6

Modes of Data Insertion and Acquisition

6.1 Physical Possession of the Computer

The fact that physical possession of a computer by an investigator allows that investigator to search for all evidence in the computer is self-evident and needs no further elaboration. It is the basic premise behind computer forensics as practiced by law enforcement. If there is any unencrypted information left behind in the confiscated data storage media, and if the forensics investigation is thorough enough, that information will be found. Physical possession does not have to be clandestine; when computers are taken to be serviced, service technicians have full access to them.

6.2 Physical Access to the Computer

Physical access to a targeted computer is just as good as full possession of it, if such access allows one to make a full magnetic copy of the computer's hard disk(s). In legal proceedings, it must be shown that the disk(s) copied could not have been contaminated by the copying process, and the disks must be removed from the targeted computer and placed in another one over which the forensics investigator has full control. Safeback (see Section 3.3.2) is one of the standard pieces of software used to make a track-by-track and sector-by-sector copy of a targeted disk onto another disk of equal or greater capacity.

If the purpose of the forensics investigation is to collect data without having to show it in court, then disks can be copied even without removal from a computer, as long as the investigator has taken steps to ensure that there is no booby-trapped software running that would delete or modify disk(s) that are copied by a stranger.

Similarly, physical access can allow for surreptitious data collection, by law enforcement or anyone else. The commercial sector is full of devices that transmit information fed into them. An interceptor who has somehow obtained physical access to someone else's premises (or just to that person's computer, such as when it was taken in for repair) could elect to combine a data-interception device with a small radio transmitter that transmits the intercepted data out to a receiver.

The only limits as to how to send out the data that has been collected from a targeted computer are one's imagination, nerve, and pocketbook.

6.3 Keystroke-Capturing Hardware Device

A commercial device is openly available worldwide from a New Zealand firm, KeyGhost Ltd. (http://www.keyghost.com/); surreptitiously placed on the target computer, it looks like a small adapter on the cable connecting the keyboard to the computer. This device requires no external power (and hence lasts indefinitely) and no software installation (and hence cannot be detected by any software). Numerous versions are available, as shown in Figure 6.1. Figure 6.2 depicts the keystroke-capturing device itself, with adapters for different computers. It comes with the requisite adapters and manual "out of the box," for installation by nonspecialists, as shown in Figure 6.3.

The high-end models, which sell for around $250, can store 500,000 keystrokes, or about 80,000 words (approximately the size of a 160-page paperback book). Special versions of the device can capture and store one to four million keystrokes. An upcoming KeyGhost mini will look like a normal keyboard extension cable.

For an extra $50 or $60 more, one can buy a standard or Microsoft Natural keyboard with the device built inside it, thereby making it totally invisible, as shown in Figure 6.4.

The captured keystrokes are stored in the device in 128-bit encrypted form (i.e., unbreakable for all practical purposes). Unlike the software-based keystroke-capturing commercial and freeware products discussed in Section 6.4, a hardware-based keystroke capture works even if one boots a computer from a floppy disk, and is independent of the operating system used. It can

Model	Capacity	Ghost Playback	Encryption	Fast Download Adapter	Casing
Keyghost II Professional SE	2,000,000 Keystrokes	Yes	128 bit	Yes	EMC Balun
Keyghost II Professional	500,000 Keystrokes	Yes	128 bit	Yes	EMC Balun
Keyghost II Standard	97,000 Keystrokes	Yes	None	No	EMC Balun
Keyghost Mini Covert	120,000 Keystrokes	No	N/A	Yes	PS-2 Plug
Keyghost II Security Keyboard (Pro)	500,000 Keystrokes	Yes	128 bit	Yes	Keyboard
Keyghost II Security Keyboard (Std)	97,000 Keystrokes	Yes	None	No	Keyboard

Figure 6.1 Versions of KeyGhost keystroke-capturing device. (Courtesy of KeyGhost Ltd.)

Figure 6.2 KeyGhost device with adapters.(Courtesy of KeyGhost Ltd.)

Figure 6.3 Installation of KeyGhost device. (Courtesy of KeyGhost Ltd.)

be placed on password-protected computers without having to defeat such passwords. In fact, a device such as this can also capture the initial BIOS

Figure 6.4 Invisibly modified keyboard to capture keystrokes. (Courtesy of KeyGhost Ltd.)

password optionally used by any computer. If the entire data storage area of the device is filled up unretrieved, it will proceed to overwrite the oldest stored data.

The information captured by the device can be retrieved by anyone who can get physical access to the computer by entering the appropriate installer-selected password; since this can be up to 12 characters long, it is highly unlikely that such passwords can be typed accidentally. Alternately, the device itself (cable or keyboard) can be swapped with a normal one that looks the same, and taken to another computer where its contents can be retrieved at leisure.

6.4 Keystroke-Recording Software

Numerous software packages are openly available on the Internet, some for a fee and many for free, that record all keystrokes. Those listed here are downloadable from http://www.cotse.com/winnt.htm:

- Playback.zip
- Win95pwgrabber.zip
- Keycopy V.1.01
- Keylogger V.1.5
- 9x_int09.zip
- achtung.zip

Other openly available keystroke-logging software includes:

- **Internet Tracker** 2.1. Intended to track stolen computers; reports on a computer's activities by e-mail.
- **The Investigator** 3.0. This records all keystrokes and sends the data out to whomever the surreptitious installer specified. It is sold for $99 by "WinWhatWhere," and is popular with employers for monitoring employees. According to CMP's Tech Web, this software has been purchased, among others, by the U.S. State Department, the U.S. Mint in Denver, Exxon, Delta Airlines, the accounting firm Ernst and Young, the U.S. Department of Veteran Affairs, and Lockheed Martin.

The following software-based keystroke-capturers can be obtained from http://winfiles/cnet.com/apps/98/access-control.html.

- **Gotyour Keystrokes** (freeware). Developed as a tool for parental control.
- **SpyAgent Professional** (shareware, $34.95). Powerful full-featured software.
- **NetSpy** (shareware, $19.95). Also allows the snoop to see what Web sites were accessed by the targeted computer, as well as e-mail, even if it is subsequently deleted. Currently supports Netscape Navigator, Internet Explorer, AOL, and Prodigy.
- **Desktop Detective** (shareware, $29). Full-featured snooping utility.
- **Spytech Shadow** (shareware, $29.95). Emphasizes visual screen monitoring rather than text capture and records full visual screens every few seconds.

Additionally, one can purchase software such as "KeyKey," from http://www.keykey.com/index1.html and from http://cyberdetective.net/keykey.htm. For Windows 95/98, NT, and 2000, this product asserts that it hides itself from antimonitoring software and records date/time stamps; it sells for $19.95. KeyKey's versatility is evident from Figure 6.5, which shows the reporting options available to the surreptitious installer of that software; notice that these options include e-mailing of the captured keystrokes.

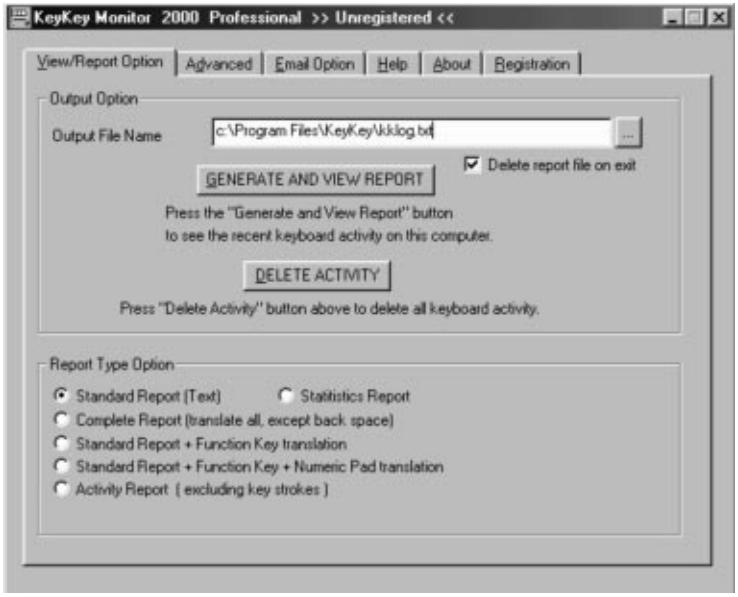

Figure 6.5 KeyKey's keystroke-capturing reporting options. (Courtesy of Mikko Technology.)

KeyKey's "professional" version comes with a Screen Capture package; as this name suggests, it surreptitiously captures, stores, and can transmit what someone is viewing on the screen as well, as shown in Figure 6.6. Notice that the options include capturing screenfuls at preset intervals of time, or when the mouse or keyboard is used in any mode defined by the surreptitious installer.

6.5 Internet or Network Connections

A serious security threat results from merely being on-line. Unless one has taken drastic steps to defend against a wide assortment of hacking attacks (see Chapters 8 through 14), one is highly likely to become the target of trolling hackers who delight in identifying and exploiting security weaknesses of anyone who stays on-line long enough. Such attacks can be minimized by:

- *Using a good firewall.* (See Section 12.16.)

Figure 6.6 KeyKey screen-capturing options. (Courtesy of Mikko Technology.)

- *Not staying on-line for long*. Hacking attacks probe one's weaknesses based on one's dynamically assigned (meaning that it changes every time one goes on-line) Internet Protocol (IP) address. An IP address is the unique identifying address of anyone connected to the Internet; it is the equivalent of one's telephone number. Since there are more Internet users than there are IP addresses, an Internet service provider has a pool of such IP addresses from which it selects at random to assign to each user when that user goes on-line; when this user goes off-line, that IP address is assigned to someone else. The longer one stays with a single IP address, the longer a hacker has to probe for weaknesses. Users of high-speed connections (cable modems and xDSL lines) would be well advised to disconnect their computers from the network when not actually using them.
- *Using virus/Trojan/worm protection software* and keeping it current; this means checking for updates once a day or, if one uses a computer sparingly, prior to each new use.

Unless a user has taken drastic and current measures to prevent access to his or her computer by others on a network or the Internet, there is a vast

repertoire of ways whereby a knowledgeable person can extract data from a user's computer while that user is on-line. The extent of what can be remotely extracted in this manner ranges from literally everything on one's hard disk to nothing, depending on what protective measures have been taken along the lines of those described in Part II of this book.

6.5.1 Internet Service Providers or ISP Security Breaches

The primary security threat to a computer connected to the Internet is not the malicious remote Web site or the malicious remote hacker—although both of these dangers are very real—but one's own Internet service provider. The ISP is always in a position to know what one does on-line, who one connects to, the content of incoming and outgoing e-mail, who one communicates with and when, and so on. The only exceptions are:

- When a user elects to connect to remote Web sites with SSL encryption (see Section 12.7.1), which provides end-to-end encryption between the user and such sites; the ISP is incapable of knowing what data is moving back and forth.
- When a user elects to use a virtual private network (VPN) connection to the remote site, as per Section 12.4. Comments made above about SSL encryption apply here as well.
- When a user elects to use encryption to hide the contents of e-mail and attachments. This still does not hide the "from whom" and "to whom" information, unless the user has also elected to use multiple concatenated remailers (see Section 11.5.2); in this case, the ISP knows that a remailer is being used.

While the methods above do provide the protection shown, they also raise the user's profile in the eyes of the suspicious ISP, as someone who is "hiding something."

If one wants to "have cake and eat it too," then steganography is the only way out (see Section 14.5), as long as it is employed judiciously so that its use is not alerting.

It is not "paranoia" to assume that an ISP has a financial interest in a user's on-line activities: A company called Predictive Networks is promoting a scheme that would pay ISPs to track users' every move on the Internet so as to sell detailed profiles to numerous buyers who want to target their

advertising. (See http://home.mpinet.net/pilobilus/CS01.html, http://www.vortex.com/privacy/priv.09.13, and http://www.predictivenetworks.com/.)

6.5.2 Telephone Taps

Anything that an ISP can see can also be seen through a tap on the communications medium used by an individual to connect to the Internet, be that a telephone line, a cable modem, an xDSL line, or a wireless link; most any wireless link (e.g., cellular phone, Ricochet modem) eventually becomes a wired connection, more practical for someone to intercept.

6.5.3 Remote Web Sites

The litany of ways whereby remote Web sites can extract information from one's computer on-line is almost endless. (See Chapters 10 through 14 for protective measures.) Rather than enumerating the vast number of such threats, Chapters 10 through 14 approach the topic from the perspective of wholesale negation of them.

"Cookies" (see Chapter 10) have been correctly blamed for allowing Web sites that the individual accesses to track the individual's Web-browsing habits. (A "cookie" is simply a small amount of data sent by the accessed Web site to the individual's computer and stored in that computer; such data is supposed to be readable only by the site that sent it, but in fact can be read by any Web site that elects to do so.)

In fact, a Web site does not need to store anything at all in an individual's computer to track that individual's browsing habits. As a user accesses any Web page, that site has to know the user's IP address in order to send the information requested. If that site elects to record the IP address for posterity, then it can easily tell if a user has visited that site before. This is only true for users with fixed IP addresses (such as most users with xDSL or cable modem access who have not deployed protective measures) but is not true for dial-up users because such users get a different IP address every time they dial up their ISP to connect to the Internet.

The most recent culprit is a device known as CueCat, which has been mailed gratis to numerous individuals in the United States. CueCat is a digital bar-code scanner promoted by a Denver, Colorado, organization, which has a personal tracking feature within it [1]. The idea is that individuals can scan the bar codes of items in print and then are automatically linked to

assorted Web pages. The problem is that such devices seem to be individually identifiable. Don't use them.

Technical information on how to disable the individually identifiable serial number of these devices is available on-line at http://www.air-soldier.com/~cuecat/.

It is just as easy for a remote entity to retrieve information from one's computer on-line as it is to insert files in it. Given that mere possession of some kinds of material by individuals is strictly illegal in some regimes (e.g., subversive files, bomb-making files, files marked as classified, and even erotic imagery in the case of most regimes), one should be particularly careful about the possibility that incriminating "evidence" may find its way into one's computer under some circumstances. Similarly, defense attorneys must also be aware of this possibility. This incriminating "evidence" can be intentionally inserted by a remote party; it can also be unknowingly received by an innocent user who never solicited it, in the following ways:

- One is accessing an Internet Web site and either mistypes the URL or the correct URL gets one to the wrong site (say, a pornographic one) as a result of domain server name (DNS)[1] problems.
- One is accessing a legitimate Internet site on the Web which is also supported by advertising revenue (as most are today) obtained by flashing unsolicited images and "windows" on the user's screen; those images end up getting saved on the user's computer despite no active "clicking" or other act by the user. An overzealous law enforcer can find this as "evidence of possessing illegal imagery"; unless the defense counsel is well versed on this issue, a nontechnical jury (or judge) will likely convict a totally innocent person.

6.6 Acquisitive Software

Numerous software packages can capture, store, and forward a targeted computer's on-line and off-line activities. A small sampling of such software is provided here.

1. DNS servers are the telephone directories of the Internet. When one types in a Web address—http://www.somename.com/—a DNS server is queried to produce the corresponding IP address (e.g., 123.456.789.012) for that name. Time and again, hackers have managed to poison select DNS servers so as to deny access to numerous Web sites.

- **Mom** (http://www.avsweb.com/mom/) tracks a targeted individual's on-line activities.
- **DIRT.** Data Interception by Remote Transmission (DIRT) is a tool that claims to provide remote monitoring of one or more targeted computers without the need for physical access. It is sold by Codex Data Systems (http://www.codexdatasystems.com/menu.html). According to the company's Web site, "All that someone with DIRT needs to know is your e-mail address. Period. All he has to do is send you an e-mail with the imbedded DIRT-Trojan Horse and he is home free, and you are a clueless victim."
- **NoKnock E-Warrant.** Also by Codex Data Systems, this product asserts that it can "execute judicial search warrants by stealth via the Internet" for the purposes of "remotely searching a target hard drive and comparing results with known databases."
- **Investigator.** Put out by WinWhatWhere (http://winwhatwhere.com/), this product offers a broad range of capabilities including keystroke monitoring and Internet tracking.
- **SilentRunner.** Offered by Raytheon (Lexington, Massachusetts), this product is intended for network monitoring. The program uses algorithms to analyze communications patterns and turns its analysis into three-dimensional pictures.
- **Silent Guard.** Adavi advertises this product as the "premier surveillance software that allows a single user to monitor keystrokes and Internet traffic for later review." This program can monitor up to 49 computers in real time from a single screen and even provide alarms to the person doing the monitoring "when users reach objectionable Web sites or inappropriate text content based on a dictionary of the user's choice."

6.6.1 Spyware and Adware

Most individuals are unaware of the monetary value of their names and buying habits. Supermarkets in the United States have long been offering substantial discounts to shoppers who agree to fill out a form with their name, address, phone number, and e-mail address. Similarly, the many "free" ISPs are not free at all: Instead of getting paid in cash by users, they get paid in terms of the monetary value of users' names and Web-browsing habits; this

information is, in turn, converted into cash by the commercial advertisers to whom it is sold.

A lot of free software (and some commercial for-pay software) makers have also learned the commercial value of software users' names and choices (measured in terms of what other software exists in a user's computer, as well as the user's on-line habits). The moment such software is installed in an unsuspecting user's computer, it starts collecting and relaying this data; this often continues even if that program is never used, and even if it is uninstalled—hence the epithet "spyware."

A current list of software reputed to offer this capability can be found at sites such as http://home.att.net/~willowbrookemill/spylist.pdf, http://www.grc.com/, http://www.alphalink.com.au/~johnf/dspypdf.html, http://www.infoforce.qc.ca/spyware/, and elsewhere. The interested reader is encouraged to check the Usenet forum ALT.PRIVACY.SPYWARE for the latest information on the topic.

TSADBOT, by Conducent, which has since gone out of business, is an example of the type of Trojan horse that can enter an individual's system attached to certain "free" software that the individual has installed. The information is from http://cexx.org/tsadbot.htm. It makes multiple connections to Conducent ad servers, including adsdl.conducent.com and redirects.conducent.com (various ports). Its use of proxy service prevents NETSTAT and similar network tools from disclosing actual addresses that it connects to (they appear in the form of ADS*:portnumber).

TSADBOT is installed as a Windows service when certain software is installed, most notably new versions of PKZip. Several sources actually list this program under "viruses," and it is not difficult to see why. It is secretly loaded onto computer systems when the user installs (or merely attempts to install) completely unrelated software; it makes clandestine network connections without the user's knowledge; it persists even after the software it came with has been uninstalled; and it is very difficult to remove.

Once installed, the TSADBOT program is loaded every time Windows starts and runs invisibly in the background until the computer is shut down. It connects to the Internet and downloads ads, whether the advertising-supported application is running or not, and implements an unauthorized proxy server on the user's system that disguises the adware's network connections. AdGateway (demographic/behavioral) "profiles" are stored in encrypted files on the user's system, and may be transmitted by the TSADBOT software. The TSADBOT software accesses the user's browser cache and history (list of sites one has visited) for purposes unknown, and

may use this information in the creation of behavioral profiles or transmit this information.

Once installed, TSADBOT (like many adwares) is very difficult to remove. If deleted, it will often forcibly reinstall itself. In addition, it remains on one's system and continues to monitor one's viewing habits, even after the associated application has been uninstalled. This means that if one installs a "free" version of PKZip or a similar application, runs it once, and finds out that it is powered by adware and immediately uninstalls it, the TSADBOT process remains on one's system and secretly continues to perform its unwanted functions.

The *Risks Digest* (Volume 20, Issue 65) provides information about another "feature" of TSADBOT:

> [A]n even worse fate occurs if the AdBot is thwarted in its attempts to connect to Conducent by a firewall or other controls. It starts to attempt to connect continually, about 10 times/second causing a huge load on local network facilities. If it can't connect even then, it tries to connect using Telnet and other ports with the background AdBot retrying the HTTP connects after several hours.

To a privacy-minded person, the most disturbing aspect of this program is what it does with one's Web browser history. Just as disturbing are the statements made on the Web site responsible for TSADBOT:

> By collecting valuable user data and marketing new and existing software titles to dedicated users, publishers can drive retail sales of specific titles. Conducent offers Advertisers the unique opportunity to reach specific software users in highly targeted categories.

6.6.1.1 "Fixes" Against Adware and Spyware

One easy "fix" that worked in the past was for the individual to download Steve Gibson's OptOut program from http://grc.com/files/optout.exe. This product is no longer current. A better product, "Ad-aware," is available freely from http://www.lavasoft.de/.

Some programs that install spyware will refuse to run if one removes the spyware functionality; Go!Zilla is one such example. Some will keep reinstalling the spyware function; to get rid of it, one must remove the software that continues to install it.

A user should determine if a new piece of software in his or her computer has any reason to be accessing the Internet; a good firewall (see

Section 12.16) will alert the user most of the time, but not all of the time[2] if a program is trying to access the Internet, at which time a user can permit or not permit that to happen.

One can search one's computer for such telltale file names as "ad.dll," "advert.dll," and so forth. Rename them; if everything still works, delete them. In particular, look for and remove any of the following:

Tsadbot.exe[3] (usually installed as a Windows "service" in software, such as in new versions of PKZip)

Dssagent.exe

Adimage.dll

Amcis.dll

Amcis2.dll

Anadsc.ocx

Anadscb.ocx

Htmdeng.exe

Ipcclient.dll

Msipcsv.exe

Tfde.dll

Tsad.dll

---

2. If a piece of software has installed the capability in one's computer to access the Internet through valid ports and through other valid software (e.g., using port 80 of one's Web browser while that browser is being used by the user anyway), then the user will be oblivious to this, and no firewall will catch it. About the only way to catch such an unauthorized hijacking of one's computer and software is through the use of a "packet sniffer," which actually looks at and displays all data entering and leaving one's computer; WinDump is one such product, and can be obtained, for example, from http://netgroup-serv.polito.it/windump/.

3. TSABOT connects to the Internet without a user's knowledge, downloads ads, sets up a proxy server on one's own system so as to disguise this adware program's network connections, accesses the user's history of Web sites visited and also the Web browser's cache of saved documents, stores profiles in encrypted form in the user's computer, and transmits information to Conducent. TSABOT stays in one's system and continues to function even after the software that installed it, such as PKZip, has been removed. To delete it, one must do so from within DOS, because the file reports as being "in use" if one tries to delete it from inside Windows. Also, Run/REGEDIT and look for any reference to TSABOT and delete it and do not run the program that installed it in the first place (such as PKZip). Finally, if you have a personal firewall that allows you to block access to particular domains, block access to all Conducent domains.

Vcpdll.dll

FlexActv.dll

Look in the Startup folder for any inexplicable entries and remove them. Sometimes, adware/spyware will reinstall entries in the Startup folder; in this case, assuming that one knows what sequence of letters for which to look, one can look in the registry for that sequence and delete those references. *Caution:* Do not edit the registry unless you know what you are doing (see Chapter 4).

6.6.2 Other Unauthorized "Backdoor Santas"

6.6.2.1 Netscape Navigator/Communicator

Do not use Netscape's Smart Update. It has been shown to report to Netscape. Go into Edit/Preferences/Advanced/SmartUpdate and uncheck it.

Unless you are particularly fond of AOL Instant Messenger in Netscape Navigator/Communicator, remove it as follows:

1. Go to C:/Program Files/Netscape/Users/ and remove the shortcut for AOL Instant Messenger ("launch.aim") for each and every profile you have. Do not run Netscape until you complete the additional steps below; otherwise, the program will reinsert the shortcuts just deleted.
2. Go to Search/Find/Folders and enter "AOL" and, separately later, "AIM." Delete any folder identified with either name.
3. Run REGEDIT and search for the string "AOL" and, separately, "AIM." Delete every entry identified that is clearly referring to the AOL Instant Messenger. *Caution:* Ensure that the entry being deleted is indeed referring to AOL's Instant Messenger before deleting it. See Section 4.4 about concerns that must be addressed when editing the registry.
4. Reboot.
5. Double-click on the Netscape icon and make sure that everything is working properly.

6.6.2.2 Registration Wizards

Do not use registration wizards. Time and again, companies—including very reputable ones—have been caught using the on-line registration process to

send to the software maker a lot more than the registration information, such as a digest of what is in one's hard disk.

6.6.2.3 Eudora 3.0

All variants of Eudora 3.0, namely the so-called Lite, the fully paid and the ad supported—as well as many other software products today—have an unfortunate feature whereby the software regularly "calls home" (i.e., connects to the Eudora servers without notifying the user). The makers of Eudora (and other software makers) assert that this is done solely to check if a newer version of the software has been released; the fact remains, however, that the Eudora server gets notified on a regular basis whenever a user uses his or her copy of the software, and this happens without the user's knowledge. This feature can be and should be disabled as shown in Section 11.3.3.

6.6.2.4 Microsoft's WebCheck

Microsoft's WebCheck manages subscriptions and user profiles for Internet Explorer versions 4 and 5. (If you don't use subscriptions, you don't need it.) This parasite is run by the registry using the entry

> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunBrowserWebCheck="loadwc.exe"

> *Caution:* Removing this line causes endless subsequent errors.

6.6.2.5 PKWARE

Like Microsoft's WebCheck, PKWARE also installs a parasite, which allows advertisements to be carried inside zip files. It is launched by the registry with the entry

> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunTimeSinkAdClient="C:\ProgramFiles\TimeSink\AdGateway\TSADBOT.EXE

6.6.2.6 HP Registration

HP Registration often installs a registration parasite if one does not register the product. It takes up 6–20 MB and runs remind32.dll, which nags the user to register. Remind32.dll is executed from Start/Programs/Startup.

6.6.2.7 Boreland C++ 5.0

Boreland C++ 5.0 (DOS) also installs a registration parasite that takes up 1 MB of disk space and is invoked by the following line in the win.ini file:

```
[windows]load C:\BC5\PIPELINE\remind.exe
```

Clearly, one can remove both the above line and the remind.exe file itself.

6.6.2.8 Microsoft Office 2000 Script Editor

Microsoft's Office 2000 Script Editor allows the user the option of installing the Machine Debug Manager (mdm.exe) through the registry entry

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Cur-
rentVersion\RunServices
```

The problem with this feature is that it creates temporary files every time that one boots the computer, and never deletes them, thereby posing a security threat.

6.7 Van Eck Radiation

Information in this section is based entirely and exclusively on the openly available sources identified herein.

6.7.1 General

In 1985, Wim van Eck published a paper called "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" [2]. Electromagnetic radiation as a computer security risk was mentioned in the open literature as early as 1967 [3]. Since then, numerous articles on the subject have appeared on the Internet, such as the ones shown in the Selected Bibliography on Van Eck Radiation at the end of this chapter. Additionally, there are numerous openly available scientific documents on the subject, also shown in the Selected Bibliography.

Because of the obvious security concern with unintended emanations from electronic equipment used in sensitive government activities, standards and procedures have been developed for the purpose of reducing these emanations to sufficiently low levels. These standards and procedures are

collectively known as "TEMPEST." TEMPEST is an acronym for Transient Electromagnetic Pulse Emanation Standard.

In the United Kingdom, where TV fees must be paid on a regular basis, vans are routinely deployed that are equipped with means to detect the oscillators of TV sets and compare them against the list of those who have paid for operating a TV. In fact, according to the University of Cambridge's Ross Anderson, unpaid TV fees are a main reason that women in the United Kingdom end up in prison if they cannot pay the £1,000 fine when caught for this offense.

"Data Security by Design," an article by George R. Wilson (http://jya.com/datasec.htm), asserts that such emissions can be picked up "as far away as half a mile" using "a broad band radio scanner, a good antenna and a TV set—all available at electronic stores such as Radio Shack for a few hundred dollars."

According to Kuhn and Anderson [4]:

- "[P]ower and ground connections can also leak high frequency information."
- "Yet another risk comes from 'active attacks' [5].... an attacker who knows the resonant frequency of (say) a PC's keyboard cable can irradiate it with this frequency and then detect keypress codes in the retransmitted signal."
- "A reader of an early version of this paper reported that he was able to get data signals out of a U.S. Tempest certified equipment by directing a 10 GHz microwave beam at it."
- "Smulders showed that even shielded RS-232 cables can often be eavesdropped at a distance" [6].

This same paper by Kuhn and Anderson [4] depicts test equipment alleged to be capable of doing such an interception, the DataSafe/ESL Model 400, by DataSafe Ltd. of Cheltenham, England, shown in Figure 6.7.

The tests performed by Kuhn and Anderson proved the feasibility of such interception, as evidenced from the two images in Figures 6.8 and 6.9, which depict the original screen of the computer being intercepted and the display at the eavesdropping site. It is noteworthy that the targeted computer is a laptop, which had long been considered safe from Van Eck radiation, in comparison to desktop computers.

Figure 6.7 DataSafe/ESL Model 400 laboratory equipment. (*Source:* Markus Kuhn, Computer Laboratory, University of Cambridge.)

Figure 6.8 Screen display of encryption key setup on targeted computer. (*Source:* Markus Kuhn, Computer Laboratory, University of Cambridge.)

In the conclusion of [4], Kuhn and Anderson state that "[t]hings will be made much worse by the arrival of cheap software radios...[which] will allow low-budget attackers to implement sophisticated TEMPEST attacks which were previously only possible with very expensive dedicated equipment." An image of the equipment used is provided in Figure 6.10.

See [4] for a list of openly available references on this topic.

More to the point, there are numerous commercial entities that sell equipment for this purpose. In October 1996, the Discovery Channel's *Cyberlife* show aired an interview with the CEO of a company called Codex

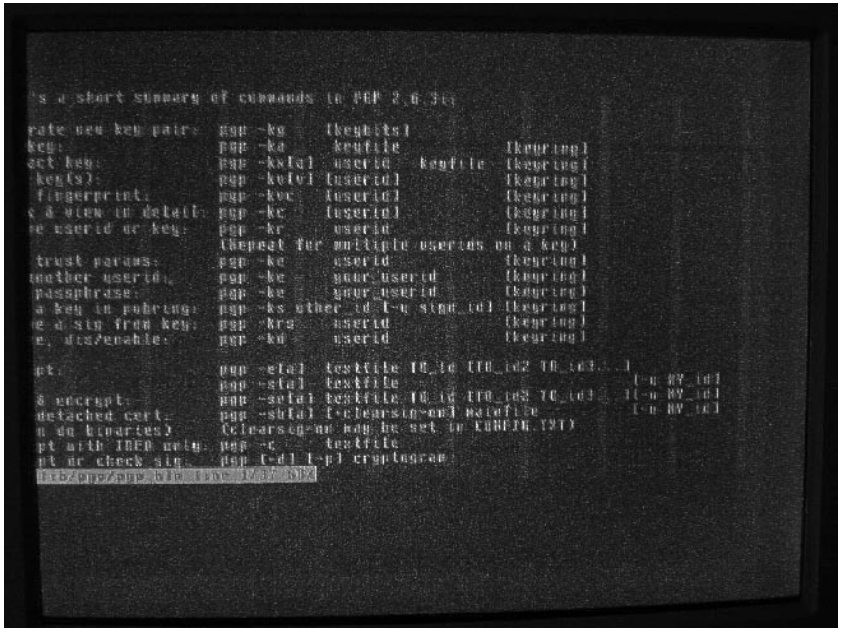

Figure 6.9 Intercepted image of encryption keys using Van Eck radiation. (*Source:* Markus Kuhn, Computer Laboratory, University of Cambridge.)

in which a demonstration was given of such interception. The Web site for Codex Data Systems (http://codexdatasystems.com/tempeav.html) depicts the system demonstrated.

A portable device sold by Codex (http://www.codexdatasystems.com/datascan.html) is claimed to be usable for ranges exceeding 1,000 yards. (According to Codex, "The DataScan manufactured by Codex captures the dominant video signal generated by any computer CRT screen and reconstructs it via a sophisticated antenna system and special receiver off-premises. Range has exceeded 1,000 yards under optimum conditions. The unit is entirely passive in nature. It does not allow the user to access the target computer but rather to monitor via radio wave what is displayed on the target computer's CRT screen every time the computer is operational.")

6.7.2 Protective Measures

A U.S. patent (US5297201) offers "A system for preventing remote detection of computer data from tempest signal emanations" (http://patent.womplex.ibm.com/details?patent_number=5297201). According to "Data Security

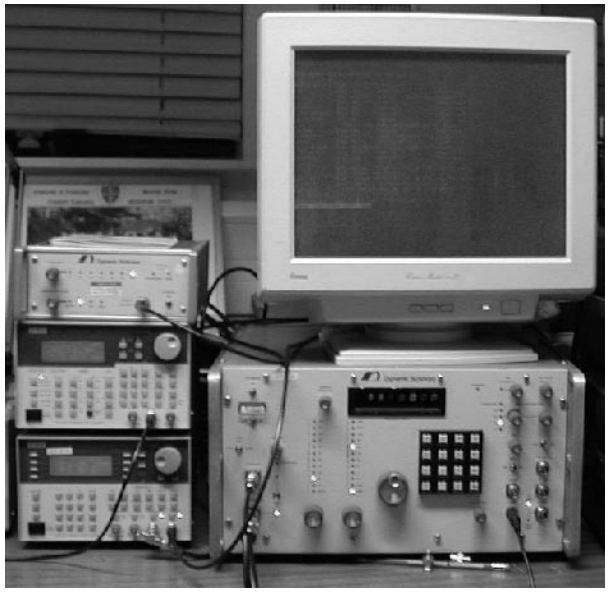

Figure 6.10 Standard laboratory equipment used for Van Eck interception by Kuhn and Anderson. (*Source:* Markus Kuhn, Computer Laboratory, University of Cambridge.)

by Design," by George R. Wilson (http://jya.com/datasec.htm), shielding from electromagnetic emanations is the protective measure one can deploy to thwart this threat to privacy. To this effect, there are numerous companies (such as TeckNit, http://www.tecknit.com/) that offer assorted EMI shielding products.

Similarly, "The TEMPEST Solution" (http://www.ionet.net/~everett/solution.html) suggests numerous steps one should take, such as reducing the length of cables, "using ferrite toroids and split beads on cables," and so on. The interested reader is referred to that article for the specifics. A publicly accessible document (http://www.cryptome.org/af-hb202d.htm) gives an allegedly official perspective on the topic.

An interesting protective scheme is, in fact, built into some openly available versions of the popular encryption software PGP: It offers one the option of using a fuzzy font that is claimed to be difficult to intercept through emanations. Similarly, ScramDisk (see Section 14.4) offers a "red screen mode" for one to enter the password in a manner that is claimed to defeat a TEMPEST attach; this only works for U.S. QWERTY keyboards and not for European

and Asian nonstandard keyboards (unless one uses only figures and numbers for the password). Similarly, one can download a "zero emission pad" freeware from DEMCOM, which makes the Steganos Security Suite software, at http://www.steganos.com/english/steganos/zep.htm. The example shown by that company's Web site of how it modifies the fonts that get displayed on the screen is shown in Figure 6.11.

An excellent reference for fonts that ostensibly defeat TEMPEST is at http://www.infowar.com/resource/99/resource_040599b_j.shtml, which also contains downloadable fonts at http://www.cl.cam.ac.uk/~mgk25/st-fonts.zip, which contains Soft TEMPEST filtered and anti-aliased versions of the Courier font, produced using the public domain X11 pixel font –adobe-courier-*-r-normal—40-386-75-75-m-0-iso8859-1. The two available fixed glyph cell sizes are 13×24 pixels and 8×13 pixels, in both medium (m) and bold (b) weight.

According to http://www.infowar.com/resource/99/resource_040599 b_j.shtml, "Since filtered fonts require successful eavesdroppers to come much closer to the target machine, they reduce the probability of a successful interception of confidential text considerably. They are therefore a valuable additional precaution that can be applied easily to maintain a reasonable level of communication and computer security. TEMPEST protection by filtered fonts and related techniques are in the process of being patented internationally."

The reader interested in preventing compromises of his or her privacy through this technology should read the patent description by Kuhn and Anderson, "Low Cost Countermeasures Against Compromising Computer Emanations," U.K. patent application no. 9801745.2, January 28, 1998.

Figure 6.11 Freeware fonts for protection from emanations interception. (Courtesy of DECOM GmbH.)

References

[1] Oslen, S., "Privacy Group Slams Web Tracking 'Cat'," CNET News.com, September 22, 2000, http://news.cnet.com/news/0-1005-200-2841044.html.

[2] Available at http://www.shmoo.com/tempest/emr.pdf, 1985.

[3] Highland, H. J., "Electromagnetic Radiation Revisited," *Computers and Security,* Vol. 5, 1986, pp. 85–93; 181–184.

[4] Anderson, R., and M. Kuhn, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," University of Cambridge Computer Laboratory, p. 126, full document at http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf.

[5] "Schutzmassnamen gegen Launschangriffe" (Protection Against Eavesdropping Attacks), Faltblaetter des BSI 5, Bonn: German Information Security Agency, 1996.

[6] Smulders, P., "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cable," *Computers and Security*, Vol. 9, 1990, pp. 53–58.

Selected Bibliography on Van Eck Radiation

Complete Unofficial TEMPEST Information Page, http://www.eskimo.com/~joelm/tempest.html.

"Electronic Eavesdropping Is Becoming Mere Child's Play," *New Scientist,* http://www.newscientist.com/ns/19991106/newsstory6.html.

"Electromagnetic Eavesdropping Machines for Christmas?" *Computers and Security*, Vol. 7, No. 4, 1988.

Jones, Frank, "Nowhere to Run...Nowhere to Hide: The Vulnerability of CRT's, CPU's and Peripherals to TEMPEST Monitoring in the Real World," CodexDataSystems, http://www.codexdatasystems.com/, 1996.

McLellan, V., *PC Week*, Vol. 4, March 10, 1987, p. 35(2).

Phrak44, http://www.shmoo.com/tempest/PHRACK44-11.

Russell, D., and G. T. Gangemi, Sr., *Computer Security Basics*, Sebastopol, CA: O'Reilly and Associates, 1991. (See specifically Chapter 10 on TEMPEST.)

Smulders, P., "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables," Department of Electronic Engineering, Eindhoven University of Technology, 1990.

"The Tempest Solution," http://www.ionet.net/~everett/solution.html.