, 160 bits é de uma em 2^{160}, tem-se uma enorme garantia de que a assinatura no hash equivale a uma assinatura no documento.

Este protocolo possui outros benefícios:

Pode-se ter um repositório para hashes de documentos; em caso de disputa, por exemplo, de patentes, os contendores são chamados a apresentar o documento cujo hash está contido no repositório; um selo temporal pode ser ponto em cada hash, de modo tal a garantir a ordem de apresentação de documentos: pode-se requerer direitos autorais de um documento sem trazê-lo a público.

Assinaturas múltiplas

E no caso de uma transação com mais de dois participantes, por exemplo, um contrato de compra e venda? Vejamos:

1. A assina o hash do documento;
2. B assina o hash do documento;
3. B envia o resultado de sua assinatura para A;
4. A envia o documento, sua assinatura e a de B para um terceiro (por exemplo, o cartório C);
5. C verifica a assinatura de A e de B.

A e B podem executar os passos 1 e 2 em série ou em paralelo. De qualquer modo, C pode verificar a assinatura de um de modo independente da do outro.

Não repúdio e assinaturas digitais

A pode trapacear com sua assinatura digital. Pode, por exemplo, assinar um documento e depois alegar que não o fez. Primeiro, assina o documento normalmente. Depois, divulga, anonimamente, sua chave privada. Alega, então, que sua chave foi comprometida e outros a estão usando.

O uso de selos temporais pode minorar este efeito, mas A sempre dizer que o comprometimento ocorreu antes. Este problema deriva do fato da chave privada estar em algum recipiente violável ou transmissível.

Infra-estrutura de chaves públicas

Conforme já se disse anteriormente, os certificados digitais são utilizados quando há a necessidade de trocar-se chaves públicas com alguém mais. Para pequenos grupos de pessoas que desejam comunicar-se seguramente, é mais fácil proceder a uma distribuição manual, através de disquetes ou e-mail, desde que confiáveis, contendo as chaves públicas a serem comunicadas. Esta é a chamada distribuição manual de chaves públicas, e, claramente, só é prática até um certo ponto. Além deste ponto, torna-se necessário utilizar sistemas que garantam os mecanismos segurança, armazenamento e intercâmbio de chaves públicas, para ambientes do cooperação, parceiros comerciais e destinatários dos mais variados alcances. Estas estruturas podem ser apenas repositórios de certificados, os chamados Servidores de Certificados, ou podem acrescentar características completas para a gerência de chaves, num conjunto chamado Infra-estrutura de chaves públicas - ICP (do inglês, *Public Key Infrastructures – PKI*).

Além de contar com um servidor para o armazenamento das chaves, uma ICP conta ainda com facilidades completas de gerenciamento de chaves, tais como as facilidades de emitir, revogar, armazenar, distribuir e autenticar certificados.

A principal característica de uma ICP é a introdução da chamada Autoridade Certificadora – AC (do inglês *Certificate Authority – CA*), que é a entidade – pessoa, grupo, departamento, empresa ou outra associação – que assegura a uma organização a capacidade de emitir certificados a seus usuários. Uma AC cria certificados e os assina digitalmente com a chave privada da AC, autenticando sua originalidade e confiabilidade. Pelo seu papel na criação de certificados, a AC é o componente central de uma ICP. Usando a chave pública da AC, qualquer pessoa que deseje assegurar a autenticidade de um certificado pode verificar a assinatura digital da AC, e garantir, assim, a integridade do conteúdo deste certificado (mais importante ainda, da chave pública e da identidade do detentor do certificado).

Serviços Viabilizados pela ICP

Dentre os serviços que se pode prover tendo como base uma ICP, pode-se citar:

Comunicação segura

Entendida como a transmissão de dados com uma ou mais da propriedades de autenticidade, integridade e confidencialidade. Este serviço se baseia, além das características da ICP, em protocolos de redes e de comunicações para criar um serviço expandido, que pode atender a correio eletrônico, web servers, redes privadas virtuais (do inglês *Virtual Private Network – VPN*), etc.

Cartório digital

Oferece as facilidades de certificação de dados, ou seja, atesta que os dados em questão são válidos, através da verificação da assinatura digital com a chave pública contida no certificado emitido pela AC, e que a entidade envolvida é de fato a detentora do certificado.

Não-repudiação ou irretratabilidade

Serviço através do qual uma pessoa ou entidade não pode negar ter cometido uma ação que de fato realizou, senão por imperícia ou má-fé. Como um exemplo, o emissor de uma mensagem com assinatura digital não pode afirmar não tê-la mandado, uma vez que, quando o receber decriptar a mensagem com o uso da chave pública correspondente, apenas o detentor daquela chave privada poderia ter feito a assinatura. Desta forma, ou sua chave está comprometida, ou ele de fato enviou a mensagem. Esta é a chamada não-repudiação de envio. Há ainda a não-repudiação de recebimento, de criação, de aprovação e de intermediação, que operam de modos análogos.

Certificados e Certificação

Toda a segurança de uma transação realizada através de certificados digitais baseia-se nas seguintes premissas:

a) a integridade da chave pública, e de quaisquer outras informações a elas associadas, deve ser assegurada;
b) a chave pública, bem como quaisquer outras informações a ela associadas, está relacionada a quem alega ser seu proprietário, de forma confiável.

A fim de assegurar estas premissas, e para garantir a interoperabilidade dos certificados entre diferentes plataformas, a ITU-T (International Telecommunication Union – Telecom Standardization) definiu um padrão de certificados digitais, chamado X.509, que apresenta o seguinte formato:

Campo	Utilização
Versão	Identifica a versão do certificado. A versão corrente é v3
Número serial	Identifica univocamente este certificado junto ao seu emissor (AC)
Assinatura	Indica o algoritmo utilizado para gerar a assinatura do certificado
Emissor	Nome único (Distinguished name – DN) do emissor
Validade	Indica a data de validade do certificado, a menos que ele seja revogado
Detentor	Nome único (DN) do proprietário do certificado
Chave pública	Chave e identificador do algoritmo de chave pública utilizado
Campos opcionais	Podem incluir extensões e outras informações que se considere relevantes

Naturalmente, os certificados em si, se não forem devidamente gerados, mantidos e utilizados, não são capazes de garantir a segurança que deles se espera. Nos casos de troca de certificados entre domínios de múltiplas ICPs, um conjunto de normas e políticas de certificação deve ser estabelecido, a fim de garantir a interoperabilidade entre as distintas AC envolvidas.

Além disso, uma outra entidade fundamental numa ICP é a Autoridade Registradora - AR (do inglês *Registration Authority, RA*). Ela atua em conjunto com a AC para aumentar a escalabilidade do funcionamento desta última, além de operacionalizar os custos envolvidos com a gerência dos certificados.

Embora as funções de AR possam variar, via de regra ela é responsável por:

- Estabelecer e confirmar a identidade de um indivíduo como parte do processo de inicialização da certificação (ou seja, coletar informações, documentos, etc.;
- Iniciar o processo de certificação junto à AC para os usuários finais;
- Gerar material de apoio em benefício do usuário final;
- Realizar algumas atividades de gerenciamento no ciclo de vida das chave e do certificado, tais como iniciar um processo de revogação.

A Gerência de Chaves e de Certificados

Dados volumes de informações que as aplicações do mundo real exigem, para o correto estabelecimento e funcionamento de uma ICP, e tendo em vista os requisitos de funcionalidade que uma tal infra-estrutura precisa ter para ser de fato útil e prática, deve-se ter em mente as seguintes características:

- O gerenciamento do ciclo de vida da chave e do certificado por parte da entidade final não é prático;
- Este gerenciamento deve ser o mais automatizado possível;
- ciclo de vida deve ser o menos invasivo o possível na rotina de seus usuários e participantes;
- O gerenciamento completo do ciclo de vida requer a operação e cooperação seguras de entidades confiáveis tais como a AC e a AR, assim como de software para usuários finais que interajam com estes componentes, quando necessário.

As várias fases do gerenciamento do ciclo de vida das chaves e dos certificados pode ser esquematizada pela figura 4.

Fase de inicialização

Antes que os usuários possam utilizar os serviços providos pela ICP, eles devem passar pelas etapas ilustradas na figura acima. O processo de registro pode ser feito de diversas maneiras, sendo que uma das possíveis é ilustrada pela figura 4. Ali estão envolvidos o usuário, a AC e a AR, sendo que esta última, em algumas aplicações, pode estar ausente deste processo.

O processo de geração do par de chaves (pública e privada) pode ser realizado no sistema do usuário (por exemplo, através de um browser), na AR, ou na AC. Em alguns ambientes, um uma facilidade de geração de chaves confiável, provida por terceiro, pode ser necessária. O local de geração do par de chaves é uma consideração de grande importância, e objeto de debates. Fatores que podem influir nesta escolha incluem a capacidade, performance, segurança, requisitos legais, e uso pretendido da chave.

Também a realização ou não do backup da chave é objeto de acalorados debates, pois pode ensejar, se mal utilizado, o uso indevido de um item que deveria ser de propriedade exclusiva do usuário.

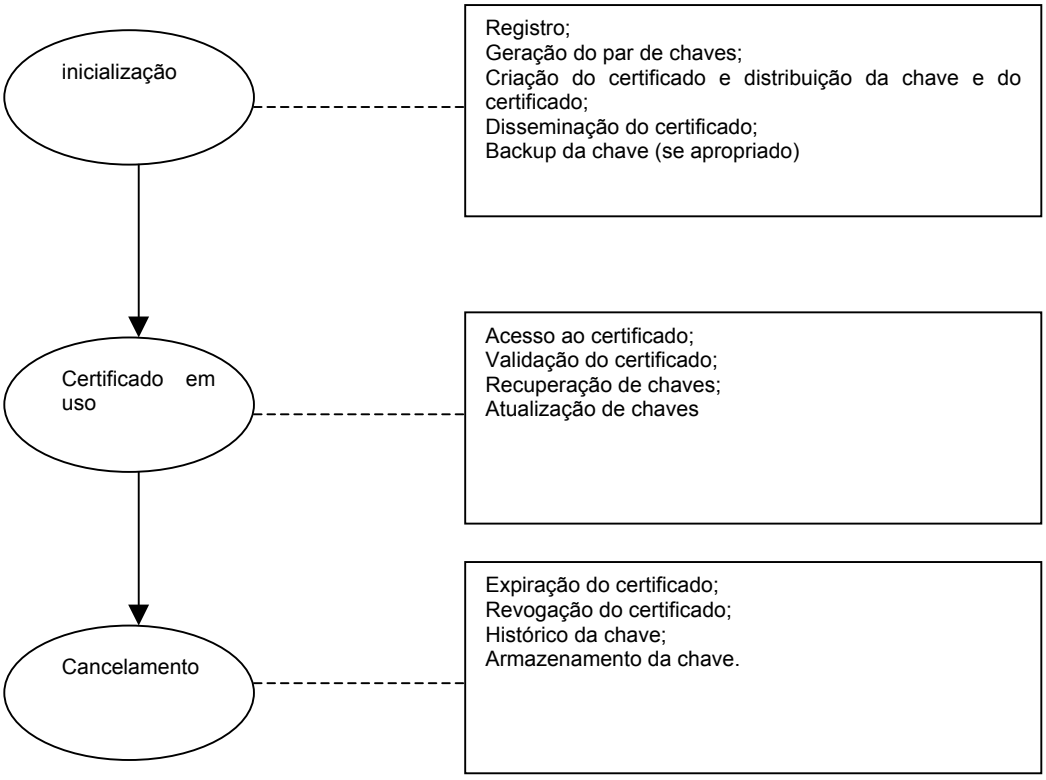

Figura 4 – Ciclo de vida de gerenciamento de chaves e certificados

A Revogação de Certificados

Os certificados somente são úteis enquanto são válidos. É altamente inseguro assumir que um certificado tenha validade indefinida. Em todas as ICPs, certificados têm um tempo de vida útil limitado, o que restringe o período no qual um sistema se torna vulnerável, caso ocorra um comprometimento do certificado respectivo.

Assim, os certificados são criados com um período de validade, conforme indicado em sua estrutura, período durante o qual espera-se que o certificado preserve sua utilidade. Quando o certificado expira, ele não será mais válido, uma vez que a autenticidade do seu par chave/identificação não será mais assegurada. Pode-se, quando muito, usar este certificado para confirmar informações que foram encriptadas ou assinadas durante seu período de validade – mas nada além deste ponto.

Há, ainda, situações em que pode ser necessário invalidar um certificado antes de sua data de expiração. Por exemplo, quando o empregado que é seu detentor encerra seu contrato de trabalho com a empresa, ou quando exista a suspeita de que chave privada correspondente àquele certificado tenha sido comprometida. Este último processo e chamado revogação. Um certificado revogado é muito mais suspeito que um certificado expirado. Certificados expirados não são úteis, exceto quanto à ressalva feita anteriormente, mas não trazem o mesmo comprometimento que um certificado revogado.

Qualquer usuário que tenha assinado um certificado pode revogar sua assinatura (desde que use a mesma chave privada utilizada quando da criação do certificado). Uma assinatura

revogada indica que o assinante não confia mais na associação entre chave pública e informações de identificação, ou que a chave pública do certificado (ou a chave privada correspondente) foi comprometida.

No caso dos certificados X.509, uma assinatura revogada tem praticamente a mesma importância que um certificado revogado, desde que a assinatura de revogação seja a mesma que tornou o certificado válido inicialmente – a assinatura da AC - somente o emissor do certificado pode revogá-lo.

Quando um certificado é revogado, é fundamental que os seus potenciais usuários sejam informados de que ele não é mais válido. Num ambiente de ICP, a comunicação dos certificados revogados é feita através de uma estrutura chamada Lista de Revogação de Certificados – LRC (do inglês *Certificate Revocation List*), que é publicada pela AC. A LRC contém uma lista de todos os certificados revogados e não expirados do sistema. Após a expiração, os certificados são retirados da lista. A AC distribui LRC para os seus usuários em intervalos regulares, ou potencialmente quando um certificado é revogado, o que, teoricamente, previne que se confie num certificado comprometido. Contudo, caso não haja um mecanismo de temporização extremamente confiável, é possível que se utilize um certificado comprometido entre duas emissões da LRC.

Modelos de Confiança

Em ambientes menores, a confiança entre entidades é estabelecida diretamente. No caso de grandes redes, a confiança entre entidades e principalmente entre certificados deve ser transmitida de outras formas.

Na maioria dos casos, em ambiente de ICP, os participantes confiam completamente na AC para estabelecer a validade dos seus certificados. Isto implica que todos se fiam na AC para realizar as tarefas de validação. Neste contexto, a AC atua como um meta-apresentador, que provê não apenas a validade das chaves, mas também a habilidade de confiar nesta validade. Ou seja, da mesma forma que um rei, ao apor seu selo num édito levado por ser seus enviados, a AC pode delegar a capacidade de validação a apresentadores confiáveis. Estes podem validar chaves da mesma forma que o meta-apresentador, mas não podem estabelecer novos apresentadores. A primeira AC, naquela em qual todos confiam, é chamada AC raiz, enquanto as demais são chamadas ACs subordinadas.

A AC Raiz usa uma chave privada associada com um tipo especial de certificado, chamado certificado de AC raiz, para assinar seus certificados. Qualquer certificado assinado pelo certificado da AC raiz é visto como válido por todas as outras ACs cujos certificados foram assinados pela AC raiz. Este processo de verificação regressiva a fim de verificar quem assinou qual certificado é chamado caminho ou cadeia de certificação.

Um modelo de confiança é o mecanismo pelo qual os usuários estabelecerão a validade dos seus certificados. Existem três tipos básicos de modelos:

a) Confiança direta, que é o modelo mais simples, no qual os participantes sabem de onde vem o certificado e conhecem o seu detentor;

b) Confiança hierárquica, na qual atribui-se confiança a certificados através da confiança em seu emissor, num caminho ascendente até uma AC raiz, e
c) Rede de confiança, que envolve ambos modelos anteriores, e no qual a confiança em um certificado é obtida parte pelo seu emissor, parte por informação adicional que se possua sobre seu detentor.

Múltiplos Certificados por Entidade

Para finalidades distintas, pode-se utilizar diferentes pares de chaves digitais. Por exemplo, indivíduos podem usar um certificado para e-mails pessoais, outro para transações financeiras, e assim por diante. Além disso, o emissor dos certificados pode aplicar a cada um restrições e privilégios distintos, bem como associar a eles atividades específicas, como procedimentos de backup, além da aplicação de regulamentos e normatização específicos para cada caso. Num contexto de múltiplas atribuições, torna-se comum que uma mesma entidade possua vários pares de chaves para as suas diferentes tarefas.

Uso de pares de chaves

Além de determinações de regulamentos ou da prática, a utilização de pares de chaves também pode ser restrita pelas sua própria construção, a partir do seu algoritmo gerador. Particularmente, um par de chaves gerado pelo *DAS (Digital Signature Algorithm)* não pode ser usado para encriptação e decriptação quando implementado conforme as especificações do algoritmo. De modo similar, um par de chaves Diffie-Hellman não pode ser usado para assinar dados e verificar as assinaturas. Além disso, uma par de chaves gerado pelo algoritmo RSA (Rivest-Shamir-Adleman), embora possa ser aritmeticamente utilizado para autenticação, integridade, confidencialidade ou troca de chaves, pode ter sua aplicabilidade reduzida, por opções de implementação, políticas de uso ou legislação, a apenas alguns casos.

Assim, um par de chaves pode estar associado com uma política específica para

Uma qualidade ou quantidade particular de uso (por exemplo, transações de compra até determinado valor), associado a

Um tipo de uso particular (por exemplo, a autorização de transações de compra), associado a

Uma categoria de uso particular (por exemplo, verificação de conteúdo de dados), associado a

Um serviço de uso particular (por exemplo, autenticação).

Outro tipo de restrição de uso pode ser uma aplicação ou protocolo em particular. Por exemplo, um par de chaves pode ser utilizado para autenticação de entidades sob o protocolo IPSec, mas não sob o protocolo SSL.

Uma ICP que se proponha completa e abrangente deve estar apta a lidar com estas situações.

Relacionamento entre pares de chaves e certificados

Se uma determinada entidade, afiliada a uma ICP, possui múltiplos pares de chaves, é de se esperar que ela tenha múltiplos certificados, pois o formato de um certificado não permite naturalmente que ele contenha mais que um par de chaves. Contudo, isto não impede que o mesmo par de chaves possa aparecer em vários certificados simultaneamente válidos.

O benefício mais citado de se permitir que um mesmo par de chaves apareça em mais de um certificado é a simplicidade de renovação do certificado. Se um par de chaves não foi comprometido (ou seja, a chave privada não foi descoberta por eventuais atacantes), e apresenta segurança criptográfica contra ataques iminentes, pelo tamanho de sua chave, então, por simplificação, pode-se supor que ao aproximar-se sua data de expiração, sua chave pública possa ser colocada num novo certificado, com um novo período de validade. Esta ação estende a "vida útil" do par de chaves, e não exige que as partes que nele confiam precisem atualizar seu conhecimento sobre a chave pública associada. Além disso, o detentor do certificado não precisa mudar sua chave, e fica assim livre de ter de manter um histórico das chaves, ao longo do tempo.

Deve ficar claro que o argumento acima é relativamente fraco para muitos ambientes. Um implementações de ICP, não se trata apenas a chave, mas sim o certificado, e assim as partes que necessitam transacionar com a entidade atualizam integralmente o certificado recebido, atualizando também o valor da chave ali contida.

Além disso, a possibilidade de que um mesmo par de chaves exista em diferentes certificados válidos pode ensejar tentativas de ataques por substituição, tentando usar um certificado para determinada finalidade com a intenção de atingir outro objetivo.

Uma última consideração diz respeito à revogação: se uma mesmo para de chaves é usado em vários certificados, e a chave privada é comprometida, deve-se proceder à imediata revogação de todos os certificados associados, sob pena de criar-se uma gravíssima falha de segurança.

Suporte à não-repudiação

Para a implementação do serviço de não-repudiação, a habilidade de tratar-se múltiplos pares de chaves é um requisito fundamental. Uma condição necessária à não-repudiação é que a chave privada envolvida na ação não seja conhecida por nenhum outra entidade que não a sua detentora.

Esta característica difere claramente do caso em que uma chave é usada para cifragem, por exemplo. Em muitos ambientes, políticas determinam que as chaves privadas de decriptação sejam copiadas por uma entidade confiável, de tal forma que, se o seu detentor perder ou esquecer a chave, os dados possam ser recuperados. Chaves de decriptação, portanto, devem ser recuperáveis. Chaves de assinatura, por outro lado, especialmente no caso de ações onde se pretenda usar o argumento da não-repudiação, jamais devem ser copiadas, devendo ser atribuídas e ser do conhecimento exclusivo do detentor do respectivo certificado .

Tendo em vista estas considerações, alguns ambientes determinam a existência de pelo menos três pares de chaves por entidade:

a) Um para encriptação/decriptação;
b) Um para assinatura/verificação de propósitos gerais;
c) Um para assinatura/verificação para casos de não-repudiação.

A Disseminação das Informações da ICP: Repositórios e Outras Técnicas

A troca de informações relativas aos certificados, sua revogação e outras informações de controle pode ser feita de variadas formas.

Disseminação privada

Talvez o mecanismo de distribuição mais básico seja a chamada disseminação privada, na qual cada indivíduo troca certificados diretamente com os demais, seja manualmente, através de disquetes, seja através de e-mail.

Nesta modalidade, a revogação de certificados é tipicamente informal e não confiável. Claramente, limita-se, em termos práticos, a grupos de usuários pequenos e presumivelmente amigáveis entre si. O protocolo PGP (Pretty Good privacy), e posteriormente o OpenPGP, baseiam-se nesta modalidade. Embora haja um número elevado de usuários, em escala real os níveis de confiabilidade se restringem a grupos pequenos, onde o conhecimento pessoal norteia a confiabilidade no grupo.

Este modelo não se aplica ao domínio das grandes corporações, principalmente devido aos seguintes motivos:

a) A disseminação privada de certificados não é escalável;
b) Como já se viu, a disseminação da revogação de certificados não é confiável, principalmente quando a agilidade da disseminação torna-se crítica;
c) Um modelo de confiança centrado no usuário é inconsistente com o modelo operacional dos domínios corporativos, nos quais o controle centralizado sobre ações dos usuários é requerida.

Publicações e repositórios

O método mais comum para a distribuição de certificados e informação de revogação é a publicação. O conceito baseia-se na colocação da informação num local conhecido, de acesso público e fácil. É um método bastante atrativo para grandes comunidades de usuários que são, em geral, desconhecidos pessoalmente uns dos outros.

No meio corporativo, é mais usual disponibilizar as informações num repositório, que pode ser qualquer base de dados capaz de armazenar informações, e de disponibilizá-las quando necessário. Neste meio, repositórios são tipicamente baseados no protocolo LDAP (Lightweight Directory Access Protocol – RFC 2251) e/ou na série de recomendações X.500. Alguns exemplos que se incluem sob o conceito de repositórios, além dos servidores LDAP, são:

- DASs (*Directory System Agents*) X.500 ;

- DNS (*Domain Name System*) com suporte a informações de certificados e revogações (RFC 2538);
- Servidores web com o mesmo suporte (RFC 2585);
- Bases de dados corporativas, com práticas de acesso e gerenciamento bem definidas;
- Módulos de resposta OCSP (*Online Certificate Status Protocol*), para o caso das informações de revogação.

As vantagens de usar-se um ou mais repositórios são várias. Uma delas é o fato de que muitas organizações já têm instalado um servidor corporativo, e basta incorporar à sua infra-estrutura as informações relativas à ICP. Também se provê uma localização centralizada a partir da qual se pode recuperar as informações. Isto reduz significativamente a quantidade de certificados e de LRCs que se necessita armazenar localmente. Em contrapartida, gera-se um overhead de tráfego de informações em rede, além da performance do servidor de repositório dever ser compatível com a demanda gerada pelos usuários, a fim de evitar-se gargalos de performance.

Características de privacidade

A existência de repositórios de acesso público introduz a preocupação com a privacidade da informação ali colocada, principalmente se ela for sensível (não é recomendável a colocação de deste tipo de informação nos certificados ou nas LRCs). Ainda que cada certificado, por si mesmo, não seja considerado sensível, a colocação de um grande volume destes em um mesmo local pode atrair a atenção de potenciais atacantes (interessados, por exemplo, na informação das pessoas e entidades ali representadas).

Num contexto de intercâmbio de informações de diferentes domínios, mormente com o mundo externo, quando uma corporação deseja comunicar-se com outras, fica evidente a necessidade de que os certificados de uma organização, assim como suas LRCs, sejam vistas e compatíveis com as das outras, e vice-versa.

Numa ICP corporativa, os certificados e as informações de revogação são tipicamente colocadas num repositório público (por exemplo, um servidor LDAP), e as informações de revogação são colocadas na forma de LRCs em pontos de distribuição de LRCs. O software cliente recupera os certificados e LRCs sob demanda. No contexto interdomínios, o método usado para disponibilizar estas informações, e a freqüência com a qual elas são atualizadas, são objeto de acordo entre os domínios cooperantes.

Existe uma preocupação crescente no nível corporativo, com relação à disseminação descontrolada de certificados e de informações de revogação. Neste caso, o conceito de um repositório numa base de dados acessível publicamente vai de encontro à políticas que determinam tais informações são sensíveis e, portanto, de acesso restrito. Informações sensíveis podem incluir dados referentes a usuários externos, infra-estrutura da organização, nomes e dados de empregados, etc. Deve-se estabelecer métodos que possibilitem a correta disseminação das informações que se deve propagar, mas com requisitos adequados de segurança, atentos a estes problemas.

Alguns artifícios usados compreendem a substituição do *DN (Distinguished Name*) por um código que seja de conhecimento apenas interno, gerando os chamados certificados anônimos – esta é uma das suas várias formas de geração.

Estes métodos, no entanto, são de utilização restrita.

Opções de implementação de repositórios interdomínios

A figura 5 ilustra algumas configurações associadas com a implementação de repositórios no cenário interdomínios. A opção A mostra o uso de acesso direto a partir de entidades externas ao repositório corporativo. A opção B ilustra outras duas alternativas possíveis. A primeira é a replicação parcial dos dados armazenados no repositório corporativo num local fora da fronteira do firewall corporativo. O repositório que hospeda esta informação parcialmente replicada é denominado repositório de borda. A segunda alternativa mostrada na opção B é que o repositório de borda torna-se um repositório intermediário, ou proxy, e as solicitações que chegam são encadeadas ao repositório alvo sem qualquer outro envolvimento do usuário. Observe-se que as opções A e B podem ser usadas em conjunto em alguns ambientes, assim como as duas derivações da opção B. Naturalmente, as necessidades de implementação irão determinar a configuração adequada a cada situação. A seguir, cada uma destas arquiteturas é discutida com maiores detalhes.

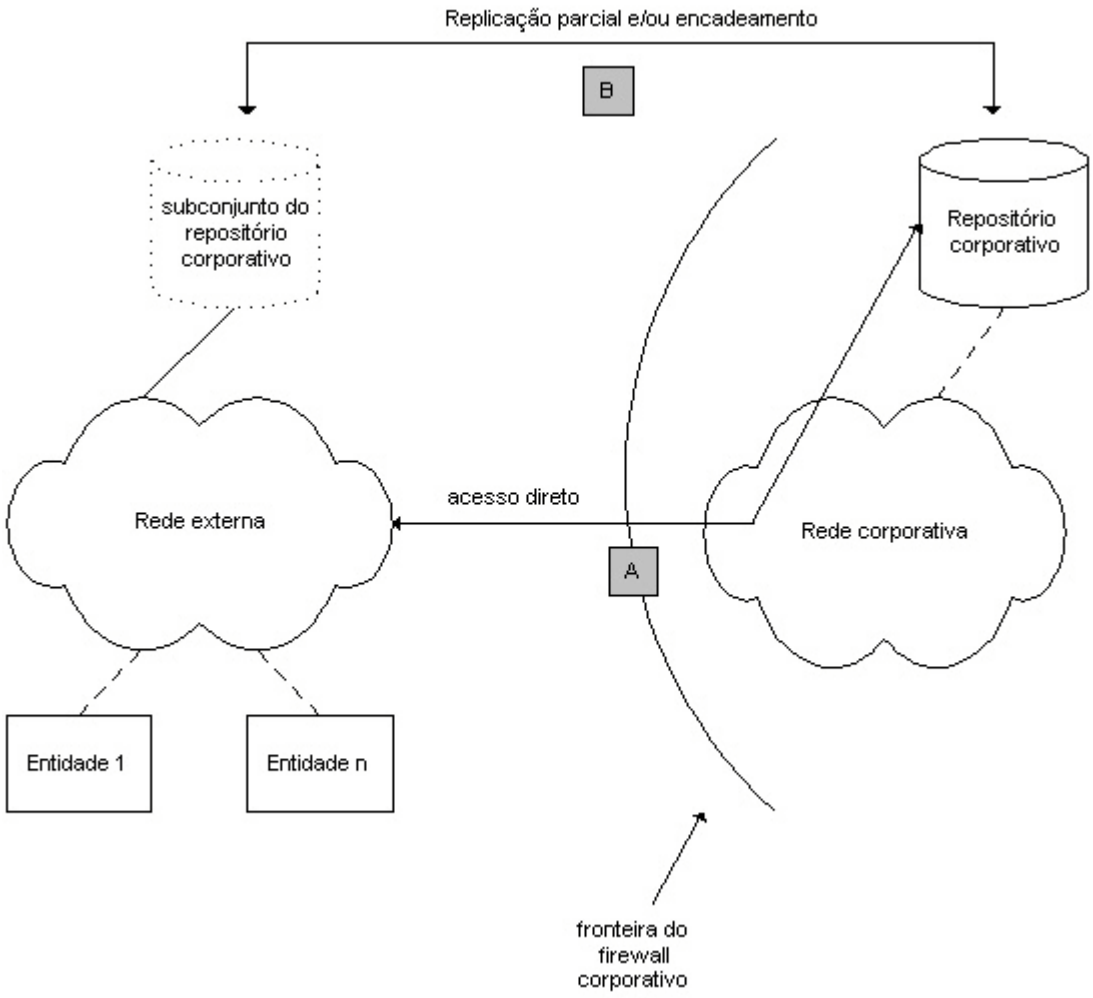

Figura 5 – Opções de implementação de repositório interdomínio

Acesso direto

A alternativa de acesso direto permite o software cliente de usuário final em um domínio possa obter acesso ao repositório em outro domínio, e vice-versa; pode, ainda, permitir que um repositório externo encadeie suas requisições de acesso diretamente ao repositório corporativo interno. Isto pode ser apropriado quando a relação de confiança entre os dois domínios é recíproco e/ou o próprio repositório é seguro e protegido contra acesso não autorizado. Além do controle de acesso, um mecanismo de confidencialidade pode ser exigido para prevenir o acesso não autorizado a informações, quando elas são transmitidas de um domínio corporativo para outro. Isto pode ser realizado de variadas formas (por exemplo, através do uso de protocolos de segurança como TLS – *Transport Layer Security*; recursos de encapsulamento do IPSec; ou com o uso de protocolos da camada de aplicação como o DAP – *Directory Access Protocol* – do X.500).

Repositório compartilhado

Um repositório compartilhado permite que cada domínio da ICP poste suas informações de certificados e de revogações num repositório comum, de modo tal que outros domínios da ICP possam recuperar estas informações, quando necessário. O repositório compartilhado pode ser de propriedade e operação conjunta de dois ou mais domínios, ou serviço provido por terceiros. Os mecanismos de postagem e recuperação de cada domínio podem ser distintos, desde que a estrutura e a freqüência das atualizações sejam mantidas como acordadas, e desde que o repositório compartilhado suporte múltiplos protocolos para este propósito. Pode-se implementar controle de acesso ao repositório compartilhado para prevenir o acesso não autorizado, e serviços de reforço de confiabilidade (como TLS) podem ser usados para prevenir a revelação de informações em trânsito.

Replicação interdomínios

Esta opção compreende a cópia das informações de certificados e de revogação, para os casos em que for aplicável, diretamente de um domínio para o outro, e vice-versa. Deve-se observar que a capacidade de automatização deste processo depende do protocolo, ou conjunto de protocolos, sendo utilizado. Por exemplo, se ambos domínios suportam serviços de diretórios baseados em X.500, isto pode ser realizado através dos mecanismos existentes no próprio protocolo (especificamente, o DISP – *Directory Information Shadowing Protocol*). Por outro lado, se o único protocolo comum entre os dois domínios é LDAP, ainda se dispõe de protocolo padrão na indústria para a replicação, embora haja grupos trabalhando neste sentido. Espera-se por uma solução do IETF (Internet Engineering Task Force) neste sentido. Outra alternativa seria o LDIF – *LDAP Data Interchange Format*.

Algumas considerações sobre o protocolo LDAP se fazem necessárias. Embora o LDAPv2 tenha sido amplamente utilizado nas implementações anteriores de ICPs, ele é, geralmente, considerado deficiente nas seguintes áreas:

- O mecanismo de autenticação de implementação obrigatória entre um cliente e um repositório é baseado em identificação do usuário e senha que trafegam em claro;
- Não existe esquema de controle de acesso padronizado;
- Não existe mecanismo padrão de replicação de dados entre repositórios LDAP (de fato, não existe suporte para comunicação servidor-a-servidor);
- Os filtros de pesquisa LDAP existentes são considerados inadequados;

- Não existe mecanismo de confidencialidade acordado, para proteger dados armazenados ou em trânsito;
- Não existe a facilidade de operações assinadas, padronizadas.

Estas limitações do LDAPv2 são amplamente conhecidas, e novas características estão sendo introduzidas com o advento do LDAPv3 (RFC 2251), a fim de corrigi-las. Particularmente, o Grupo de Trabalho do IETF LDAPext está trabalhando num grupo de melhorias, incluindo, além de outras:

- Mecanismos fortes de autenticação;
- Modelo padronizado de controle de acesso;
- Suporte a referências e orientações técnicas;
- Suporte a confidencialidade de sessão;
- Suporte a operações digitalmente assinadas.

Maiores detalhes sobre este Grupo de Trabalho podem ser obtidos em www.ietf.org/html.charters/ldapext-charter.html

Repositório de borda

Talvez uma das mais difundidas opções, nesta arquitetura um repositório em separado é mantido fora dos limites do firewall corporativo de qualquer uma das corporações participantes. As informações de certificado e de revogação são postadas neste repositório conforme a determinação e controle de cada organização, ou pode ser recuperada a partir do repositório de borda por encadeamento. Neste caso, requer-se o uso de DSP (*Directory System Protocol*) do X.500, ou a existência de um mecanismo proprietário. A especificação atual do LDAP não suporta encadeamento, explicitamente.

O acesso externo ao repositório de borda pode ser ou não controlado, dependendo-se dos requisitos e sensibilidade das informações ali concentradas. Em qualquer caso, os clientes remotos estarão aptos a obter o acesso à informação sem a necessidade de passar através do firewall corporativo, e, conseqüentemente, sem acessar diretamente as bases de dados corporativas (vide opção B da figura 5).

Guarda

Esta opção envolve a implementação de um mecanismo de guarda que aceitaria requisições externas e, após verificações adequadas de controle de acesso, recuperaria a informação solicitada dos repositórios internos, retornando a resposta à entidade final externa. Embora similar a um firewall corporativo, esta opção difere no sentido de que ela não permite que a requisição original atravesse a rede interna corporativa e obtenha acesso direto ao repositório alvo. Pode-se considerar este mecanismo como um proxy: as requisições externas são interceptadas, e a informação apropriada é recuperada pelo guarda somente quando permitido. Os resultados (que podem ser ainda filtrados pelo guarda), são então passados em resposta ao solicitante.

Intercâmbio por protocolos sob demanda

Publicação e disseminação privativas não são os únicos métodos que podem ser usados para transportar informações de certificados e de revogação. O intercâmbio por protocolos sob

demanda pode ser suportado como parte dos protocolos de comunicação. Por exemplo, isto pode ser provido com e-mail implementado a versão 3 de S/MIME (*Secure/Multipurpose Internet Mail Extensions*). Outros protocolos que têm a capacidade de realizar a troca de informações de certificados e revogação incluem TSL e IPSec (especificamente, o protocolo IKE, ou *Internet Key Exchange*).

Em alguns ambientes, o intercâmbio de informações da ICP por protocolos sob demanda pode ser a única forma de conduzir esta informação aos seus destinatários. Por exemplo, a Internet confia neste mecanismo, pois não existe nenhum sistema de repositórios único, de forma tal a disseminar todas as informações de ICPs. Contudo, já se observa uma mudança em direção a uma verificação de status de certificados na Internet, para alguma aplicações. Entretanto, se existirá um sistema de repositório único (talvez baseado em DNS) na Internet é ainda uma questão a se ver no futuro.

Observe-se que o uso de intercâmbio de informações por protocolos sob demanda pode complementar o uso de repositório, mas não o substitui. Por exemplo, o certificado de verificação de um emissor pode ser enviado juntamente com um e-mail digitalmente assinado. Isto permite ao destinatário a verificação da assinatura digital do emissor sem a necessidade de consulta a um repositório. Contudo, o certificado de encriptação para o destinatário pretendido pode ser recuperado de um repositório na origem da mensagem, e a informação de revogação associada ao certificado do emissor pode também ser recuperada de um repositório como parte de um processo de verificação de assinatura digital. Esta orientação é comumente encontrada em práticas de implementação correntes.

Considerações Operacionais sobre ICPs

A fim de se operar com sucesso uma ICP, deve-se levar em conta determinados requisitos, características e opções de caráter operacional. Algumas delas são discutidas a seguir.

Software de plataforma cliente

Um componente da ICP para o lado cliente é essencial, dadas as limitações nas aplicações atuais (por exemplo, com respeito à verificação de revogação, gerência do ciclo de vida da chaves, ou ao reforço da política de certificação durante a validação). Não se deve considerar que o aumento da segurança em aplicações de prateleira, como browsers, gerarão um decréscimo na necessidade de software cliente. Deve-se lembrar que, por mais poderosa que seja uma ferramenta como um browser, em termos de segurança, ela é apenas uma das várias aplicações que um usuário utiliza ou executa em sua plataforma. Para acesso consistente e uniformemente seguro entre plataformas (cliente-servidor), a funcionalidade e segurança deve se posicionar fora (e ainda assim ser chamada a partir) de qualquer aplicação em particular. Esta é a arquitetura escalável e gerenciável que se reflete na definição de uma ICP. Observe-se que inserir a funcionalidade de segurança no sistema operacional ainda não é uma solução genérica o suficiente, pois isto poderia impedir uniformidade de segurança multiplataforma. O componente da ICP do lado cliente deveria ser uma biblioteca (ou módulo, toolkit, applet, ou que forma tenha) independente, passível de ser chamada pelo sistema operacional.

É importante notar que, a menos que todos os sistemas operacionais e aplicações utilizem o mesmo componente de ICP do lado cliente, a uniformidade multiplataforma não

poderá ser alcançada. Pode-se argumentar, ainda, que o suporte a funções de ICP no espaço do usuário e da aplicação é mais vulnerável a ataques e modificações do que funções embutidas no sistema operacional.

Contudo, não é garantido que o sistema operacional é sempre menos vulnerável. Além disso, diferentes sistemas operacionais proverão diferentes níveis de segurança e diferentes funcionalidades de ICPs. Por estes motivos, a uniformidade de segurança através de componentes do lado cliente é mais facilmente alcançável, ao menos a curto e médio prazos.

Em algumas circunstâncias, pode ser desejável deslocar funcionalidades mais complexas, computacionalmente pesadas e de consumo intensivo de memória, dos clientes. Dispositivos como os PDAs (*Personal Digital Assistants*), telefones celulares, pagers, etc., podem não ter capacidades para incorporar estas funcionalidades localmente. O uso destes mecanismos pode trazer à baila os benefícios da autenticação, integridade e confidencialidade, mas os dispositivos, em si, podem ser fisicamente incapazes de implementar operações completas de uma ICP (por exemplo, validação completa do caminho de um certificado, e gerenciamento do ciclo de vida de chaves). Uma solução possível (além de esperar que estes dispositivos atinjam maturidade tecnológica adequada), é dividir a funcionalidade. O dispositivo, assim , em vez de fazer por si mesmo o processamento do caminho de um certificado, envia o certificado para algum servidor confiável, recebendo apenas um O.k. ou não quanto à confiabilidade do certificado em tratamento. Naturalmente, considerações a respeito deste modelo devem ser tomadas.

Esta arquitetura parece vir ao encontro de componentes de ICP sem lado do cliente, pois um servidor central pode realizar todas as operações da ICP, enquanto os dispositivos da plataforma local apenas enviam suas requisições e aguardam pela resposta. Recursos do lado do cliente protegem os dispositivos (seus sistemas operacionais, aplicações locais, etc.) da necessidade de compreender e processar a segurança corretamente, além de facilitar a administração. Por exemplo, se uma falha de segurança é encontrada no protocolo de requisição/resposta, pode ser muito mais fácil atualizar um módulo do lado do cliente do que modificar um número potencialmente numeroso de aplicações cliente que implementarem o protocolo diretamente.

Estas considerações, nitidamente operacionais, têm grande impacto sobre a escolha dos dispositivos que irão compor a arquitetura da ICP.

Operações off-line

Uma decisão de arquitetura que deve ser feita dia respeito à preocupação quanto à operação dos requisitos on-line/off-line da ICP: os usuários da ICP devem estar on-line a fim de que com ela interagirem, ou a operação off-line é permitida? Esta decisão é importante porque deve-se reconhecer que ao menos alguns dos usuários estarão desconectados (por exemplo, em viagem). A funcionalidade obtida por estes usuários é uma função das aplicações sendo implementadas no ambiente da ICP. Algumas requerem conectividade, e assim os usuários devem estar conectados. Outras são projetadas para funcionar em esquemas de enfileiramento, permitindo o seu uso quando o usuário estiver desconectado da rede. Um exemplo de uso off-line é a composição de e-mail, num laptop. Se a operação da ICP off-line é possível, o e-mail composto pode ser assinado digitalmente, e também cifrado para seus destinatários, usando-se certificados, informações de revogação e outras contidas no cache da

máquina. Por outro lado, se a operação off-line não é permitida (por exemplo, desabilitando-se o cache local de dados da ICP), o e-mail pode ser redigido, mas não pode ser cifrado. Isto significa que ele deve ser armazenado em claro na máquina local (a menos que se use uma ferramenta para cifragem de armazenamento), até que o usuário possa reconectar-se à rede, cifrar a mensagem e transmiti-la.

Ainda com respeito à operação off-line, certas implicações de segurança devem ser levadas em consideração. Por exemplo, embora a informação de revogação (como as LRCs) possam ser armazenadas em cache local, esta informação pode ficar "congelada" pelo tempo em que o usuário não a atualiza. Ou seja, fora da rede, ele pode não ter acesso à informação de revogação mais atualizada, podendo aceitar um certificado que já não é mais válido.

Além disso, um servidor de temporizações, por exemplo, estaria indisponível para os usuários off-line, assim como quaisquer serviços de cartório digital e não-repudiação. Em ambientes típicos, vários usuários da ICP irão requerer tanto acesso on-line quanto off-line.

Segurança física

Os componentes mais sensíveis da ICP deveriam ser protegidos fisicamente em ambientes de alta segurança, prevenindo o acesso indevido, modificação ou destruição destes componentes.

A segurança física inclui um ou mais dentre os seguintes aspectos:

- Restrição ou eliminação do acesso via rede;
- Concentração dos componentes numa sala reforçada, fechada;
- Instalação de dispositivos de controle de acesso adequados (talvez com a inclusão de recursos biométricos);
- Uso de salvaguardas adequadas em backups em fitas e CDs.

Além disso, qualquer transferência de dados entre a rede e os componentes fisicamente seguros deve se dar de forma "limpa" (ou seja, demonstradamente, sem a presença de vírus, backdoors, etc.).

Deve-se observar que sempre existe uma permuta entre a segurança e a facilidade de uso dos sistemas. A segurança física tende a introduzir a intervenção manual, operações complexas e retardo de performance que não existiriam em ambientes onde a segurança fosse menor. Costuma-se dizer que "segurança é o inverso da conveniência", ou

$$Segurança = \frac{1}{Conveniência}$$

Componentes de hardware

Uma instalação de ICP baseada apenas em software (particularmente para a operação da entidade final) é perfeitamente adequada para alguns ambientes. Contudo, software aplicativo pode ser vulnerável a hackers, cavalos de Tróia, vírus, e uma ampla gama de tipos de ataque.

Mesmo usuários bem-intencionados podem causar falhas de segurança pela modificação inadvertida de componentes do sistema.

A fim de ampliar a proteção contra os riscos associados à implementação de ICPs apenas por software, alguns componentes de hardware podem ser agregados. Por exemplo, segurança adicional pode ser obtida através da combinação dos seguintes componentes:

- Dispositivos de hardware para realizar operações criptográficas;
- Smart cards, cartões PCMCIA ("PC cards"), ou outros tokens de hardware para armazenar chaves privadas ou outras informações sensíveis;
- Dispositivos biométricos para habilitar a identificação de usuários (e permitir funcionalidade da ICP do lado cliente).

Assim como no caso da segurança física, há uma permuta entre a segurança e a facilidade de uso. Porém, o impacto aqui é maior: com o acréscimo de componentes de hardware, a degradação da facilidade de acesso atinge uma parcela maior da população de usuários da ICP do que a atingida pela inserção de salvaguardas físicas.

Além disso, o uso de componentes de hardware tem grande impacto sobre a performance (especialmente smarts cards, com requisitos de memória e E/S), apelo e aceitação pelos usuários, e sobre os custos totais da solução.

Comprometimento da chave

O comprometimento da chave (ou seja, a revelação de uma chave privada para alguém não autorizado a sabê-lo), pode ser considerado em dois contextos:

Comprometimento da chave de uma entidade final, e
Comprometimento da chave privada de uma AC.

Esta seção trata do primeiro caso, ficando o segundo para a sessão seguinte.

Como um usuário toma conhecimento de que sua chave foi comprometida? Isto não é imediatamente óbvio (algo como alguém invadindo a residência de outrem, memorizando seu número de cartão de crédito, sem levá-lo e sem qualquer furto evidente). As entidades finais de ICP devem ser treinadas a observar qualquer atividade suspeita em seus ambientes, tais como arquivos movidos ou apagados, diretórios modificados, ou objetos que aparecem sem razão. Qualquer atividade não usual deveria levar a possibilidade de comprometimento da chave privada. Isto inclui o caso da plataforma – como um notebook ou um desktop – ser roubada ou extraviada.

Naturalmente, há total grau de certeza no caso da chave sob suspeita ser utilizada por outros. Nestes casos, a revogação do par de chaves, com a sua substituição por um novo par, deve ser imediata.

Tão logo se perceba (ou se suspeite) que a chave privada está comprometida, deve-se tomar as seguintes ações:

a) Enviar um pedido de revogação à autoridade apropriada, de tal forma que esta informação seja divulgada aos parceiros relevantes, para que interrompam o uso da chave pública correspondente, e
b) Proceder-se, caso desejado, à geração de um novo par de chaves, de tal forma a continuar a comunicação segura com os parceiros.

A primeira ação acima é criticamente importante, e deve ser realizada com a máxima urgência, pois a demora causa uma janela maior de oportunidades para a entidade que agora faz uso ilegítimo da chave comprometida. Num esforço para minimizar o tamanho desta janela, algumas das técnicas de revogação, como a usada pelo X.509 e PKIX-CMP (RFC 2510), incluem o conceito de uma data de comprometimento, tanto na solicitação da revogação quanto na LRC resultante. Assim, pode-se dizer, "descobriu-se o comprometimento hoje, mas acabo de voltar de uma semana de férias, e assim o comprometimento pode ter ocorrido em algum instante na semana passada. Por favor, revogue este certificado imediatamente, e informe aos usuários que a data estimada de comprometimento é de uma semana atrás".

Entretanto, este mecanismo é sujeito à má utilização, particularmente com respeito ao serviço de não-repudiação. Um usuário que deseja repudiar sua assinatura num contrato de três dias atrás, precisa apenas enviar uma mensagem à autoridade apropriada e alegar um comprometimento suspeito há quatro dias, uma semana, ou qualquer data de seu interesse. O certificado é revogado, a notificação de revogação reflete a data apresentada, e este usuário não está mais sujeito àquele contrato. Observe-se que não há modos de prevenir este mal uso por parte de usuários mal intencionados, mas legítimos. Em particular, se a não-repudiação deverá ser implementada, a "data estimada de comprometimento" não deveria estar disponível para as entidades da ICP.

A segunda ação listada, a certificação de um novo para de chaves, é teoricamente opcional, mas é tipicamente realizada, para que as entidades envolvidas continuem a fazer uso confiável das operações da ICP. Este processo de "recertificação" pode ser automatizado, ou pode requerer quase tanta operação manual e comunicação quanto o processo de inicialização original. O fator determinante é se os usuário ainda possui uma chave de assinatura não comprometida e o correspondente certificado de verificação. Se for este o caso, e a depender da flexibilidade do protocolo sendo usado, uma mensagem de solicitação de certificação para o novo par pode ser assinada pela chave não comprometida, e a validade do certificado de verificação atesta a autenticidade da solicitação. Por outro lado, uma chave de assinatura válida pode não estar mais disponível (por exemplo, se a entidade tem somente uma chave de assinatura e é esta chave que está comprometida). O processo de certificação de um novo par de chaves pode então exigir uma troca não automática de informações com a AC ou a AR, possivelmente incluindo um encontro físico ou uma chamada telefônica, para estabelecer a autenticidade exigida.

As conseqüências específicas do comprometimento de uma chave para uma entidade final dependem do tipo da chave. Por exemplo, se uma chave de assinatura é comprometida, o usuário pode revogar o certificado imediatamente, mas, com o mecanismo de temporização adequado, pode não precisar tomar qualquer outra ação. A revogação impede que o atacante possa personificar o usuário lesado. Contudo, sem temporização, todos os documentos assinados pelo usuário com esta chave se tornam suspeitos, pois não se pode provar conclusivamente quais foram assinados por ele antes do comprometimento. Mesmo que a temporização seja implementada, há algumas considerações que se deve tomar. Por exemplo, o atacante pode usar seu conhecimento da chave pública do usuário, e seu novo conhecimento da

chave privada, para solicitar um certificado de verificação para si próprio, associando este par de chaves ao seu nome. Ele pode, então, substituir seu certificado pelo do usuário numa mensagem assinada, e assim personalizar o usuário lesado. Este ataque não funcionará se os dados originalmente incluem uma cópia do certificado a ser usado para verificar a assinatura (prática sempre recomendada), mas poucos protocolos de envelope digital incluem esta facilidade como um padrão.

Se a chave comprometida é de decriptação ou de troca de informações, o usuário não somente deve revogar o certificado imediatamente, como também deve encontrar todos os documentos importantes que forma encriptados com uma chave simétrica que era protegida pelo par comprometido. Este documentos devem então reprotegidos (caso contrário, o atacante pode ler seu conteúdo). Novamente, esta solução não é perfeita. Cópias dos documentos do usuário podem existir noutros lugares, sem seu conhecimento (alguns podem já estar de posse do atacante). Por serem encriptados, o usuário pode não ter tomado os necessários cuidados na guarda ou cópia (backup) destes documentos.

Da discussão acima, nota-se a importância de manter-se os usuários cientes das preocupações quanto à segurança, não apenas a sua própria, mas de toda a ICP.

Preparação e recuperação de desastres

Conforme pode-se observar pela sessão anterior, o comprometimento de uma chave pode envolver a chave privada de uma entidade final ou de uma autoridade (por exemplo, AC ou AR). Em geral, o comprometimento da chave de uma autoridade é um problema maior que a perda do uso de uma chave: ambos eventos requerem o estabelecimento da confiança numa nova chave, mas o comprometimento da chave destrói a confiança das entidades nos documentos assinados por aquela entidade (tais como certificados). Se um atacante pode obter o conhecimento da chave privada de assinatura de certificados de AC, ele se torna, para todos os efeitos, a própria AC, e pode emitir os certificados que quiser no domínio daquela AC, com os prazos de validade que desejar. Pode ainda criar certificados cruzados, que podem fazer com que entidades dentro do domínio da ICP comprometida estendam sua confiança a AC que de outra maneira não seriam confiáveis. As implicações de segurança destes eventos são extremas, e podem levar a ICP a um cenário francamente desastroso.

Notificação de parceiros de confiança

Uma das razões pelas quais o comprometimento da chave de uma AC não tem uma série de passos de tratamento padronizada é que, para alguns ambientes, simplesmente informar as comunidades de confiança que um desastre ocorreu é um problema não resolvido. Por exemplo, num modelo de confiança em rede, uma AC cuja chave pública esteja inserida em um mais browsers populares não pode conhecer quem são, precisamente, os seus parceiros de confiança. Browsers são instalados por milhões de usuários, e baixados de milhares de diferentes servidores; é virtualmente impossível determinar que usuários têm que browsers, em quem, dentre estes usuários, confia em que chaves ali inseridas. Assim, se a chave privada de uma AC é comprometida, não existe maneira confiável de informar às entidades da ICP que isto ocorreu, e alertá-las a não aceitar certificados assinados com esta chave.

Para alguns ambientes, o problema de notificar os parceiros de confiança pode ser parcialmente resolvido pela colocação do certificado auto-assinado correspondente à chave

privada comprometida da AC numa LRA - Lista de Revogação de Autoridades – LRA (ARL - *Authority Revocation List*). Embora contra a intuição comum (não é imediatamente óbvio porque uma lista de revogação assinada com uma chave que se proclama comprometida deva obter a confiança de alguém), isto pode ter seu valor. Se um atacante descobre a chave privada de uma AC, precisamente, a última coisa que ele deseja fazer é tornar seu novo poder, revogando o certificado correspondente. Ainda que ele deseja perpetrar uma ou duas atividades e depois revogar o certificado, tentando cobrir sua trilha, uma LRA alegando que a chave privada de AC foi comprometida deveria ser vista com seriedade pela entidades da ICP atingida. Assim, a confiança na chave pública correspondente deve ser interrompida.

Uma forma alternativa de habilitar-se a notificação de LRAs é a implementada nas especificação do SET (Secure Electronic Transaction). Neste mecanismo, uma LRA contendo a chave comprometida é expedida, assinada pela nova chave privada da AC (ou seja, a que substitui a comprometida). Os parceiros de confiança estão aptos a validar esta assinatura recuperando a nova chave pública da AC, calculando o hash desta chave, e comparando o resultado com o valor do hash inserido no velho certificado da AC. Este método funciona bem, mas ele exige que a AC gere seu novo par de chaves (o de substituição) no momento de certificação de seu par de chaves atual (de tal forma que ele possa incluir o hash da próxima chave pública no certificado atual). Assim, os pares de chaves atual e próximo existem simultaneamente, aumentando a probabilidade de que o comprometimento de uma leve ao comprometimento da outra (por exemplo, se forem armazenadas no mesmo local).

Em qualquer caso, inclusão numa LRA é uma solução parcial, por ao menos duas razões. Primeiro, a chave pública de uma AC nem sempre é empacotada como um certificado auto-assinado, no ambiente local de um parceiro de confiança (ela pode ser gravada como uma chave "nua", exposta). Nestes casos, não há como apontar esta chave numa LRA, como hoje definidas as LRAs, pois a sintaxe das LRAs aponta para certificados usando nome do emissor e número serial do certificado. Depois, e talvez mais importante, o software dos parceiros de confiança pode ser capaz de verificar uma LRC por um certificado de entidade, mas não ser geral genérico o suficiente para também verificar uma LRA (porque tal lista de revogação são tipicamente usadas somente em ambientes que suportam certificação cruzada).

Assim, a notificação não automática do comprometimento da chave de uma AC é sempre útil e sempre recomendada. Isto pode ter a forma de mensagem direta e direcionada (sempre que os membros da comunidade de parceiros de confiança são conhecidos da AC), pode usar comunicações de massa (algo que a AC pode relutar em utilizar), e ainda outros métodos.

Preparação

Obviamente, a melhor forma de preparar-se para uma catástrofe é tentar assegurar-se de que a catástrofe jamais ocorra. Assim, cada AC deve seguir todos os passos imagináveis para proteger sua(s) chave(s) privada(s).

No caso de comprometimento, uma AC pode tomar um ou mais dos seguintes caminhos para ajudar a minimizar o dano decorrente:

- Tentar, de todos os modos possíveis, obter conhecimento detalhado de quem é a comunidade de confiança, de tal modo que notificações possam ser enviadas

somente a este conjunto, se o comprometimento ocorrer. Isto é extremamente difícil, se não impossível, num ambiente de Internet;

- Armazenar a chave pública confiável como um certificado no domínio local dos parceiros de confiança, suportar a publicação periódica de uma LRA, e encorajar que o software relevante à ICP dos parceiros, realize a verificação da LRA. Isto pode ajudar a minimizar o dano porque a confiança na chave comprometida pode ser cancelada de forma automática, sem a intervenção das entidades finais. Este mecanismo é mais adequado a ambientes que verificam o status do certificado via listas de revogação, mas também pode ser apropriado para ambientes nos quais o status é verificado via outros servidores autorizados (por exemplo, usando OCSP ou outros protocolos similares);
- Tem um período de validade razoável para o par de chaves de assinatura. Um chave comprometida depois de 10 anos de uso tipicamente resulta em mais danos que uma chave comprometida após um ano; contudo, deve-se analisar os custos de uma troca freqüente de chaves;
- Implementar um mecanismo controlado e automatizado de mudança de chave da AC. Este mecanismo, como o PKIX-CMP (RFC 2510) pode ajudar a minimizar o dano causado por tal comprometimento de duas formas. Primeiramente, torna-se transparente aos parceiros, em alguns ambientes, diminuindo assim o tempo de aceitação dos certificados da AC. Em segundo lugar, permite uma fase de passagem para a comunidade para a próxima chave da AC, de tal modo que a qualquer tempo o número de entidades afetadas pelo comprometimento da chave da AC seja menor que a comunidade de confiança completa.

É altamente recomendado que os administradores da AC planejam criteriosamente as atitudes a serem tomadas em caso de comprometimento da chave da AC.

Recuperação

Se a chave privada de uma AC foi comprometida, não há atalhos para o processo de recuperação. Nada mais assinado por aquela chave pode ser digno de confiança, incluindo certificados, LRCs e LRAs (exceto o caso notado anteriormente). Caso esta chave de assinatura tenha sido usado para outros propósitos, tais como autenticação de mensagens de protocolos, ou comandos de políticas e práticas, estas também não podem ser mais confiáveis.

O caminho completo para a recuperação em caso de comprometimento de uma chave de uma AC é: a ICP deve ser reinicializada, essencialmente desde o início, para toda a comunidade de confiança afetada. Ou seja, um novo par de chaves de assinatura deve ser gerado, e algum processo não automatizado, confiável, deve ser usado para instalar uma cópia da chave pública no ambiente local de todas as entidades relevantes à ICP. Nenhum mecanismo envolvendo o uso da chave comprometida pode ser digno de confiança para facilitar, simplificar ou contornar este processo. A ICP deve ser reconstruída tal como se ela jamais tivesse existido para este conjunto de entidades.

Observações adicionais

O comprometimento da chave privada de uma AC traz consigo seríssimas conseqüências de segurança. Para aqueles que possuem diretamente uma cópia da chave pública correspondente, como um fator de confiabilidade, é um verdadeiro desastre operacional. Para os que indiretamente são membros da comunidade de confiança através de certificação cruzada, o

dano é, de algum modo, menos extensivo. Isto se deve ao fato de que a revogação do certificado cruzado pela AC confiável cancela automática e imediatamente qualquer confiança adicional na AC comprometida e, por extensão, nos certificados de sua comunidade. Para ambos os conjuntos de entidades (comunidades diretas e indiretas) tudo o que foi assinado pela chave comprometida é imediatamente inválido, a menos que seu uso tenha a corroboração de servidores de temporização confiáveis. Neste caso, deve ser provado, para todos os efeitos, precisamente que assinaturas foram criadas antes do comprometimento. Estas ações ilustram a importância de uma preparação cuidadosa pelos administradores da AC antes da implementação da ICP.

O Arcabouço Legal (ICP-Brasil)

Observando a evolução da tecnologia de ICPs e sua utilização, como meio seguro, para a garantia dos serviços listados anteriormente, como autenticação, integridade e confidencialidade, o governo federal brasileiro instituiu, através do Decreto No. 3505, de 13 de junho de 2000, a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal. Entre os seus pressupostos, figura o de "assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição" (Art. 1°, Inciso I).

Em seu artigo 6° , o Decreto instituiu o Comitê Gestor da Segurança da Informação, órgão interministerial com a atribuição de "assessorar a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos neste Decreto".

Em 5 de setembro de 2000, através do Decreto no. 3587, estabelecia-se normas para a Infra-estrutura de Chaves Públicas do Poder Executivo Federal – ICP-Gov.

Em 18 de julho de 2001, o Decreto no. 3.872 dispunha sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas brasileira – CG ICP-Brasil.

A Medida Provisória no. 2200-2, de 24 de agosto de 2001, institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil. Eis seu Art. 1° : "Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras."

O Decreto no. 3996, de 31 de outubro de 2001, revoga o Decreto no. 3587, e estabelece em seu Art. 2° que "somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital."

A Resolução no. 1 do Comitê Gestor da ICP-Brasil, de 25 de setembro de 2001, aprova a Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil, que é o Instituto Nacional de Tecnologia da Informação, órgão do Ministério da Ciência e Tecnologia.

A Resolução no. 2 do Comitê Gestor da ICP-Brasil, da mesma data, aprova a Política de Segurança da ICP-Brasil, abrangendo requisitos de segurança humana, física, lógica, e dos recursos criptográficos.

A Resolução no. 6 do mesmo Comitê, de 22 de novembro de 2001, aprova os critérios e procedimentos de credenciamento dos integrantes da ICP-Brasil.

O Decreto no. 4036, de 28 de novembro de 2001, vincula o Instituto Nacional de Tecnologia da Informação diretamente à Presidência da República.

Em 30 de dezembro de 2001 foi gerado o par de chaves criptográficas e o respectivo certificado da AC Raiz da ICP-Brasil, nas instalações do SERPRO, no Rio de Janeiro. A partir desta data, portanto, é possível emitir certificados para as AC que desejarem compor a ICP-Brasil.

A Resolução no. 7 do mesmo Comitê, de 12 de dezembro de 2001, aprova os requisitos mínimos para políticas de certificado na ICP-Brasil.

A Resolução no. 11 do mesmo Comitê, de 14 de fevereiro de 2002, altera os requisitos mínimos para as políticas de certificado na ICP-Brasil, a declaração de práticas de certificação da AC Raiz da ICP-Brasil e delega novas atribuições à AC Raiz da ICP-Brasil, tais como aprovar políticas de certificados e regras de certificação das AC, e credenciar e autorizar o funcionamento das AC e das AR.

Por fim, a Resolução no. 11, da mesma data, estabelece regras processuais para credenciamento na ICP-Brasil.

Referências bibliográficas

[SCH 96] Schneier, Bruce. *Applied Cryptography*. John Wiley and Sons. 1996.

Menezes, A, Oorschot, P. Van, & Vanstone, S. *Handbook of applied cryprography*. CRC Press. 1996.

Adams, Carlisle & Lloyd, Steve. *Understanding public-key infrastructure*. McMillan Technical Publishing. 1999.