4 Tools and Methods Used in Cybercrime

Learning Objectives

After reading this chapter, you will be able to:

- Understand about proxy servers and anonymizers.
- Learn about password cracking.
- Learn what keyloggers and Spywares do.
- Get an overview of virus and worms.
- Learn about Trojan Horses and backdoors.
- Understand what steganography is.
- Learn about DoS and DDoS attacks.
- Learn about SQL injection.
- Understand buffer overflow.
- Get an overview of wireless network hacking.

4.1 Introduction

In Chapter 2, we have learnt about how criminals/attackers plan cyberoffenses against an individual and/or against an organization. In Chapter 3, we have learnt how mobile technology plays an important role to launch cyberattacks. With this background, in this chapter, we will focus upon different forms of attacks through which attackers target the computer systems. There are various tools and techniques (see Box 4.1) and complex methodologies used to launch attacks against the target. Although discussing all of them is virtually impossible in a single chapter, yet still, we have provided an insight toward these techniques to enable the reader to understand how the computer is an indispensable tool for almost all cybercrimes. As the Internet and computer networks are integral parts of information systems, attackers have in-depth knowledge about the technology and/or they gain thorough knowledge about it. (See Section 10.4.2, Chapter 10 in CD.)

Network attack incidents reveal that attackers are often very systematic in launching their attacks (see Section 7.13, Chapter 7). The basic stages of an attack are described here to understand how an attacker can compromise a network here:

1. **Initial uncovering:** We have explained this in Chapter 2. Two steps are involved here. In the first step called as *reconnaissance*, the attacker gathers information, as much as possible, about the target by legitimate means – searching the information about the target on the Internet by Googling social networking websites and people finder websites. The information can also be gathered by surfing the public websites/searching news articles/press releases if the target is an organization/institute. In the second step, the attacker uncovers as much information as possible on the company's internal network, such as, Internet domain, machine names and the company's Internet Protocol (IP) address ranges. From prevention perspective, at this stage, it is really not possible to detect the attackers because they have done nothing illegal as yet and so their information requests are considered legitimate.

Box 4.1 Scareware, Malvertising, Clickjacking and Ransomware

1. **Scareware**: It comprises several classes of scam software with malicious payloads (explained in chapter 1), or of limited or no benefit, which are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety or the perception of a threat, generally directed at an unsuspecting user. Some forms of Spyware and Adware also use scareware tactics. Some websites display pop-up advertisement windows or banners with text such as: "Your computer may be infected with harmful Spyware programs. Immediate removal may be required. To scan, click 'Yes' below." These websites can go as far as saying that a user's job, career or marriage would be at risk. Webpages displaying such advertisements for such products are often considered as scareware. Serious scareware applications qualify as rogue software.
2. **Malvertising:** It is a malicious advertising – malware + advertising – an online criminal methodology that appears focused on the installation of unwanted or outright malicious software through the use of Internet advertising media networks, exchanges and other user-supplied content publishing services common to the social networking space. Cybercriminals attempt to distribute malware through advertising. Possible vectors of attack include Malicious Code hidden within an advertisement, embedded into a webpage or within software which is available for download.
3. **Clickjacking:** It is a malicious technique of tricking netizens into revealing confidential information and/or taking control of their system while clicking on seemingly innocuous webpages. Clickjacking takes the form of embedded code and/or script which is executed without netizen's knowledge Cybercriminals take the advantage of vulnerability across a variety of browsers and platforms to launch this type of attack, for example clicking on a button that appears to perform another function. The term "clickjacking" was coined by Jeremiah Grossman and Robert Hansen in 2008. The exploit is also known as *U*ser-*I*nterface (UI) redressing.
4. **Ransomware:** It is computer malware that holds a computer system, or the data it contains, hostage against its user by demanding a ransom for its restoration. It typically propagates as a conventional computer worm, entering a system through, for example, vulnerability in a network service or an E-Mail attachment. It may then
   - disable an essential system service or lock the display at system start-up and
   - encrypt some of the user's personal files.

   In both cases, the malware may extort by
   - prompting the user to enter a code obtainable only after wiring payment to the attacker or sending an SMS message and accruing a charge;
   - urging the user to buy a decryption or removal tool.

Sources: http://en.wikipedia.org/wiki/Scareware (10 January 10); http://www.anti-malvertising.com/ (10 January 10); http://en.wikipedia.org/wiki/Clickjacking (10 February 10); http://en.wikipedia.org/wiki/Ransomware_(malware) (10 January 10).

2. **Network probe:** At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool (see Table 2.2) is used to discover exactly which services are running on the target system. At this point, the attacker has still not done anything that would be considered as an abnormal activity on the network or anything that can be classified as an intrusion.
3. **Crossing the line toward electronic crime (E-crime):** Now the attacker is toward committing what is technically a "computer crime." He/she does this by exploiting possible holes on the target system. The attacker usually goes through several stages of exploits to gain access to the system. Certain programming errors can be used by attackers to compromise a system and are quite common in practice (see Table 4.1 for list of websites commonly browsed by attackers to obtain the information on the vulnerabilities). Exploits usually include vulnerabilities in common gateway interface (CGI) scripts or well-known buffer-overflow holes, but the easiest way to gain an entry is by checking for default login accounts with easily guessable (or empty) passwords. Once the attackers are able to access a user account without many privileges, they will attempt further exploits to get an administrator or "root" access. Root access is a Unix term

Table 4.1 | Websites and tools used to find the common vulnerabilities

Website	*Brief Description*
http://www.us-cert.gov/	US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). US-CERT also provides a way for citizens, businesses and other institutions to communicate and coordinate directly with the US government about cybersecurity. US-CERT publishes information about a variety of vulnerabilities under "US-CERT Vulnerabilities Notes."
http://cve.mitre.org/	Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures and free for public use. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.
http://secunia.com/	It has thousands of vulnerability lists that are updated periodically. It has vulnerability database and provides in-depth analysis about virus, worm alerts and software vulnerability.
http://www.hackerstorm.com/	This website was created for open-source vulnerability database (OSVBD) tool. Since then it has grown in popularity and provides additional information about penetration testing. The site is updated with whole bunch of news and alerts about vulnerability research.
http://www.hackerwatch.org/	It is an online community where Internet users can report and share information to block and identify security threats and unwanted traffic.
http://www.zone-h.org/	It reports on recent web attacks and cybercrimes and lists them on the website. One can view numerous defaced webpages and details about them.
http://www.milworm.com/	It contains day-wise information about exploits.
http://www.osvdb.org/	**OSVDB:** This is an open-source vulnerability database providing a large quantity of technical information and resources about thousands of vulnerabilities.
http://www.metasploit.com/	Metasploit is an open-source computer security project that provides information about security vulnerabilities and aids in penetration testing. Its most well-known subproject is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. The Metasploit Project is also well-known for antiforensic and evasion tools, some of which are built into the Metasploit Framework.
http://www.w00w00.org/files/LibExploit	LibExploit is a generic exploit creation library. It helps cybersecurity community when writing exploits to test vulnerability.
http://www.immunitysec.com/products-canvas.shtml	Canvas is a commercial vulnerability exploitation tool from Dave Aitel's ImmunitySec. It includes more than 150 exploits and also available are VisualSploit Plugin for drag and drop GUI exploit creation (optional).
http://www.coresecurity.com/content/core-impact-overview	Core Impact is widely considered to be the most powerful exploitation tool available. It sports a large, regularly updated database of professional exploits, and can do neat tricks such as exploiting one system and then establishing an encrypted tunnel through that system to reach and exploit other systems.

and is associated with the system privileges required to run all services and access all files on the system (readers are expected to have a basic familiarity with Unix-based systems). "Root" is basically an administrator or super-user access and grants them the privileges to do anything on the system.

4. **Capturing the network:** At this stage, the attacker attempts to "own" the network. The attacker gains a foothold in the internal network quickly and easily, by compromising low-priority target systems. The next step is to remove any evidence of the attack. The attacker will usually install a set of tools that replace existing files and services with Trojan files (*Trojan Horse* is further discussed in detail in this chapter) and services that have a backdoor password. There are a number of "hacking tools" which can clean up log files and remove any trace of an intrusion; most of the time, they are individual programs written by hackers. Such tools provide copies of system files that look and act like real thing, but in fact they provide the attacker a backdoor entry into the system and hide processes he/she might be running on that system and his/her user information. This allows the attacker to return to the system at will, which means that the attacker has "captured" the network. Once the attacker has gained access to one system, he/she will then repeat the process by using the system as a stepping stone to access other systems deeper within the network, as most networks have fewer defenses against attacks from internal sources.
5. **Grab the data:** Now that the attacker has "captured the network," he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites from your network, causing a potentially expensive and embarrassing situation for an individual and/or for an organization.
6. **Covering tracks:** This is the last step in any cyberattack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected. The attacker can remain undetected for long periods or use this phase either to start a fresh reconnaissance to a related target system or continued use of resources, removing evidence of hacking, avoiding legal action, etc. (See Table 4.2 to know tools used to cover tracks.)

During this entire process, the attacker takes optimum care to hide his/her identity (ID) from the first step itself. How is it possible is described in the next section.

Table 4.2 | Tools used to cover tracks

Sr. No.	*Website*	*Brief Description*
1	http://www.ibt.ku.dk/jesper/ELSave/	**ELSave:** It is a tool to save and/or clear an NT event log. ELSave is written by Jesper Lauritsen. The executable is available on the weblink, but source code is not available.
2	http://ntsecurity.nu/toolbox/winzapper/	**WinZapper:** This tool enables to erase event records selectively from the security log in Windows NT 4.0 and Windows 2000. This program corrupts the event logs, therefore, they must be cleared completely.
3	http://www.evidence-eliminator.com/	**Evidence eliminator**: It is simple and one of the top-quality professional PC cleaning program that is capable of defeating all known investigative Forensic Software. Evidence eliminator permanently wipes out evidence so that forensic analysis becomes impossible.
4	http://www.traceless.com/computer-forensics/	**Traceless**: It is a privacy cleaner for Internet explorer (IE) that can delete common Internet tracks, including history, cache, typed URLs, cookies, etc.

(*Continued*)

Table 4.2 | (*Continued*)

Sr. No.	*Website*	*Brief Description*
5	http://www.acesoft.net/	**Tracks Eraser Pro:** It deletes following history data: • Delete address bar history of IE, Netscape, AOL, Opera. • Delete cookies of IE, Netscape, AOL, Opera. • Delete Internet cache (temporary Internet files). • Delete Internet history files. • Delete Internet search history. • Delete history of autocomplete. • Delete IE plugins (selectable). • Delete index.dat file. • Delete history of start menu run box. • Delete history of start menu search box. • Delete windows temp files. • Delete history of open/save dialog box. • Empty recycle bin.

4.2 Proxy Servers and Anonymizers

Proxy server is a computer on a network which acts as an intermediary for connections with other computers on that network.

The attacker first connects to a proxy server and establishes a connection with the target system through existing connection with proxy. This enables an attacker to surf on the Web anonymously and/or hide the attack. A client connects to the proxy server and requests some services (such as a file, webpage, connection or other resource) available from a different server. The proxy server evaluates the request and provides the resource by establishing the connection to the respective server and/or requests the required service on behalf of the client. Using a proxy server can allow an attacker to hide ID (i.e., become anonymous on the network).

A proxy server has following purposes:

1. Keep the systems behind the curtain (mainly for security reasons).
2. Speed up access to a resource (through "caching"). It is usually used to cache the webpages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address (visit http://www.multiproxy.org/multiproxy.htm for more information).

One of the advantages of a proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy's cache memory, which will improve user response time. In fact there are special servers available known as *cache servers*. A proxy can also do logging.

Listed are few websites where free proxy servers can be found:

1. http://www.proxy4free.com
2. http://www.publicproxyservers.com

3. http://www.proxz.com
4. http://www.anonymitychecker.com
5. http://www.surf24h.com
6. http://www.hidemyass.com

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.[1] Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client. In 1997 the first anonymizer software tool was created by Lance Cottrell, developed by Anonymizer.com. The anonymizer hides/removes all the identifying information from a user's computer while the user surfs on the Internet, which ensures the privacy of the user. (See Section 9.7, Chapter 9.)

Listed are few websites where more information about anonymizers can be found:

1. http://www.anonymizer.com
2. http://www.browzar.com
3. http://www.anonymize.net
4. http://www.anonymouse.ws
5. http://www.anonymousindex.com

Box 4.2 Being Anonymous While Searching on Google!

Google Cookie

Google was the first search engine to use a cookie.[2] Google set the standard and nowadays cookies are commonplace among search engines. This cookie places a unique ID number on your hard disk. Anytime you visit Google, user gets a Google cookie if a user doesn't already have one. If a user has one then it will read and record the unique ID number. Google can build a detailed list of your search terms over many years. (Google's cookies are set to expire by the year 2038, unless a user deletes before its expiry.)

Cookie

Cookie (also know as HTTP cookie/browser cookie) is a small text file that contains a string of alphanumeric characters and is used for storing netizen's website preferences/authentication while visiting the same webpage again and again or also acts as identifier for server-based session – such browser mechanism of setting and reading cookies invites attackers to use these cookies as "Spyware." There are two types of cookies:

1. Persistent cookie and
2. session cookie.

Persistent cookie is stored by the web browser into the cookie folder on the PC's hard disk. It remains under the cookie folder, which is maintained by the web browser. Session cookie is a temporary cookie and does not reside on the PC once the browser is closed (see Boxes 9.2, 9.3 and 9.4, Chapter 9).

DoubleClick

It is a subsidiary of Google and provides Internet ad-serving services and paid search products listing (*DART Search*[3]) and utilize the cookies, which are called DART cookie. Internet Advertising Network was started by Kevin O'Connor and Dwight Merriman in 1995. IAN and the DoubleClick division of Poppe-Tyson were merged into a new corporation named DoubleClick in 1996. DoubleClick was first in the online media representative business, that is, representing websites to sell advertising space to marketers. In 1997 it began offering the online ad serving and management technology they had

Box 4.2 Being Anonymous . . . (*Continued*)

developed to other publishers as the DART services. The DART cookie is a persistent cookie, which consists of the name of the domain that has set the cookie, the lifetime of the cookie and a "value." DoubleClick's DART mechanism generates a unique series of characters for the "value" portion of the cookie. These DoubleClick DART cookies help marketers learn how well their Internet advertising campaigns or paid search listings perform. Many marketers and Internet websites use DoubleClick's DART technology to deliver and serve their advertisements or manage their paid search listings. DoubleClick's DART products set or recognize a unique, persistent cookie when an ad is displayed or a paid listing is selected. The information that the DART cookie helps to give marketers includes the number of unique users their advertisements displayed to, how many users clicked on their Internet ads or paid listings and which ads or paid listings they clicked on.

G-Zapper

G-Zapper[4] utility helps to stay anonymous while searching Google. Google stores a unique identifier in a cookie on the computer (i.e., on the hard disk) which allows to track keywords that are searched for. This information is used to compile reports, track user habits and test features. In the future, it would be possible that this information is sold and/or shared with others.

G-Zapper helps to protect users' ID and search history. G-Zapper reads the Google cookie installed on users' PC, displays the date it was installed, determines how long user searches have been tracked and displays Google searches. G-Zapper allows user to automatically delete or entirely block the Google search cookie from future installation.

This utility can be downloaded from http://www.dummysoftware.com/gzapper.html

4.3 Phishing

While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening him/her to close the bank account if he/she does not reply immediately. Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail. This message and other such messages are examples of Phishing – in addition to stealing personal and financial data – and can infect systems with viruses and also a method of online ID theft in various cases. Most people associate Phishing with E-Mail messages that spoof or mimic banks, credit card companies or other business such as Amazon and eBay. These messages look authentic and attempt to get users to reveal their personal information.

It is believed that *Phishing* is an alternative spelling of "fishing," as in "to fish for information." The first documented use of the word "Phishing" was in 1996.

4.3.1 How Phishing Works?

Phishers work in the following ways[5]:

1. **Planning:** Criminals, usually called as phishers, decide the target (i.e., specific business/business house/an individual) and determine how to get E-Mail address of that target or customers of that business. Phishers often use mass mailing and address collection techniques as spammers.
2. **Setup:** Once phishers know which business/business house to spoof and who their victims are, they will create methods for delivering the message and to collect the data about the target. Most often this involves E-Mail addresses and a webpage.

3. **Attack:** This is the step people are most familiar with – the phisher sends a phony message that appears to be from a reputable source.
4. **Collection:** Phishers record the information of victims entering into webpages or pop-up windows.
5. **Identity theft and fraud:** Phishers use the information that they have gathered to make illegal purchases or commit fraud.

Phishing started off as being part of popular hacking culture. Nowadays, more and more organizations/institutes provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level. We have explained Phishing and Identity Theft in detail in Chapter 5.

4.4 Password Cracking

Password is like a key to get an entry into computerized systems like a lock. Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.[6] Usually, an attacker follows a common approach – repeatedly making guesses for the password. The purpose of password cracking is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps:

1. Find a valid user account such as an Administrator or Guest;
2. create a list of possible passwords;
3. rank the passwords from high to low probability;
4. key-in each password;
5. try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information (explained in Chapter 5). Examples of guessable passwords include:

1. Blank (none);
2. the words like "password," "passcode" and "admin";
3. series of letters from the "QWERTY" keyboard, for example, qwerty, asdf or qwertyuiop;
4. user's name or login name;
5. name of user's friend/relative/pet;
6. user's birthplace or date of birth, or a relative's or a friend's;
7. user's vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user;
9. simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list. This is still considered manual cracking, is time-consuming and not usually effective.

Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource. To ensure confidentiality of passwords, the

password verification data is usually not stored in a clear text format. For example, one-way function (which may be either an encryption function or a cryptographic hash) is applied to the password, possibly in combination with other data, and the resulting value is stored. When a user attempts to login to the system by entering the password, the same function is applied to the entered value and the result is compared with the stored value. If they match, user gains the access; this process is called *authentication*.

Even though these functions create hashed passwords, which may be cryptographically secure, an attacker attempts to get possession of the hashed password, which will help to provide a quick way to test guesses for the password by applying the one-way function to each guess and comparing the result to the verification data. The most commonly used hash functions can be computed rapidly and the attacker can test these hashes with the help of passwords cracking tools (see Table 4.3) to get the plain text password.

Table 4.3 | Password cracking tools

Website	*Brief Description*
www.defaultpassword.com	**Default password(s):** Network devices such as switches, hubs and routers are equipped with "default passwords" and usually these passwords are not changed after commissioning these devices into the network (i.e., into LAN). The intruders can gain the access using these default passwords by visiting the said website.
http://www.oxid.it/cain.html	**Cain & Abel:** This password recovery tool is typically used for Microsoft Operating Systems (OSs). It allows to crack the passwords by sniffing the network, cracking encrypted passwords using dictionary, brute force attacks, decoding scrambled passwords and recovering wireless network keys.
http://www.openwall.com/john	**John the Ripper:** This is a free and open-source software – fast password cracker, compatible with many OSs like different flavors of Unix, Windows, DOS, BeOS and OpenVMS. Its primary purpose is to detect weak Unix passwords.
http://freeworld.thc.org/thc-hydra	**THC-Hydra:** It is a very fast network logon cracker which supports many different services.
http://www.aircrack-ng.org	**Aircrack-ng:** It is a set of tools used for wireless networks. This tool is used for 802.11a/b/g wired equivalent privacy (WEP) and *Wi*-Fi *P*rotected *A*ccess (WPA) cracking. It can recover a 40 through 512-bit WEP key once enough encrypted packets have been gathered. It can also attack WPA 1 or 2 networks using advanced cryptographic methods or by brute force.
http://www.l0phtcrack.com	**L0phtCrack:** It is used to crack Windows passwords from hashes which it can obtain from stand-alone Windows workstations, networked servers, primary domain controllers or Active Directory. It also has numerous methods of generating password guesses (dictionary, brute force, etc.).
http://airsnort.shmoo.com	**AirSnort:** It is a wireless LAN (WLAN) tool which recovers encryption keys. It operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. It requires approximately 5–10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second. It runs under Windows or Linux.

(*Continued*)

Table 4.3 | (*Continued*)

Website	*Brief Description*
http://www.solarwinds.com	**SolarWinds:** It is a plethora of network discovery/monitoring/attack tools and has created dozens of special-purpose tools targeted at systems administrators. Security-related tools include many network discovery scanners, a Simple Network Management Protocol (SNMP) brute force cracker, router password decryption and more.
http://www.foofus.net/fizzgig/pwdump	**Pwdump:** It is a Window password recovery tool. Pwdump is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether Syskey is enabled. It is also capable of displaying password histories if they are available.
http://project-rainbowcrack.com	**RainbowCrack:** It is a hash cracker that makes use of a large-scale time-memory trade-off. A traditional brute force cracker tries all possible plain texts one by one, which can be time-consuming for complex passwords. RainbowCrack uses a time-memory trade-off to do all the cracking-time computation in advance and store the results in so-called "rainbow tables." It does take a long time to precompute the tables but RainbowCrack can be hundreds of times faster than a brute force cracker once the precomputation is finished.
http://www.hoobie.net/brutus	**Brutus:** It is one of the fastest, most flexible remote password crackers available for free. It is available for Windows 9x, NT and 2000. It supports HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP and more.

Password cracking attacks can be classified under three categories as follows:

1. Online attacks;
2. offline attacks;
3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving are explained in Chapter 2).

4.4.1 Online Attacks

An attacker can create a script file (i.e., automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system. The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack." It is a form of active eavesdropping[7] in which the attacker establishes a connection between a victim and the server to which a victim is connected. When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server (e.g., an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in-the-middle). This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also used to get the passwords for financial websites that would like to gain the access to banking websites.

4.4.2 Offline Attacks

Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used. Offline attacks usually require physical

Table 4.4 | Types of password cracking attacks

Type of Attack	*Description*	*Example of a Password*
Dictionary attack	Attempts to match all the words from the dictionary to get the password	Administrator
Hybrid attack	Substitutes numbers and symbols to get the password	Adm1n1strator
Brute force attack	Attempts all possible permutation-combinations of letters, numbers and special characters	Adm!n@09

access to the computer and copying the password file from the system onto removable media. Different types of offline password attacks are described in Table 4.4. Few tools listed in Table 4.2 also use these techniques to get the password in the clear text format.

4.4.3 Strong, Weak and Random Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords, such as words in the dictionary, proper names and words based on the username or common variations on these themes. Passwords that can be easily guessed by acquaintances of the netizens (such as date of birth, pet's name and spouses' name) are considered to be very weak. Here are some of the examples of "weak passwords":

1. **Susan:** Common personal name;
2. **aaaa:** repeated letters, can be guessed;
3. **rover:** common name for a pet, also a dictionary word;
4. **abc123:** can be easily guessed;
5. **admin:** can be easily guessed;
6. **1234:** can be easily guessed;
7. **QWERTY:** a sequence of adjacent letters on many keyboards;
8. **12/3/75:** date, possibly of personal importance;
9. **nbusr123:** probably a username, and if so, can be very easily guessed;
10. **p@$$\/\/0rd:** simple letter substitutions are preprogrammed into password cracking tools;
11. **password:** used very often – trivially guessed;
12. **December12:** using the date of a forced password change is very common.

A strong password is long enough, random or otherwise difficult to guess – producible only by the user who chooses it. The length of time deemed to be too long will vary with the attacker, the attacker's resources, the ease with which a password can be tried and the value of the password to the attacker. A student's password might not be worth more than a few seconds of computer time, while a password controlling access to a large bank's electronic money transfer system might be worth many weeks of computer time for trying to crack it. Here are some examples of strong passwords:

1. **Convert_£100 to Euros!:** Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.
2. **382465304H:** It is mix of numbers and a letter at the end, usually used on mass user accounts and such passwords can be generated randomly, for example, in schools and business.
3. **4pRte!ai@3:** It is not a dictionary word; however it has cases of alpha along with numeric and punctuation characters.

4. **MoOoOfIn245679:** It is long with both alphabets and numerals.
5. **t3wahSetyeT4:** It is not a dictionary word; however, it has both alphabets and numerals.

Visit http://www.microsoft.com/protect/fraud/passwords/checker.aspx to check the strength of your password.[8]

4.4.4 Random Passwords

We have explained in the previous section how most secure passwords are long with random strings of characters and how such passwords are generally most difficult to remember. Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters. The difficulty in remembering such a password increases the chance that the user will write down the password, which makes it more vulnerable to a different attack (in this case, the paper being lost or stolen and the password discovered). Whether this represents a net reduction in security depends on whether the primary threat to security is internal (e.g., social engineering) or external. A password can, at first sight, be random, but if you really examine it, it is just a pattern. One of these types of passwords is 26845. Although short, it is not easily guessed. However, the person who created the password is able to remember it because it is just the four direction keys on the square number board (found at the right of most keyboards) plus a five in the middle. If you practice it, it is just one swift motion of moving two fingers around the board (which is very easy to use). Forcing users to use system-created random passwords ensures that the password will have no connection with that user and should not be found in any dictionary. Several OSs have included such a feature. Almost all the OSs also include password aging; the users are required to choose new passwords regularly, usually after 30 or 45 days. Many users dislike these measures, particularly when they have not been taken through security awareness training. The imposition of strong random passwords may encourage the users to write down passwords, store them in personal digital assistants (PDAs) or cell phones and share them with others against memory failure, increasing the risk of disclosure.

The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

1. Passwords and user logon identities (IDs) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters (no common names or phrases).
3. There should be computer-controlled lists of prescribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words and standard names) to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues, etc. They shall not be coded into programs or noted down anywhere.
5. Passwords shall be changed every 30/45 days or less. Most operating systems (OSs) can enforce a password with an automatic expiration and prevent repeated or reused passwords.
6. User accounts should be frozen after five failed logon attempts. All erroneous password entries should be recorded in an audit log for later inspection and action, as necessary.
7. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require the passwords to be re-entered.
8. Successful logons should display the date and time of the last logon and logoff.
9. Logon IDs and passwords should be suspended after a specified period of non-use.
10. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data) for the failed user (to keep this user connected while personnel attempt to investigate the incoming connection).

Similarly, netizens should practice password guidelines to avoid being victim of getting their personal E-Mail accounts hacked/attacked by the attackers.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.
6. Passwords of personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public Internet facilities such as cybercafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyber-attacks (explained in Section 3.8, Chapter 3).
8. In the case of receipt of an E-Mail from banking/financial institutions, instructing to change the passwords, before clicking the weblinks displayed in the E-Mail, legitimacy of the E-Mail should be ensured to avoid being a victim of Phishing attacks (we will explain Phishing attack in detail in Chapter 5).
9. Similarly, in case of receipt of SMS from banking/financial institutions, instructing to change the passwords, legitimacy of the E-Mail should be ensured to avoid being a victim of Smishing attacks (explained in detail in Chapter 3).
10. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

4.5 Keyloggers and Spywares

Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.[9]

Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior. It can be classified as software keylogger and hardware keylogger.

4.5.1 Software Keyloggers

Software keyloggers are software programs (see Table 4.5) installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Software keyloggers are installed on a computer system by Trojans or viruses (will discuss more on this in subsequent sections of this chapter) without the knowledge of the user. Cybercriminals always install such tools on the insecure computer systems available in public places (i.e., cybercafes, library – we have already discussed this in Chapter 2) and can obtain the required information about the victim very easily. A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes.[10]

Table 4.5 | Software keyloggers

Website	*Brief Description*
http://www.soft-central.net	**SC-KeyLog PRO:** It allows to secretly record computer user activities such as E-Mails, chat conversations, visited websites, clipboard usage, etc. in a protected logfile. SC-KeyLog PRO also captures Windows user logon passwords. The captured information is completely hidden from the user and allows to remotely install the monitoring system through an E-Mail attachment without the user recognizing the installation at all.
http://www.spytech-web.com	**Spytech SpyAgent Stealth:** It provides a large variety of essential computer monitoring features as well as website and application filtering, chat blocking and remote delivery of logs via E-Mail or FTP.
http://www.relytec.com	**All In One Keylogger:** It is an invisible keystrokes recorder and a spy software tool that registers every activity on the PC to encrypted logs. This keylogger allows secretly tracking of all activities from all computer users and automatically receiving logs to a desired E-Mail/FTP accounting. With this keylogger, one can read chat conversations, look at the E-Mails as well as watch the sites that have been surfed.
http://www.stealthkeylogger.org	**Stealth Keylogger:** It is a computer monitoring software that enables activity log report where the entire PC keyboard activities are registered either at specific time or hourly on daily basis. The entire log reports are generated either in text or HTML file format as defined by the user. The keylogger facilitates mailing of log report at the specified E-Mail address.
http://www.blazingtools.com	**Perfect Keylogger:** It has its advanced keyword detection and notification. User can create a list of "on alert" words or phrases and keylogger will continually monitor keyboard typing, URLs and webpages for these words or phrases – for example, "bomb," "sex," "visiting places around Mumbai" and "Windows vulnerabilities." When a keyword is detected, perfect keylogger makes screenshot and sends E-Mail notification to the user.
http://kgb-spy-software.en.softonic.com	**KGB Spy:** It is a multifunctional keyboard tracking software, widely used by both regular users and IT security specialists. This program does not just record keystrokes but is also capable of recording language-specific characters. It records all typed data/all keyboard activity. It can be used to monitor children's activity at home or to ensure employees do not use company's computers inappropriately. Visit www.refog.com to find more on this product.
http://www.spy-guide.net/spybuddy-spy-software.htm	**Spy Buddy:** This, along with keylogger, has following features: • Internet conversation logging; • disk activity logging; • Window activity logging; • application activity logging; • clipboard activity logging; • AOL/Internet explorer history; • printed documents logging; • keylogger keystroke monitoring; • websites activity logging; • screenshot capturing; • WebWatch keyword alerting

(*Continued*)

Table 4.5 | (*Continued*)

Website	*Brief Description*
http://www.elite-keylogger.com	**Elite Keylogger:** It captures every keystroke typed, all passwords (including Windows logon passwords), chats, instant messages, E-Mails, websites visited, all program launched, usernames and time they worked on the computer, desktop activity, clipboard, etc.
http://www.cyberspysoftware.com	**CyberSpy:** It provides an array of features and easy-to-use graphical interface along with computer monitoring capabilities such as keep tabs on the employees and keeps track of what children are viewing on the Internet. CyberSpy can be used as complete PC monitoring solution for any home or office. CyberSpy records all websites visited, instant message conversations, passwords, E-Mails and all keystrokes pressed. It also has the ability to provide screenshots at set intervals.
http://www.mykeylogger.com	**Powered Keylogger:** Powered keylogger can be used for the following: • *Surveillance:* It is for anyone to control what happens on the computer when the computer's owner is away. • *Network administration:* It is for network administrators to control outgoing traffic and sites visited. • *Shared PC activity tracking:* It is to analyze the usage of shared PC. • *Parental control:* It helps parents to monitor their children's computer and Internet activity. • *Employee productivity monitoring:* It helps managers to check and increase productivity of their stuff or just to prevent the leak of important information.
http://www.x-pcsoft.com	**XPC Spy:** XPC Spy is one of the powerful keylogger spy software, runs stealthy under MS Windows and has the following features: • Records all keystrokes typed; • records all websites visited; • records all programs executed, folders explored, files opened or edited, documents printed, etc.; • records all windows opened; • records all clipboard text content; • records all system activities; • records webmails sent (database update online, more and more webmail servers are supported); • records all ICQ Messenger chat conversations; • records all MSN Messenger chat conversations; • records all AOL/AIM Messenger chat conversations; • records all Yahoo! Messenger chat conversations; • runs invisible in the background and is protected by password; • is built-in screenshot pictures viewer; • schedules monitor process, sets time to start or stop monitoring; • sends logs report via E-Mail.

4.5.2 Hardware Keyloggers

To install these keyloggers, physical access to the computer system is required. Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device. Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs. Each keypress on the keyboard of the ATM gets registered by these keyloggers. These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

Listed are few websites where more information about hardware keyloggers can be found:

1. http://www.keyghost.com
2. http://www.keelog.com
3. http://www.keydevil.com
4. http://www.keykatcher.com

4.5.3 Antikeylogger

Antikeylogger[11] is a tool that can detect the keylogger installed on the computer system and also can remove the tool. Visit http://www.anti-keyloggers.com for more information.

Advantages of using antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft (we will discuss it more in Chapter 5).
5. It secures E-Mail and instant messaging/chatting.

4.5.4 Spywares

Spyware is a type of malware (i.e., malicious software – see Box 4.3 to know about different types of malwares) that is installed on computers which collects information about users without their knowledge. The presence of Spyware is typically hidden from the user; it is secretly installed on the user's personal computer. Sometimes, however, Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.[12]

It is clearly understood from the term *Spyware* that it secretly monitors the user. The features and functions of such Spywares are beyond simple monitoring. Spyware programs collect personal information about the victim, such as the Internet surfing habits/patterns and websites visited. The Spyware can also redirect Internet surfing activities by installing another stealth utility on the users' computer system. Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the Internet speed connection with Internet Service Provider (ISP). Various Spywares are available in the market and the one that are popular are listed in Table 4.6.

To overcome the emergence of Spywares that proved to be troublesome for the normal user, anti-Spyware softwares (refer to Appendix B: List of Useful Software Utilities and Websites in CD) are available in the market. Installation of anti-Spyware software has become a common element nowadays from computer security practices perspective.

Box 4.3 Malwares

Malware, short for malicious software, is a software designed to infiltrate a computer system without the owner's informed consent (see Box 9.8, Chapter 9). The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive or annoying software or program code.[13] Malware can be classified as follows:

1. **Viruses and worms:** These are known as *infectious malware*. They spread from one computer system to another with a particular behavior (will discuss more on this in Section 4.6).
2. **Trojan Horses:** A Trojan Horse,[14] Trojan for short, is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system (will discuss more on this in Section 4.7).
3. **Rootkits:** Rootkits[15] is a software system that consists of one or more programs designed to obscure the fact that a system has been compromised. For further details refer to Section 7.12.1, Chapter 7.
4. **Backdoors:** Backdoor[16] in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text and so on while attempting to remain undetected.
5. **Spyware:** For further details see Section 4.5.
6. **Botnets:** For further details see Section 2.6 in Chapter 2.
7. **Keystroke loggers:** For further details see Section 4.5.

Table 4.6 | Spywares

Website	*Brief Description*
http://www.e-spy-software.com	**007 Spy:** It has following key features: • Capability of overriding "antispy" programs like "Ad-aware"; • record all websites URL visited in Internet; • powerful keylogger engine to capture all passwords; • view logs remotely from anywhere at anytime; • export log report in HTML format to view it in the browser; • automatically clean-up on outdated logs; • password protection.
http://www.spectorsoft.com	**Spector Pro:** It has following key features: • Captures and reviews all chats and instant messages; • captures E-Mails (read, sent and received); • captures websites visited; • captures activities performed on social networking sites such as MySpace and Facebook; • enables to block any particular website and/or chatting with anyone; • acts as a keylogger to capture every single keystroke (including usernames and passwords).
http://www.spectorsoft.com	**eBlaster:** Besides keylogger and website watcher, it also records E-Mails sent and received, files uploaded/downloaded, logging users' activities, record online searches, recording MySpace and Facebook activities and any other program activity.
http://www.remotespy.com	**Remotespy:** Besides remote computer monitoring, silently and invisibly, it also monitors and records users' PC without any need for physical access. Moreover, it records keystrokes (keylogger), screenshots, E-Mail, passwords, chats, instant messenger conversations and websites visited.

(*Continued*)

Table 4.6 | (*Continued*)

Website	*Brief Description*
http://www.topofbestsoft.com	**Stealth Recorder Pro:** It is a new type of utility that enables to record a variety of sounds and transfer them automatically through Internet without being notified by original location or source. It has following features: • Real-time MP3 recording via microphone, CD, line-in and stereo mixer as MP3, WMA or WAV formatted files; • transferring via E-Mail or FTP, the recorded files to a user-defined E-Mail address or FTP automatically; • controlling from a remote location; • voice mail, records and sends the voice messages.
http://www.amplusnet.com	**Stealth Website Logger:** It records all accessed websites and a detailed report can be available on a specified E-Mail address. It has following key features: • Monitor visited websites; • reports sent to an E-Mail address; • daily log; • global log for a specified period; • log deletion after a specified period; • hotkey and password protection; • not visible in add/remove programs or task manager.
http://www.flexispy.com	**Flexispy:** It is a tool that can be installed on a cell/mobile phone. After installation, Flexispy secretly records coversation that happens on the phone and sends this information to a specified E-Mail address.
http://www.wiretappro.com	**Wiretap Professional:** It is an application for monitoring and capturing all activities on the system. It can capture the entire Internet activity. This spy software can monitor and record E-Mail, chat messages and websites visited. In addition, it helps in monitoring and recording of keystrokes, passwords entered and all documents, pictures and folders viewed.
http://www.pcphonehome.com	**PC PhoneHome:** It is a software that tracks and locates lost or stolen laptop and desktop computers. Every time a computer system on which PC PhoneHome has been installed, conneced to the Internet, a stealth E-Mail is sent to a specified E-Mail address of the user's choice and to PC PhoneHome Product Company.
http://www.spyarsenal.com	**SpyArsenal Print Monitor Pro:** It has following features: • Keep track on a printer/plotter usage; • record every document printed; • find out who and when certain paper printed with your hardware.

4.6 Virus and Worms

Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself. Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines. A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. A virus can start on event-driven effects (e.g., triggered after a specific number of executions), time-driven effects (e.g., triggered on a specific date, such as Friday the 13th) or can occur at random. Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus;
2. delete files inside the system into which viruses enter;
3. scramble data on a hard disk;
4. cause erratic screen behavior;
5. halt the system (PC);
6. just replicate themselves to propagate further harm.

Figures 4.1–4.3 explain how viruses spread (a) through the Internet, (b) through a stand-alone computer system and (c) through local networks.

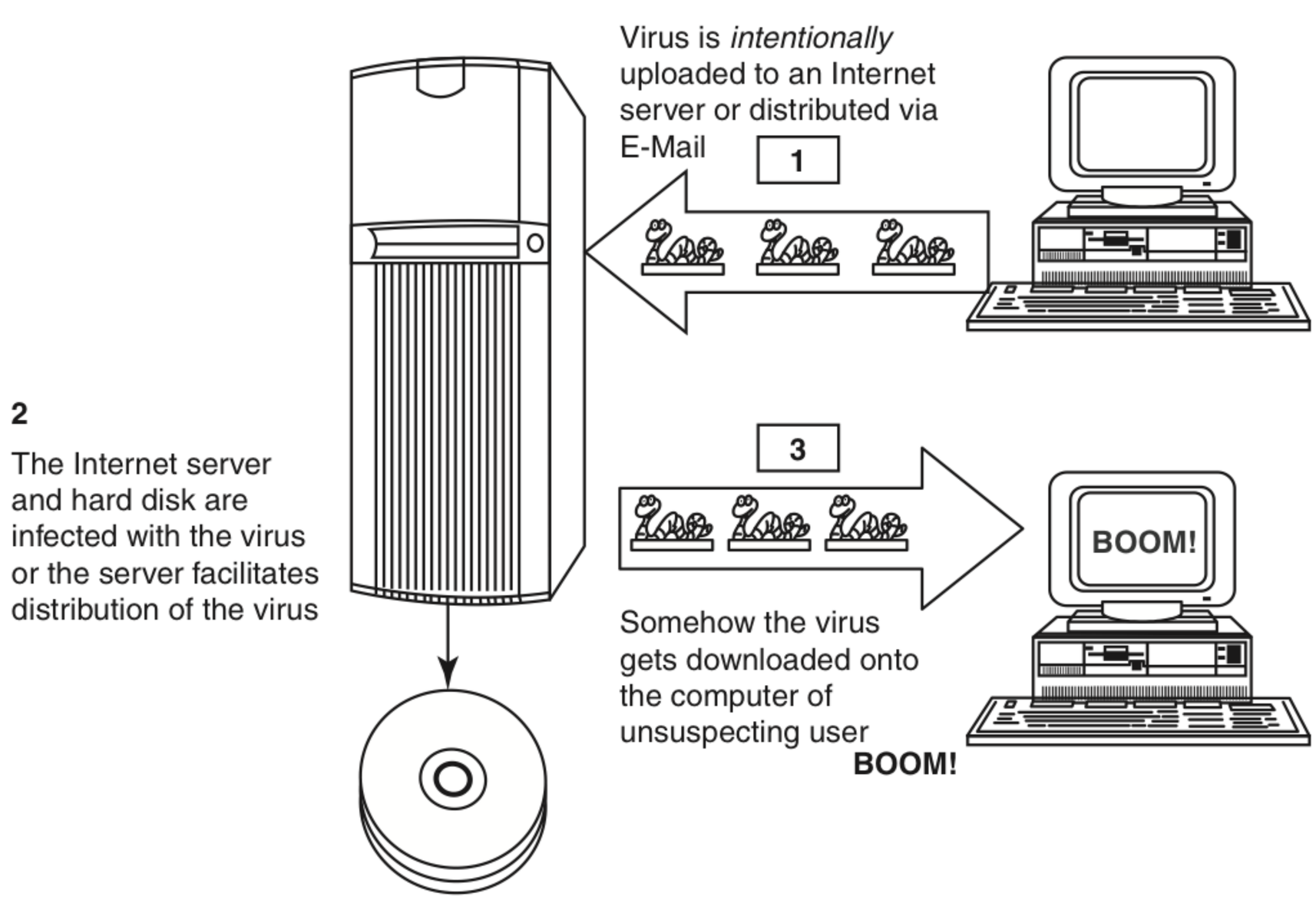

Figure 4.1 | Virus spreads through the Internet.

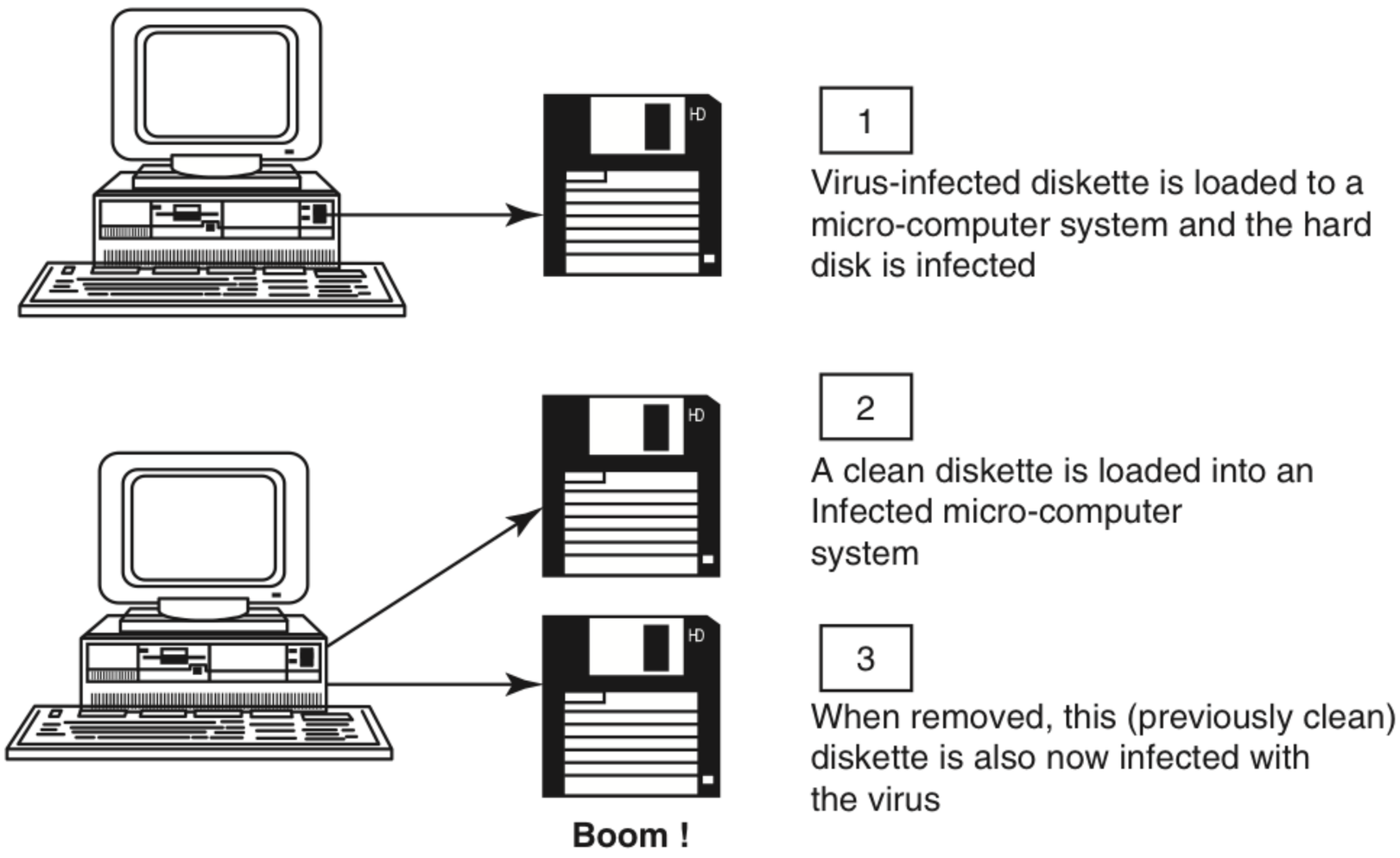

Figure 4.2 | Virus spreads through stand-alone system.

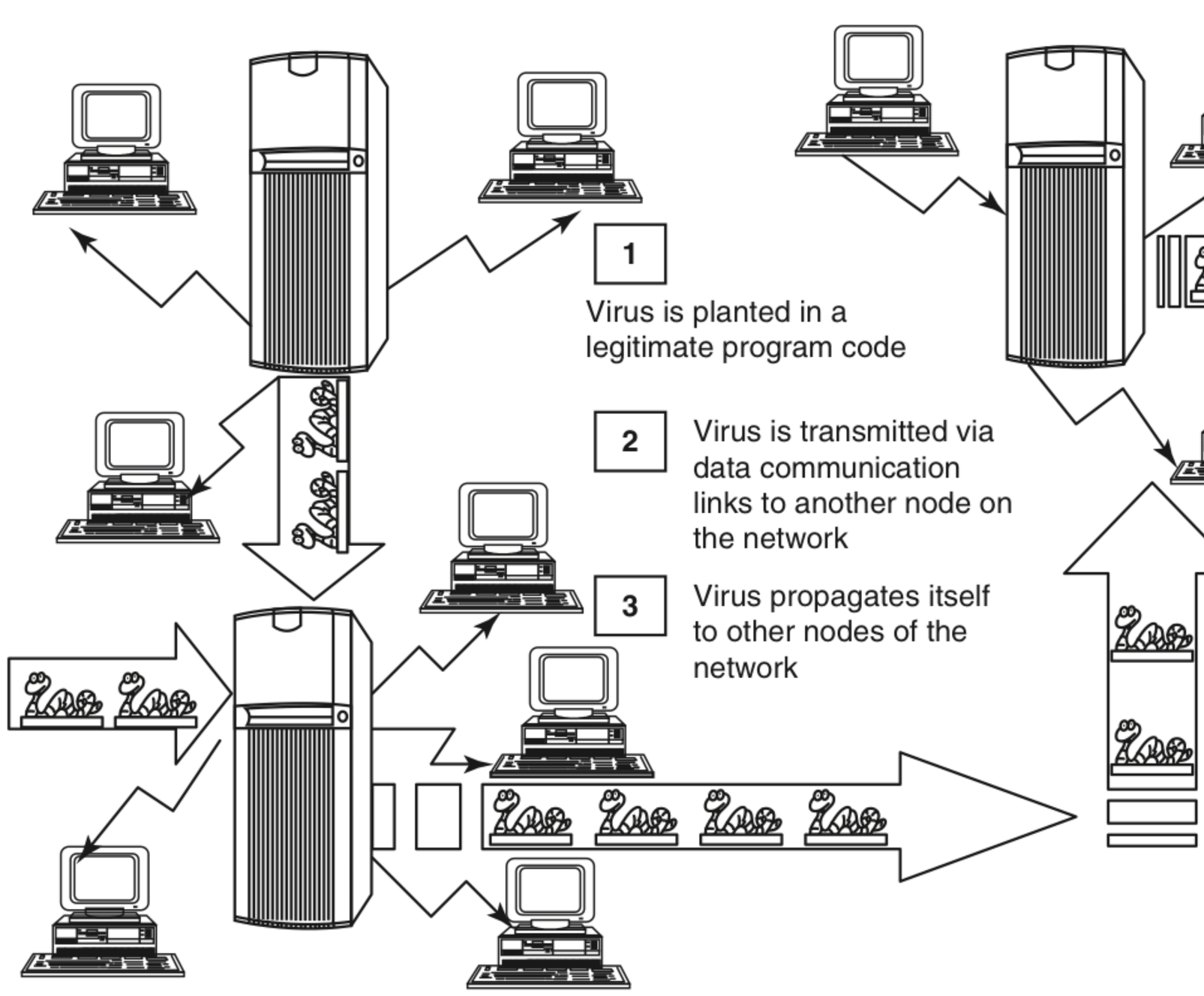

Figure 4.3 | Virus spreads through local networks.

Computer virus has the ability to copy itself and infect the system. The term *virus* is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability. A true virus can only spread from one system to another (in some form of executable code) when its host is taken to the target computer; for instance, when a user sent it over the Internet or a network, or carried it on a removable media such as CD, DVD or USB drives. Viruses can increase their chances of spreading to other systems by infecting files on a network file system or a file system that is accessed by another system.[17]

As explained in earlier sections, the term *computer virus* is sometimes used as a *catch-all phrase* to include all types of malware, Adware and Spyware programs that do not have reproductive ability. Malware includes computer viruses, worms, Trojans, most Rootkits, Spyware, dishonest Adware, crimeware and other malicious and unwanted software as well as true viruses. Viruses are sometimes confused with computer worms and Trojan Horses, which are technically different (see Table 4.7 to understand the difference between computer virus and worm). A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a code/program that appears to be harmless but hides malicious functions. Worms and Trojans, such as viruses, may harm the system's data or performance. Some viruses and other malware have noticeable symptoms that enable computer user to take necessary corrective actions, but many viruses are surreptitious or simply do nothing for user's to take note of them. Some viruses do nothing beyond reproducing themselves.[17]

Table 4.7 | Difference between computer virus and worm

Sr. No.	*Facet*	*Virus*	*Worm*
1	Different types	Stealth virus, self-modified virus, encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing networks worms
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software program that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as the first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, *The Worm Programs* and after that the name was adopted
5	Prevalence	Over 100,000 known computer viruses have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

Source: See [18] in References section.

4.6.1 Types of Viruses

Computer viruses can be categorized[19] based on attacks on various elements of the system and can put the system and personal data on the system in danger.

1. **Boot sector viruses:** It infects the storage media on which OS is stored (e.g., floppy diskettes and hard drives) and which is used to start the computer system. The entire data/programs are stored on the floppy disks and hard drives in smaller sections called sectors. The first sector is called the BOOT and it carries the master boot record (MBR). MBR's function is to read and load OS, that is, it enables computer system to start through OS. Hence, if a virus attacks an MBR or infects the boot record of a disk, such floppy disk infects victim's hard drive when he/she reboots the system while the infected disk is in the drive. Once the victim's hard drive is infected all the floppy diskettes that are being used in the system will be infected. Boot sector viruses often spread to other systems when shared infected disks and pirated software(s) are used.
2. **Program viruses:** These viruses become active when the program file (usually with extensions .bin, .com, .exe, .ovl, .drv) is excuted (i.e., opened – program is started). Once these program files get infected, the virus makes copies of itself and infects the other programs on the computer system.
3. **Multipartite viruses:** It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active. When the victim starts the computer system next time, it will infect the local drive and other programs on the victim's computer system.
4. **Stealth viruses:** It camouflages and/or masks itself and so detecting this type of virus is very difficult. It can disguise itself such a way that antivirus software also cannot detect it thereby preventing spreading into the computer system. It alters its file size and conceals itself in the computer memory to remain in the system undetected. The first computer virus, named as Brain, was a stealth virus. A good antivirus detects a stealth virus lurking on the victim's system by checking the areas the virus must have infected by leaving evidence in memory.
5. **Polymorphic viruses:** It acts like a "chameleon" that changes its virus signature (i.e., binary pattern) every time it spreads through the system (i.e., multiplies and infects a new file). Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program. *Polymorphic generators* are the routines (i.e., small programs) that can be linked with the existing viruses. These generators are not viruses but the purpose of these generators is to hide actual viruses under the cloak of polymorphism. The first all-purpose polymorphic generator was the mutation engine (MtE) published in 1991. Other known polymorphic generators are Dark Angel's Multiple Encryptor (DAME), Darwinian Genetic Mutation Engine (DGME), Dark Slayer Mutation Engine (DSME), MutaGen, Guns'n'Roses Polymorphic Engine (GPE) and Dark Slayer Confusion Engine (DSCE).
6. **Macroviruses:** Many applications, such as Microsoft Word and Microsoft Excel, support MACROs (i.e., macrolanguages). These macros are programmed as a macroembedded in a document. Once a macrovirus gets onto a victim's computer then every document he/she produces will become infected. This type of virus is relatively new and may get slipped by the antivirus software if the user does not have the most recent version installed on his/her system.
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls. Little awareness is needed about managing and controlling these settings of a web browser to prohibit and allow certain functions to work – such as enabling or disabling pop-ups, downloading files and sound – which invites the threats for the computer system being targeted by unwanted software(s) floating in cyberspace.

To know more on viruses see Box 4.4 and to know more on the world's worst virus attacks see Table 4.8. As Windows OS is the most used OS across the globe, the lists of viruses displayed in Table 4.8 are the attacks on Windows OS. The terms "Virus" and "Worm" are used interchangeably and hence readers may find that the viruses listed under Table 4.8 may be referred as worms on some websites and/or in some books.

Box 4.4 More about Viruses!

1. The early "hacking" sites that have allowed to download favorite virus are as follows:
   - www.2600.com
   - www.L0pht.com
2. The exhaustive list of viruses can be found at:

   http://en.wikipedia.org/wiki/List_of_computer_viruses_(all)
3. The viruses can attack a system 365 days a year. However, on the designated payload dates, the virsues may do more than just infect the system. Virus calendar can be found at:

   http://home.mcafee.com/virusInfo/VirusCalendar.aspx
4. **Computer virus hoax:** It is a message warning the recipient of a non-existent computer virus threat. The message is usually a chain E-Mail that tells the recipient to forward it to everyone they know. They often include announcements claimed to be from reputable organizations such as Microsoft, IBM or news sources such as CNN and include emotive language and encouragement to forward the message. These sources are quoted to add credibility to the hoax. The list of virus hoax can be found at:

   http://en.wikipedia.org/wiki/Virus_hoax
5. **Unix and Linux OS are immune from computer viruses:** This is a myth that Unix/Linux systems are as susceptible to hostile software attacks as any other systems. However, such systems usually found to be well-protected compared with Microsoft Windows because fast updates are available to most Unix/Linux vulnerabilities. The list of virus/worms found on Unix/Linux systems can be found at:

   http://en.wikipedia.org/wiki/Linux_malware

Table 4.8 The world's worst virus attacks!!!

Sr. No.	*Virus*	*Brief Description*
1	Conficker	It is also known as Downup, Downadup and Kido. It targets Microsoft Windows OS and was first detected in November 2008. It uses flaws in Windows software and dictionary attacks on administrator passwords to co-opt machines and link them into a virtual computer that can be commanded remotely by its authors. The name Conficker is blended from a English term "*configure*" and the German word "*Ficker*," which means "to have sex with" or "to mess with" in colloquial German.
2	INF/AutoRun	*AutoRun* and the companion feature *AutoPlay* are components of the Microsoft Windows OS that dictate what actions the system takes when a drive is mounted. This is the most common threat that infects a PC by creating an "autorun.inf" file. The file contains information about programs meant to run automatically when removable devices are connected to the computer. End-users must disable the AutoRun feature enabled by default in windows. AutoRun functionality is used in attack vector attacks.

(*Continued*)

Table 4.8 | (*Continued*)

Sr. No.	*Virus*	*Brief Description*
3	Win32 PSW. OnLineGames	It is a dangerous virus that replicates itself as other viruses and spreads from one computer system to another carrying a payload of destruction. It can infect several computers within few minutes. It is more concerned with gamers around the world, stealing confidential and other financial credentials as well as gaining access to the victim's account. This virus is also termed as Trojan.
4	Win32/Agent	This virus is also termed as Trojan. It copies itself into temporary locations and steals information from the infected system. It adds entries into the registry, creating several files at different places in the system folder, allowing it to run on every start-up, which enables to gather complete information about the infected system and then transferred to the intruder's system.
5	Win32/FlyStudio	It is known as Trojan with characteristics of backdoor. This virus does not replicate itself, but spreads only when the circumstances are beneficial. It is called as backdoors because the information stolen from a system is sent back to the intruder.
6	Win32/Pacex.Gen	This threat designates a wide range of malwares that makes use of an obfuscation layer to steal passwords and other information from the infected system.
7	Win32/Qhost	This virus copies itself to the System32 folder of the Windows directory giving control of the computer to the attacker. The attacker then modifies the Domain Name Server/System (DNS) settings redirecting the computer to other domains. This is done to compromise the infected machine from downloading any updates and redirect any attempts made to a website that downloads other malicious files on the victim's computer.
8	WMA/ TrojanDownloader. GetCodec	This threat as the suffix .GetCodec modifies the audio files present on the system to ".wma" format and adds a URL header that points to the location of the new codec. In this manner, the host computer is forced to download the new codec and along with the new codec several other Malicious Codes are also downloaded. This means that the end-user will download the new codec believing that something new might happen, whereas the Malicious Code runs in the background causing harm to the host computer. At present, there is no way to verify the authenticity of the codec being downloaded as a new enhancement or a Trojan Horse; therefore, users must avoid unnecessary downloading of new codecs unless they are downloaded from a trusted website. Unnecessary downloading of codecs should also be avoided.

Source: http://www.brighthub.com/computing/smb-security/articles/44811.aspx

A computer worm is a self-replicating malware computer program.[20] It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to security shortcomings on the target computer. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.[18] See Table 4.9 to know more on World's worst worm attacks.

Table 4.9 | The world's worst virus and worm attacks!!!

Sr. No.	*Worm*	*Brief Description*
1	Morris Worm	It is also known as "Great Worm" or Internet Worm. It was written by a student, Robert Tappan Morris, at Cornell University and launched on 2 November 1988 from MIT. It was reported that around 6,000 major Unix machines were infected by the Morris worm and the total cost of the damage calculated was US$ 10–100 millions.
2	ILOVEYOU	It is also known as VBS/Loveletter or Love Bug Worm. It successfully attacked tens of millions of Windows computers in 2000. The E-Mail was sent with the subject line as "ILOVEYOU" and an attachment "LOVE-LETTER-FOR-YOU.TXT.vbs." The file extension "vbs" was hidden, hence the receiver downloads the attachment and opens it to see the contents.
3	Nimda	It is the most widespread computer worm and a file infector. It can affect Internet's within 22 minutes. Nimda affected both user workstations (i.e., clients) running on Windows 95, 98, Me, NT, 2000 or XP and Servers running on Windows NT and 2000. It is "admin" when this worm's name is spelled backward.
4	Code Red	This computer worm was observed on the Internet on 13 July 2001. It attacked computers running on Microsoft's IIS web server. The Code Red worm was first discovered and researched by eEye Digital Security employees, Marc Maiffret and Ryan Permeh. They named the worm Code Red because they were drinking Pepsi's "Mountain Dew Code Red" over the weekend. They analyzed it because of the phrase "Hacked by Chinese!" with which the worm defaced websites. On 4 August 2001 "Code Red II" appeared on the Internet and was found to be a variant of the original Code Red worm.
5	Melissa	It is also known as "Melissa," "Simpsons," "Kwyjibo" or "Kwejeebo." It is a mass-mailing macro worm. Melissa was written by David L. Smith in Aberdeen Township, New Jersey, who named it after a lap dancer he met in Florida. The worm was in a file called "List.DOC" which had passwords that allow the access into 80 pornographic websites. This worm in the original form was sent through an E-Mail to many Internet users. Melissa spread on Microsoft Word 97, Word 2000 and also on Microsoft Excel 97, 2000 and 2003. It can mass-mail itself from E-Mail client Microsoft Outlook 97 or Outlook 98.
6	MSBlast	The Blaster Worm: It is also known as Lovsan or Lovesan, found during August 2003, which spread across the systems running on Microsoft Windows XP and Windows 2000. The worm also creates an entry under OS registry to launch the worm every time Windows starts. This worm contains two messages hidden in strings. The first, "I just want to say LOVE YOU SAN!!" and so the worm sometimes was called "Lovesan worm." The second message, "Billy gates why do you make this possible? Stop making money and fix your software!!" This message was for Bill Gates, the co-founder of Microsoft and target of the worm.
7	Sobig	This worm, found during August 2003, infected millions of Internet-connected computers that were running on Microsoft Windows. It was written in Microsoft Visual C++ and compressed using a data compression tool, "tElock." This Worm not only replicates by itself but also a Trojan Horse that it masquerades as something other than malware. It will appear as an E-Mail with one of the following subjects: • Re: Approved • Re: Details

(*Continued*)

Table 4.9 | (*Continued*)

Sr. No.	*Worm*	*Brief Description*
		• Re: Re: My details • Re: Thank you! • Re: That movie • Re: Wicked screensaver • Re: Your application • Thank you! • Your details It will contain the text as "See the attached file for details" or "Please see the attached file for details." The E-Mail will also contain an attachment by one of the names mentioned below: • application.pif • details.pif • document_9446.pif • document_all.pif • movie0045.pif • thank_you.pif • your_details.pif • your_document.pif • wicked_scr.scr
8	Storm Worm	This worm, found on 17 January 2007, is also known as a backdoor Trojan Horse that affects the systems running on Microsoft OSs. The Storm worm infected thousands of computer systems in Europe and in the US on Friday, 19 January 2007, through an E-Mail with a subject line about a recent weather disaster, "230 dead as storm batters Europe." The worm is also known as: • Small.dam or Trojan-Downloader.Win32.Small.dam • CME-711 • W32/Nuwar@MM and Downloader-BAI • Troj/Dorf and Mal/Dorf • Trojan.DL.Tibs.Gen!Pac13 • Trojan.Downloader-647 • Trojan.Peacomm • TROJ_SMALL.EDW • Win32/Nuwar • Win32/Nuwar.N@MM!CME-711 • W32/Zhelatin • Trojan.Peed, Trojan.Tibs
9	Michelangelo	It is a worm discovered in April 1991 in New Zealand. This worm was designed primarily to infect the systems that were running on disk operating system (DOS) systems. Like other boot sector viruses, Michelangelo operated at the BIOS level and remained dormant until 6 March, the birthday of an artist "Michelangelo di Lodovico Buonarroti Simoni" – an Italian Renaissance painter, sculptor, architect and poet.

(*Continued*)

Table 4.9 | *(Continued)*

Sr. No.	*Worm*	*Brief Description*
10	Jerusalem	This worm is also known as "BlackBox." Jerusalem infected the files residing on DOS that was detected in Jerusalem, Israel, in October 1987. It has become memory resident (using 2 KB of memory). Once the system gets infected then it infects every executable file, except "COMMAND.COM." ".COM" files grow by 1,813 bytes when infected by Jerusalem and are not reinfected. Similarly ".EXE" files grow from 1,808 to 1,823 bytes each time they get infected. Jerusalem reinfects ".EXE" files each time the file is loaded until their size is increased that is found to be "too large to load into memory."

Almost every day new viruses/worms are created and they become new threat to netizens. (See Box 4.4 to know more about viruses.) In summary, in spite of different platforms (i.e., OS and/or applications), a typical definition of computer virus/worms might have various aspects[21] such as:

1. A virus attacks specific file types (or files).
2. A virus manipulates a program to execute tasks unintentionally.
3. An infected program produces more viruses.
4. An infected program may run without error for a long time.
5. Viruses can modify themselves and may possibly escape detection this way.

4.7 Trojan Horses and Backdoors

Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk. A Trojan Horse may get widely redistributed as part of a computer virus.[22] The term Trojan Horse comes from Greek mythology about the Trojan War (see Box 4.5).

Box 4.5 Trojan War

The Trojan Horse is a tale from the Trojan War, as told in Virgil's Latin epic poem *The Aeneid* Quintus of Smyrna. The events in this story from the Bronze Age took place after Homer's *Iliad* and before his *Odyssey*. It was the stratagem that allowed the Greeks finally to enter the city of Troy and end the conflict. In the best-known version, after a fruitless 10-year siege, the Greeks construct a huge wooden horse in an attempt to once and for all destroy Troy from the inside. According to Quintus, it was Odysseus who came up with the idea of building a great wooden horse in which 30 men could hide to be wheeled into the city without the Trojans knowing. The Greeks build a huge, magnificent wooden horse in 3 days under the leadership of Epeios. Odysseus' plan also calls for one man to remain outside of the horse. This man will act as though the Greeks abandoned him, leaving the horse as a gift for the Trojans. The Greeks chose their soldier Sinon to play this role, as he is the only volunteer. Virgil describes the actual encounter between Sinon and the Trojans; Sinon successfully convinces the Trojans that he has been left behind and the Greeks are gone, and the horse is wheeled inside the city walls as a victory trophy. That night, the Greek soldiers hidden inside the horse emerged and opened the city gates for the rest of the Greek army. They raid and destroy the city of Troy, finally ending the Trojan War.

Source: http://en.wikipedia.org/wiki/Trojan_Horse (11 January 10).

Like Spyware and Adware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail or in a bundle with other software downloaded from the Internet. It is also possible to inadvertently transfer malware through a USB flash drive or other portable media. It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines. (Users would not know that these could infect their network while bringing some music along with them to be downloaded.)

Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive. On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.

For example, waterfalls.scr is a waterfall screen saver as originally claimed by the author; however, it can be associated with malware and become a Trojan to unload hidden programs and allow unauthorized access to the user's PC.

Visit http://en.wikipedia.org/wiki/List_of_trojan_horses to get the list of noteworthy Trojan Horses. Some typical examples of threats by Trojans[23] are as follows:

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses (by a dropper Trojan).
3. They deactivate or interfere with antivirus and firewall programs.
4. They allow remote access to your computer (by a remote access Trojan).
5. They upload and download files without your knowledge.
6. They gather E-Mail addresses and use them for Spam.
7. They log keystrokes to steal information such as passwords and credit card numbers.
8. They copy fake links to false websites, display porno sites, play sounds/videos and display images.
9. They slow down, restart or shutdown the system.
10. They reinstall themselves after being disabled.
11. They disable the task manager.
12. They disable the control panel.

4.7.1 Backdoor

A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. However, attackers often use backdoors that they detect or install themselves as part of an exploit. In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack[24]

A backdoor works in background and hides from the user. It is very similar to a virus and, therefore, is quite difficult to detect and completely disable. A backdoor is one of the most dangerous parasite, as it allows a malicious person to perform any possible action on a compromised system. Most backdoors are autonomic malicious programs that must be somehow installed to a computer. Some parasites do not require installation, as their parts are already integrated into particular software running on a remote host. Programmers sometimes leave such backdoors in their software for diagnostics and troubleshooting purposes. Attackers often discover these undocumented features and use them to intrude into the system.

What a Backdoor Does?

Following are some functions of backdoor[25]:

1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands; change any system settings; alter the Windows registry; run, control and terminate applications; install arbitrary software and parasites.

2. It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission (see Section 7.13.7, Chapter 7).
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and tracks web browsing habits.
4. It records keystrokes that a user types on a computer's keyboard and captures screenshots.
5. It sends all gathered data to a predefined E-Mail address, uploads it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.
6. It infects files, corrupts installed applications and damages the entire system.
7. It distributes infected files to remote computers with certain security vulnerabilities and performs attacks against hacker-defined remote hosts.
8. It installs hidden FTP server that can be used by malicious persons for various illegal purposes.
9. It degrades Internet connection speed and overall system performance, decreases system security and causes software instability. Some parasites are badly programmed as they waste too many computer resources and conflict with installed applications.
10. It provides no uninstall feature, and hides processes, files and other objects to complicate its removal as much as possible.

Following are a few examples of backdoor Trojans:

1. **Back Orifice:** It is a well-known example of backdoor Trojan designed for remote system administration. It enables a user to control a computer running the Microsoft Windows OS from a remote location. The name is a word play on Microsoft BackOffice Server software. Readers may visit http://www.cultdeadcow.com/tools/bo.html to know more about backdoor.
2. **Bifrost:** It is another backdoor Trojan that can infect Windows 95 through Vista. It uses the typical server, server builder and client backdoor program configuration to allow a remote attacker, who uses client, to execute arbitrary code on the compromised machine.
3. **SAP backdoors**[26]: SAP is an Enterprise Resource Planning (ERP) system and nowadays ERP is the heart of the business technological platform. These systems handle the key business processes of the organization, such as procurement, invoicing, human resources management, billing, stock management and financial planning. Backdoors can present into SAP User Master that supports an authentication mechanism when a user connects to access SAP and ABAP Program Modules which support SAP Business Objects.
4. **Onapsis Bizploit:** It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs. Bizploit assists security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized ERP penetration tests. Readers may visit http://www.onapsis.com/research.html to know more about this tool.

4.7.2 How to Protect from Trojan Horses and Backdoors

Follow the following steps to protect your systems from Trojan Horses and backdoors:

1. **Stay away from suspect websites/weblinks:** Avoid downloading free/pirated softwares that often get infected by Trojans, worms, viruses and other things. We have addressed "how to determine a legitimate website" in Chapter 5.
2. **Surf on the Web cautiously:** Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats. P2P networks create files packed with malicious software, and then rename them to files with the criteria of common search that are used while surfing the information on the Web.

(See Box 4.6 to know more on P2P networks.) It may be experienced that, after downloading the file, it never works and here is a threat that – although the file has not worked, something must have happened to the system – the malicious software deploys its gizmos and the system is at serious health risk. Enabling Spam filter "ON" is a good practice but is not 100% foolproof, as spammers are constantly developing new ways to get through such filters.

3. **Install antivirus/Trojan remover software:** Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses. Free Trojan remover programs are also available on the Web and some of them are really good.

Box 4.6 Peer-to-Peer (P2P) Networks

Peer-to-peer, commonly abbreviated as P2P, is any distributed network architecture composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances (such as servers or stable hosts). Peers are both suppliers and consumers of resources, in contrast to the traditional client–server model where only servers supply and clients consume.[27]
There are different levels of P2P networking[28]:

1. **Hybrid P2P:** There is a central server that keeps information about the network. The peers are responsible for storing the information. If they want to contact another peer, they query the server for the address.
2. **Pure P2P:** There is absolutely no central server or router. Each peer acts as both client and server at the same time. This is also sometimes referred to as "serverless" P2P.
3. **Mixed P2P:** It is between "hybrid" and "pure" P2P networks. An example of such a network is Gnutella that has no central server but clusters its nodes around so-called "supernodes."

Advantages of P2P Networks

1. It enables faster delivery of information from one computer to another by bypassing a central server.
2. It increases personal efficiency and personal empowerment. Users will no longer have to wait in queues to perform essential tasks, as all activities take place at the user's discretion.
3. It represents significant cost savings over client/server models. As resources and computing power are distributed across the entire network, there is no need for expensive centralized servers; this will reduce the need for centralized management, storage and other related resources.
4. It offers easy scalability and all that is necessary for a network to grow is add more peers.
5. It increases a network's fault tolerance. As no part of the system is essential to its operation, you can take down a few nodes and the network remains functional.
6. It leverages previously unused resources found on hundreds of millions of computers (and other services) that are connected to the "edges" of the Internet.
7. It frees up bandwidth on the Internet (or on a private network). In traditional client–server model, the server is the bottleneck and often cannot handle everything the client requests.
8. It requires no centralized management, oversight or control.
9. It offers increased privacy, as all data and messages are directly exchange between two computers.
10. It results in networks that are more flexible and adaptable compared with traditional client–server networks.

Besides all these advantages, there are still many reasons why P2P might not be the right model and is used only for specific set of activities.

Box 4.6 Peer-to-Peer . . . (*Continued*)

Drawbacks of P2P Networks

1. It propagates all sorts of undesirable items and activities including misinformation.
2. It increases network's, an individual system's, exposure to network attacks, viruses and other malicious damage.
3. It makes no guarantee that content/resources will always be available – any peer can go "dark" if he/she shuts down his/her computer.
4. It does not enforce content ownership (copyright).
5. It cannot enforce standards (either technological or ethical/moral/social).
6. It can be overwhelmed by increased traffic when it is unprepared (Napster uses many clogged university networks).
7. It is plagued by lack of standards, infrastructure and support. It is a kind of "Wild West" of the Internet.
8. Its transactions are difficult to translate into revenues streams and this lack of revenue generation could hinder its future development.

Ares, BitTorrent, Limewire and Kazaa are a few examples of popular P2P file-sharing programs. Readers may visit http://www.bestsecuritytips.com/xfsection+article.articleid+49.htm to know more on these popular P2P file-sharing programs.

Source: www.bus.ucf.edu/leigh/ism5937/linked/Ledesma_J.doc (17 May 2010).

4.8 Steganography

Steganography is a Greek word that means "sheltered writing." It is a method that attempts to hide the existence of a message or communication. The word "steganography" comes from the two Greek words: steganos meaning "covered" and graphein meaning "to write" that means "concealed writing." This idea of data hiding is not a novelty; it has been used for centuries all across the world under different regimes. The practice dates back to ancient Rome and Greece where the messages were etched into wooden tablets and then covered with wax or when messages were passed by shaving a messenger's head and then tattooing a secret message on it, letting his hair grow back and then shaving it again after he arrived at the receiving party to reveal the message.

Given the sheer volume of data stored and transmitted electronically in the world today, it is no surprise that countless methods of protecting such data have evolved. One lesser known but rapidly growing method is steganography, the art and science of hiding information so that it does not even appear to exist! Steganography is always misunderstood with cryptography (see Box 4.7 to know difference between these two techniques). The different names for steganography are data hiding, information hiding (explained in Section 7.12.2, Chapter 7) and digital watermarking.

For example, in a digital image the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Steganography can be used to make a digital watermark to detect illegal copying of digital images. Thus, it aids confidentiality and integrity of the data. *Digital watermarking* is the process of possibly irreversibly embedding information into a digital signal. The signal may be, for example, audio, pictures or video. If the signal is copied then the information is also carried in the copy.[29]

Box 4.7 Difference between Steganography and Cryptography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. It is said that terrorists use steganography techniques to hide their communication in images on the Internet; most popular images are used such as those of film actresses or other celebrities. In its basic form, steganography is simple. For example, say every fourth letter of a memo could hide a message. This simple technique has an added advantage over encryption that it does not arouse suspicion, that is, there is not much scope for getting started an investigation! Presence of an encryption could set off an investigation, but a message hidden in plain sight would get ignored (see Box 7.13, Chapter 7).

In October 2001, the New York Times published an article claiming that al-Qaeda had used steganographic techniques to encode messages into images, and then transported these via E-Mail and possibly via Usenet to prepare and execute the 11 September 2001 Terrorist Attack.[30]

The term "cover" or "cover medium" is used to describe the original, innocent message, data, audio, still, video and so on. It is the medium that hides the secret message (see Fig. 4.4). It must have parts that can be altered or used without damaging or noticeably changing the cover media. If the cover media are digital, these alterable parts are called "redundant bits." These bits or a subset can be replaced with the message that is intended to be hidden. Interestingly, steganography in digital media is very similar to "digital watermarking." In other words, when steganography is used to place a hidden "trademark" in images, music and software, the result is a technique referred to as "watermarking" (see Table 4.10 to know more about steganography tools).

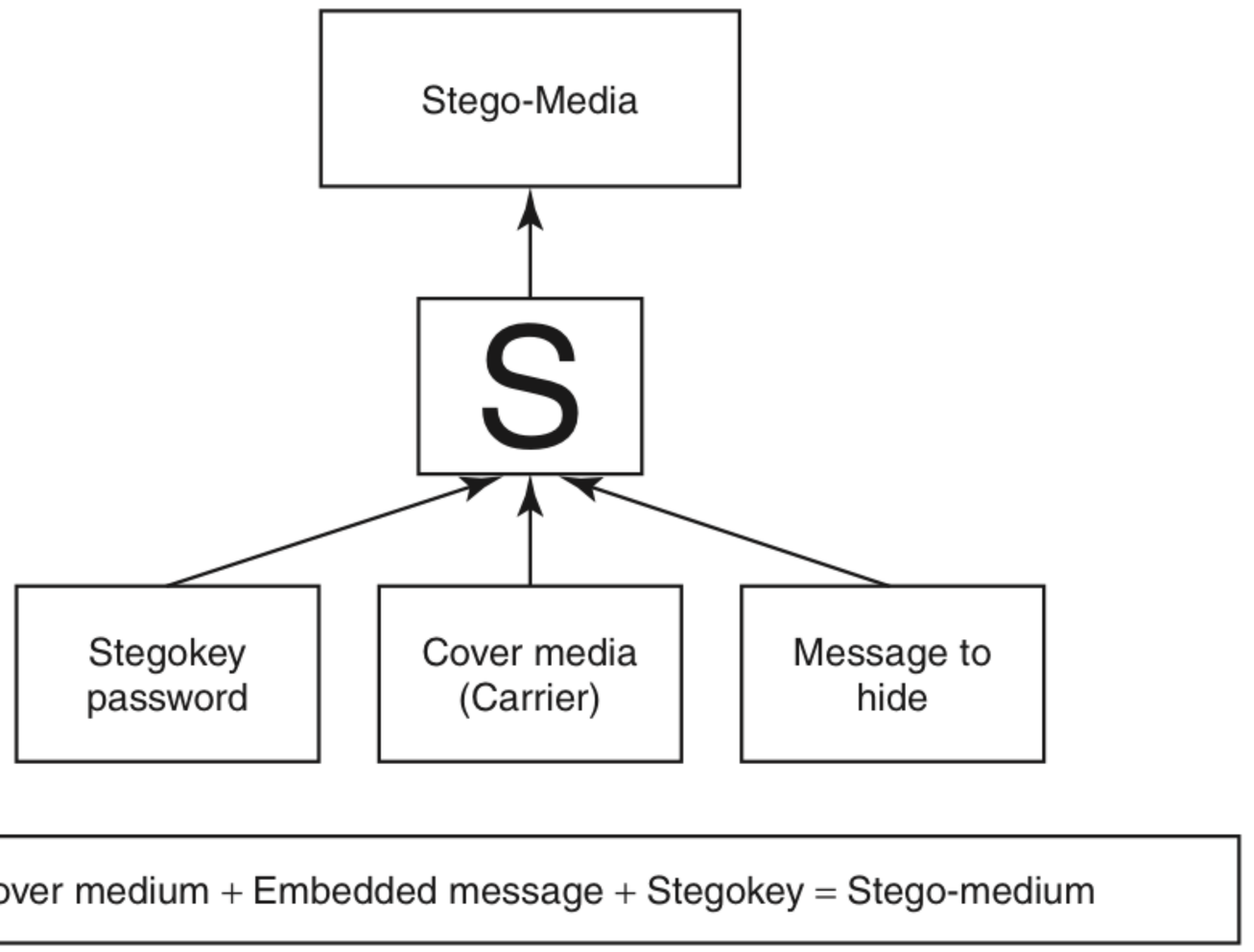

Figure 4.4 How steganography works.
Source: http://www.cosc.iup.edu/sezekiel/Seminar/steg.ppt#452,15,Steganography%20of%20today's%20talk (11 May 10).

Table 4.10 | Steganography tools

Website	*Brief Description*
http://www.securityfocus.com	**DiSi-Steganograph:** It is a very small, DOS-based steganographic program that embeds data in PCX images.
http://www.brothersoft.com/invisible-folders-54597.html	**Invisible Folders:** It has the ability to make any file or folder invisible to anyone using your PC even on a network.
http://www.invisiblesecrets.com	**Invisible Secrets:** It not only encrypts the data and files for safe-keeping or for secure transfer across the Net but also hides them in places such as picture or sound files or webpages. These types of files are a perfect disguise for sensitive information.
http://www.programurl.com/stealth-files.htm	**Stealth Files:** It hides any type of file in almost any other type of file. Using steganography technique, Stealth Files compresses, encrypts and then hides any type of file inside various types of files (including EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, BMP) and other types of video, image and executable files.
http://www.programurl.com/hermetic-stego.htm	**Hermetic Stego:** It is a steganography program that allows to encrypt and hide contents of any data file in another file so that the addition of the data to the container file will not noticeably change the appearance of that file. This program allows hiding a file of any size in one or more BMP image files with or without the use of a user-specified stego/encryption key so that (a) the presence of the hidden file is undetectable (even by forensic software using statistical methods) and (b) if a user-specified stego key is used then the hidden file can be extracted only by someone, using this software, who knows that stego key.
http://www.securstar.com/products_drivecryptpp.php	**DriveCrypt Plus (DCPP):** It has following features: • It allows secure hiding of an entire OS inside the free space of another OS. • Full-disk encryption (encrypts parts or 100% of your hard disk including the OS). • Preboot authentication (before the machines boots, a password is requested to decrypt the disk and start your machine).
http://www.petitcolas.net/fabien/steganography/mp3stego	**MP3Stego:** It hides information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream.
http://compression.ru/video/stego_video/index_en.html	**MSU StegoVideo:** It allows hiding any file in a video sequence. Main features are as follows: • Small video distortions after hiding information. • It is possible to extract information after video compression. • Information is protected with the password.

Steganography, Sudoku Puzzle and SMS: It is a revised version of information hiding (i.e., steganography) using Sudoku puzzle. This methodology was proposed by Chang *et al.* during 2008, which was inspired by Zhang and Wang's method and Sudoku solutions. Sudoku game has gained popularity recently and SMS is a popular medium of communication nowadays – messages are concealed into Suduko puzzle, which are then communicated to intended recipient through SMS. As soon as recipient solves the puzzle, he/she can extract the data hidden into Sudoko puzzle image.

4.8.1 Steganalysis

Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography. The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them, and if possible recover it. Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files (see Table 4.11 for more details).

4.9 DoS and DDoS Attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource (i.e., information systems) unavailable to its intended users.

4.9.1 DoS Attacks

In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent the Internet site or service from functioning efficiently or at all, temporarily or indefinitely. The attackers typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, mobile phone networks and even root name servers (i.e., domain name

Table 4.11 | Steganalysis tools

Website	*Brief Description*
http://www.sarc-wv.com/products/stegalyzeras.aspx	**StegAlyzerAS:** It is a digital forensic analysis tool designed to scan "suspect media" or "forensic images" of suspect media for known artifacts of steganography applications.
http://www.sarc-wv.com/stegalyzerss.aspx	**StegAlyzerSS:** It is a digital forensic analysis tool designed to scan "suspect media" or "forensic images" of suspect media for uniquely identifiable hexadecimal byte patterns, or known signatures, left inside files when particular steganography applications are used to embed hidden information within them.
http://www.spy-hunter.com/stegspydownload.htm	**StegSpy:** It is a program that is always in progress and the latest version includes identification of a "steganized" file. It detects steganography and the program used to hide the message. The latest version also identifies the location of the hidden content as well. StegSpy identifies programs such as Hiderman, JPHideandSeek, Masker, JPegX and Invisible Secrets.
http://www.outguess.org/detection.php	**Stegdetect:** It is an automated tool for detecting steganographic content in the images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images.
http://stegsecret.sourceforge.net	**Stegsecret:** It is a steganalysis open-source project that makes detection of hidden information possible in different digital media. It is a JAVA-based multiplatform steganalysis tool that allows the detection of hidden information by using the most known steganographic methods.
http://sourceforge.net/projects/vsl	**Virtual Steganographic Laboratory (VSL):** It is a graphical block diagramming tool that allows complex using, testing and adjusting of methods both for image steganography and steganalysis.

servers). Buffer overflow technique is employed to commit such kind of criminal attack known as *Spoofing*. The term IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the ID of the sender or impersonating another computing system. A packet is a formatted unit of data carried by a packet mode computer network. The attacker spoofs the IP address and floods the network of the victim with repeated requests. As the IP address is fake, the victim machine keeps waiting for response from the attacker's machine for each request. This consumes the bandwidth of the network which then fails to serve the legitimate requests and ultimately breaks down.

The United States Computer Emergency Response Team defines symptoms of DoS attacks to include:

1. Unusually slow network performance (opening files or accessing websites);
2. unavailability of a particular website;
3. inability to access any website;
4. dramatic increase in the number of Spam E-Mails received (this type of DoS attack is termed as an E-Mail bomb).

The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it. A DoS attack may do the following:

1. Flood a network with traffic, thereby preventing legitimate network traffic.
2. Disrupt connections between two systems, thereby preventing access to a service.
3. Prevent a particular individual from accessing a service.
4. Disrupt service to a specific system or person.

4.9.2 Classification of DoS Attacks

See Table 4.12 for classification of DoS attacks.

Table 4.12 | Classification of DoS attacks

Sr. No.	*DoS Attacks*	*Brief Description*
1	Bandwidth attacks	Loading any website takes certain time. Loading means complete webpage (i.e., with entire content of the webpage – text along with images) appearing on the screen and system is awaiting user's input. This "loading" consumes some amount of memory. Every site is given with a particular amount of bandwidth for its hosting, say for example, 50 GB. Now if more visitors consume all 50 GB bandwidth then the hosting of the site can ban this site. The attacker does the same – he/she opens 100 pages of a site and keeps on refreshing and consuming all the bandwidth, thus, the site becomes out of service.
2	Logic attacks	These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.
3	Protocol attacks	Protocols here are rules that are to be followed to send data over network. These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victim's system to consume excess amounts of its resources.
4	Unintentional DoS attack	This is a scenario where a website ends up denied not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity. This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a news story. The result is that a significant proportion of the primary sites regular users', potentially hundreds of thousands of people, click that link within a few hours and have the same effect on the target website as a DDoS attack.

4.9.3 Types or Levels of DoS Attacks

There are several types or levels of DoS attacks as follows:

1. **Flood attack:** This is the earliest form of DoS attack and is also known as *ping flood*. It is based on an attacker simply sending the victim overwhelming number of ping packets, usually by using the "ping" command, which result into more traffic than the victim can handle. This requires the attacker to have a faster network connection than the victim (i.e., access to greater bandwidth than the victim). It is very simple to launch, but to prevent it completely is the most difficult.
2. **Ping of death attack:** The ping of death attack sends oversized Internet Control Message Protocol (ICMP) packets, and it is one of the core protocols of the IP Suite. It is mainly used by networked computers' OSs to send error messages indicating (e.g., that a requested service is not available or that a host or router could not be reached) datagrams (encapsulated in IP packets) to the victim. The maximum packet size allowed is of 65,536 octets. Some systems, upon receiving the oversized packet, will crash, freeze or reboot, resulting in DoS (e.g., the ping of death attack relied on a bug in the Berkeley TCP/IP stack, which also existed on most systems that copied the Berkeley network code).
3. **SYN attack:** It is also termed as *TCP SYN Flooding*. In the Transmission Control Protocol (TCP), handshaking of network connections is done with SYN and ACK messages. An attacker initiates a TCP connection to the server with an SYN (using a legitimate or spoofed source address). The server replies with an SYN-ACK. The client then does not send back an ACK, causing the server (i.e., target system) to allocate memory for the pending connection and wait. This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system. Figure 4.5 explains how the DoS attack takes place.

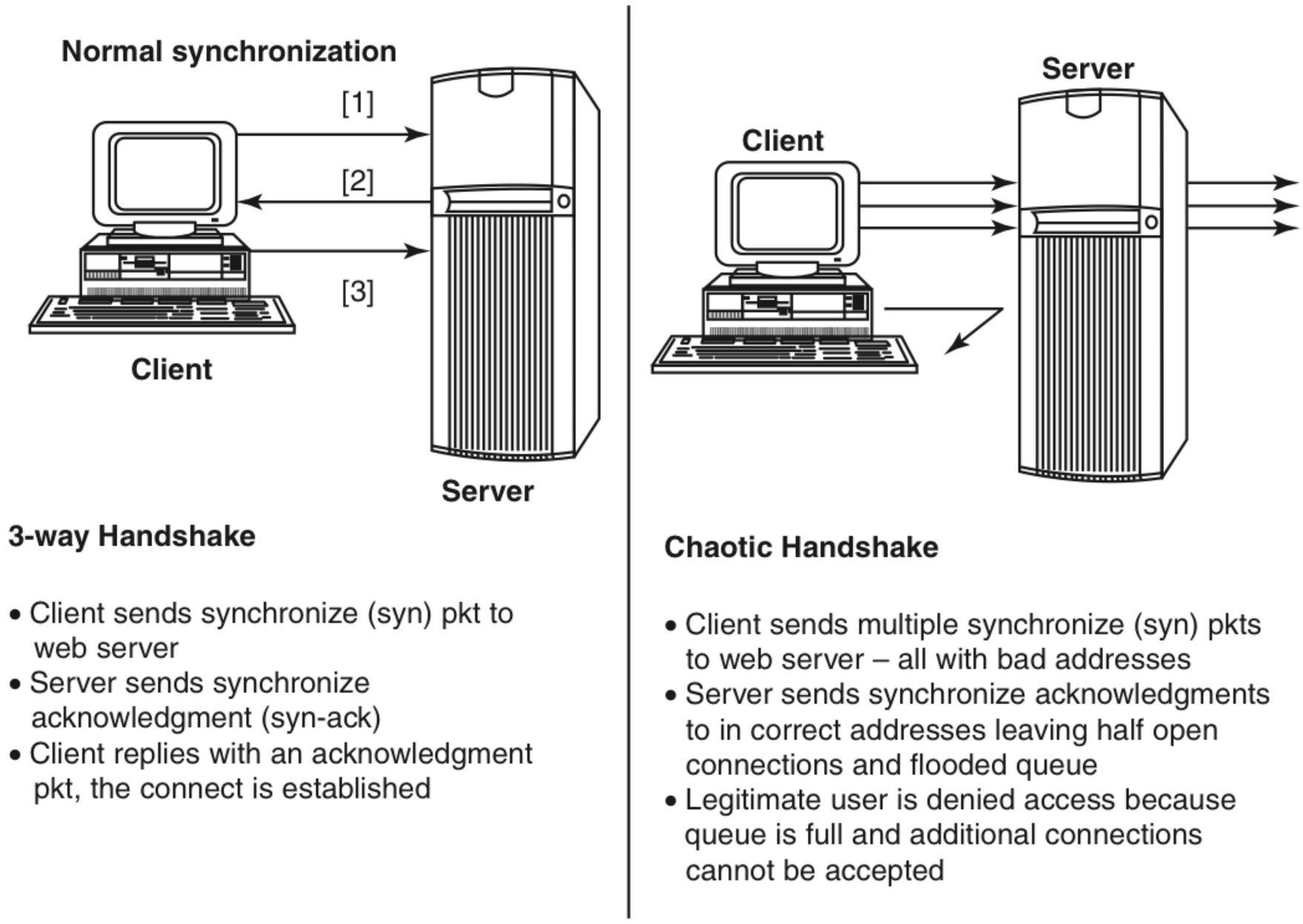

Figure 4.5 | Denial-of-service (DoS) attack.

4. **Teardrop attack:** The teardrop attack is an attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim and may hang the system. This attack can crash various OSs due to a bug in their TCP/IP fragmentation reassembly code. Windows 3.1x, Windows 95 and Windows NT OSs as well as versions of Linux (i.e., prior to versions 2.0.32 and 2.1.63) are vulnerable to this attack.[31]
5. **Smurf attack:** It is a way of generating significant computer network traffic on a victim network. This is a type of DoS attack that floods a target system via spoofed broadcast ping messages. This attack consists of a host sending an ICMP echo request (ping) to a network broadcast address (e.g., network addresses with the host portion of the address having all 1s). Every host on the network receives the ICMP echo request and sends back an ICMP echo response inundating the initiator with network traffic. On a multi-access broadcast network, hundreds of machines might reply to each packet. This creates a magnified DoS attack of ping replies, flooding the primary victim. Internet relay chat (IRC) servers are the primary victim of smurf attacks on the Internet [(IRC is a form of real-time Internet text messaging (chat) or synchronous conferencing)].
6. **Nuke:** Nuke[32] is an old DoS attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target. It is achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop. A specific example of a nuke attack that gained some prominence is the WinNuke, which exploited the vulnerability in the NetBIOS handler in Windows 95. A string of out-of-band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a *B*lue *S*creen *o*f *D*eath (BSOD).

4.9.4 Tools Used to Launch DoS Attack

Various tools (see Table 4.13) use different types of traffic to flood a victim, but the objective behind the attack and the result is the same: A service on the system or the entire system (i.e., application/website/network) is unavailable to a user because it is kept busy trying to respond to an exorbitant number of requests. A DoS attack is usually an attack of last resort because it is considered to be an unsophisticated attack as the attacker does not gain access to any information but rather annoys the target and interrupts the service. (See Box 4.8 to know more about blended threats and Box 4.9 for PDoS attacks.)

Table 4.13 | Tools used to launch DoS attack

Sr. No.	*Tool*	*Brief Description*
1	Jolt2	A major vulnerability has been discovered in Windows' networking code. The vulnerability allows remote attackers to cause a DoS attack against Windows-based machines – the attack causes the target machine to consume 100% of the CPU time on processing of illegal packets.
2	Nemesy	This program generates random packets of spoofed source IP to enable the attacker to launch DoS attack.
3	Targa	It is a program that can be used to run eight different DoS attacks. The attacker has the option to launch either individual attacks or try all the attacks until one is successful.
4	Crazy Pinger	This tool could send large packets of ICMP to a remote target network.
5	SomeTrouble	It is a remote flooder and bomber. It is developed in Delphi.

Box 4.8 Blended Threat

Blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan Horses and Malicious Code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate, transmit and thereafter spread an attack. Characteristics of blended threats are that

1. They cause harm to the infected system or network.
2. They propagate using multiple methods as attack may come from multiple points.
3. They also exploit vulnerabilities.

To be considered a blended threat, the attack would normally serve to transport multiple attacks in one payload. For example, it would not only just launch a DoS attack but it would also, for example, install a backdoor and maybe even damage a local system in one shot. Additionally, blended threats are designed to use multiple modes of transport. Therefore, while a worm may travel and spread through E-Mail, a single blended threat could use multiple routes including E-Mail, IRC and file-sharing networks.

Finally, rather than a specific attack on predetermined ".exe" files, a blended threat could do multiple malicious acts, such as modify your ".exe" files, HTML files and registry keys at the same time – basically it can cause damage to several areas of your network at one time.

Blended threats are considered to be the worst risk to security since the inception of viruses, as most blended threats require no human intervention to propagate.

Source: http://www.webopedia.com/didyouknow/internet/2004/virus.asp (11 January 2010).

Box 4.9 Permanent Denial-of-Service (PDoS) Attack

A PDoS attack damages a system so badly that it requires replacement or reinstallation of hardware. Unlike DDoS attack – which is used to sabotage a service or website or as a cover for malware delivery – PDoS is a pure hardware sabotage. It exploits security flaws that allow remote administration on the management interfaces of the victim's hardware, such as routers, printers or other networking hardware. The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt or defective firmware image – a process which when done legitimately is known as *flashing*. Owing to these features, and the potential and high probability of security exploits on network-enabled-embedded devices (NEEDs), this technique has come to the attention of numerous hacker communities. PhlashDance is a tool created by Rich Smith (an employee of Hewlett-Packard's Systems Security Lab) who detected and demonstrated PDoS vulnerabilities at the 2008 EUSecWest Applied Security Conference in London.

Source: http://en.wikipedia.org/wiki/Denial-of-service_attack (11 May 2010).

4.9.5 DDoS Attacks

In a DDoS attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the DoS attack.

A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems (as explained in Chapter 1) are called "secondary victims" and the main target is called "primary victim."

Table 4.14 | Tools used to launch DDoS attack

Sr. No.	*Tool*	*Brief Description*
1	Trinoo	It is a set of computer programs to conduct a DDoS attack. It is believed that Trinoo networks have been set up on thousands of systems on the Internet that have been compromised by remote buffer overrun exploit.
2	Tribe Flood Network (TFN)	It is a set of computer programs to conduct various DDoS attacks such as ICMP flood, SYN flood, UDP flood and Smurf attack.
3	Stacheldraht	It is written by Random for Linux and Solaris systems, which acts as a DDoS agent. It combines features of Trinoo with TFN and adds encryption.
4	Shaft	This network looks conceptually similar to a Trinoo; it is a packet flooding attack and the client controls the size of the flooding packets and duration of the attack.
5	MStream	It uses spoofed TCP packets with the ACK flag set to attack the target. Communication is not encrypted and is performed through TCP and UDP packets. Access to the handler is password protected. This program has a feature not found in other DDoS tools. It informs all connected users of access, successful or not, to the handler(s) by competing parties.

Malware can carry DDoS attack mechanisms – one of the better-known examples of this is MyDoom. Typically, DoS mechanism triggered on a specific date and time. This type of DDoS attacks involves hardcoding the target IP address prior to release of the malware, hence no further interaction is necessary to launch the attack. A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent. Nowadays, Botnet (as explained in Chapter 2) is the popular medium to launch DoS/DDoS attacks. Attackers can also break into systems using automated tools (see Table 4.14) that exploit flaws in programs that listen for connections from remote hosts.

4.9.6 How to Protect from DoS/DDoS Attacks

Computer Emergency Response Team Coordination Center (CERT/CC) offers many preventive measures from being a victim of DoS attack.[33]

1. Implement router filters. This will lessen your exposure to certain DoS attacks.
2. If such filters are available for your system, install patches to guard against TCP SYN flooding.
3. Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.
4. Enable quota systems on your OS if they are available.
5. Observe your system's performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, central processing unit (CPU) usage or network traffic.
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files (see Table 4.15).
8. Invest in and maintain "hot spares" – machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.
11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

Table 4.15 | Tools for detecting DoS/DDoS attacks

Sr. No.	*Tool*	*Brief Description*
1	Zombie Zapper	It is a free, open-source tool that can tell a zombie system flooding packets to stop flooding. It works against Trinoo, TFN and Stacheldraht. It assumes various defaults are still in place used by these attack tools, however, it allows you to put the zombies to sleep.
2	Remote Intrusion Detector (RID)	It is a tool developed in "C" computer language, which is a highly configurable packet snooper and generator. It works by sending out packets defined in the config.txt file, then listening for appropriate replies. It detects the presence of Trinoo, TFN or Stacheldraht clients.
3	Security Auditor's Research Assistant (SARA)	It gathers information about remote hosts and networks by examining network services. This includes information about the network information services as well as potential security flaws such as incorrectly set up or configured network services, well-known bugs in the system or network utilities system software vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database and weak policy decisions.
4	Find_DDoS	It is a tool that scans a local system that likely contains a DDoS program. It can detect several known DoS attack tools.
5	DDoSPing	It is a remote network scanner for the most common DDoS programs. It can detect Trinoo, Stacheldraht and Tribe Flood Network programs running with their default settings.

Computer Emergency Response Team Coordination Center (CERT/CC) was started in December 1988 by the Defense Advanced Research Projects Agency, which was part of the US Department of Defense, after the Morris Worm disabled about 10% of all computers connected to the Internet. It is located at the Software Engineering Institute, a federally funded research center operated by Carnegie Mellon University. It studies Internet security vulnerabilities and provides services to websites that have been attacked. It also publishes security alerts.

Source: http://www.webopedia.com/TERM/C/CERTCC.html (31 May 2010).

4.10 SQL Injection

Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS). SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.[34]

Attackers target the SQL servers – common database servers used by many organizations to store confidential data. The prime objective behind SQL injection attack is to obtain the information while accessing a database table that may contain personal information such as credit card numbers, social security numbers or passwords. During an SQL injection attack, Malicious Code is inserted into a web form

field or the website's code to make a system execute a command shell or other arbitrary commands. Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field. For example, an arbitrary command from an attacker might open a command prompt or display a table from the database. This makes an SQL server a high-value target and therefore a system seems to be very attractive to attackers.

The attacker determines whether a database and the tables residing into it are vulnerable, before launching an attack. Many webpages take parameters from web user and make SQL query to the database. For example, when a user logs in with username and password, an SQL query is sent to the database to check if a user has valid name and password. With SQL injection, it is possible for an attacker to send crafted username and/or password field that will change the SQL query.

4.10.1 Steps for SQL Injection Attack

Following are some steps for SQL injection attack:

1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc. The attacker also looks for the webpages that display the HTML commands such as POST or GET by checking the site's source code.
2. To check the source code of any website, right click on the webpage and click on "view source" (if you are using IE – Internet Explorer) – source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for "FORM" tag in the HTML code. Everything between the <FORM> and </FORM> have potential parameters that might be useful to find the vulnerabilities.
   <FORM action=Search/search.asp method=post>
   <input type=hidden name=A value=C>
   </FORM>
3. The attacker inputs a *single quote* under the text box provided on the webpage to accept the username and password. This checks whether the user-input variable is sanitized or interpreted literally by the server. If the response is an error message such as *use "a" = "a"* (or something similar) then the website is found to be susceptible to an SQL injection attack.
4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

Here are few examples of variable field text the attacker uses on a webpage to test for SQL vulnerabilities:

1. *Blah' or 1=1--*
2. *Login:blah' or 1=1--*
3. *Password::blah' or 1=1--*
4. *http://search/index.asp?id=blah' or 1=1--*

Similar SQL commands may allow bypassing of a login and may return many rows in a table or even an entire database table because the SQL server is interpreting the terms literally. The double dashes near the end of the command tell SQL to ignore the rest of the command as a comment.

Blind SQL Injection

Blind SQL injection[34] is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be the one that displays data; however, it will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack can become time-intensive because a new statement must be crafted for each bit recovered. There are several tools that can automate these attacks once the location

of the vulnerability and the target information have been established. Readers may refer to Ref. #7, Additional Useful Web References, Further Reading to know about white paper.

In summary, using SQL injections, attackers can:

1. Obtain some basic information if the purpose of the attack is reconnaissance
   - To get a directory listing: Blah' ;exec master..xp_cmdshell "dir c:*.* /s >c:\directory.txt";
   - To ping an IP address: Blah' ;exec master..xp_cmdshell "ping 192.168.1.1".
2. May gain access to the database by obtaining username and their password
   - To get a user listing: SELECT * FROM users WHERE name = "OR '1' = '1'."
3. Add new data to the database
   - Execute the INSERT command: This may enable selling politically incorrect items on an E-Commerce website.
4. Modify data currently in the database
   - Execute the UPDATE command: May be used to have an expensive item suddenly be deeply "discounted."

mySQLenum: It is a command line automatic blind SQL injection tool for web application that uses MySQl server as its back-end. The main objective of this tool is to provide an easy-to-use command line interface. Readers may visit http://pentestit.com/2010/01/15/mysqlenum-automatic-blind-sql-injection-tool/ to know more on this tool.

See Table 4.16 to know some automated tools that are used either to find database vulnerabilities and/or to protect the database applications.

Table 4.16 | Tools used for SQL Server penetration

Sr. No.	*Tool*	*Brief Description*
1	http://www.appsecinc.com	**AppDetectivePro:** It is a network-based, discovery and vulnerability assessment scanner that discovers database applications within the infrastructure and assesses security strength. It locates, examines, reports and fixes security holes and misconfigurations as well as identify user rights and privilege levels based on its security methodology and extensive knowledge based on application-level vulnerabilities. Thus, organizations can harden their database applications.
2	http://www.appsecinc.com	**DbProtect:** It enables organizations with complex, heterogeneous environments to optimize database security, manage risk and bolster regulatory compliance. It integrates database asset management, vulnerability management, audit and threat management, policy management, and reporting and analytics for a complete enterprise solution.
3	http://www.iss.net	**Database Scanner:** It is an integrated part of Internet Security Systems' (ISS) Dynamic Threat Protection platform that assesses online business risks by identifying security exposures in the database applications. Database scanner offers security policy generation and reporting functionality, which instantly measures policy compliance and automates the process of securing critical online business data. Database scanner runs independently of the database and quickly generates detailed reports with all the information needed to correctly configure and secure databases.

(*Continued*)

Table 4.16 | *(Continued)*

Sr. No.	*Tool*	*Brief Description*
4	http://www.ca.com/us/securityadvisor	**SQLPoke:** It is an NT-based tool that locates Microsoft SQL (MSSQL) servers and tries to connect with the default System Administrator (SA) account. A list of SQL commands are executed if the connection is successful.
5	http://www.ngssoftware.com/	**NGSSQLCrack:** It can guard against weak passwords that make the network susceptible to attack. This is a password cracking utility for Microsoft SQL server 7 and 2000 and identifies user accounts with weak passwords so that they can be reset with stronger ones, thus, protecting the overall integrity of the system.
6	http://www.security-database.com/toolswatch	**Microsoft SQL Server Fingerprint (MSSQLFP) Tool:** This is a tool that performs fingerprinting version on Microsoft SQL Server 2000, 2005 and 2008, using well-known techniques based on several public tools that identifies the SQL version and also can be used to identify vulnerable versions of Microsoft SQL Server

4.10.2 How to Prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. **Input validation**
   - Replace all single quotes (escape quotes) to two single quotes.
   - Sanitize the input: User input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously. For example, character sequences such as ; , --, select, insert and xp_ can be used to perform an SQL injection attack.
   - Numeric values should be checked while accepting a query string value. Function – IsNumeric() for Active Server Pages (ASP) should be used to check these numeric values.
   - Keep all text boxes and form fields as short as possible to limit the length of user input.
2. **Modify error reports:** SQL errors should not be displayed to outside users and to avoid this, the developer should handle or configure the error reports very carefully. These errors some time display full query pointing to the syntax error involved and the attacker can use it for further attacks.
3. **Other preventions**
   - The default system accounts for SQL server 2000 should never be used.
   - Isolate database server and web server. Both should reside on different machines.
   - Most often attackers may make use of several extended stored procedures such as xp_cmdshell and xp_grantlogin in SQL injection attacks. In case such extended stored procedures are not used or have unused triggers, stored procedures, user-defined functions, etc., then these should be moved to an isolated server.

These are the minimum countermeasures that can be implemented to prevent SQL injection attack. Technocrats may want to know more on this topic and can go through Refs. #8 and #9, Additional Useful Web References.

SQLBlock: SQLBlock is an open data base connectivity (ODBC) driver that acts as an SQL injection protection feature. It blocks the execution and sends an alert to administrator, in case of any client-application attempt to execute any disallowed SQL statements. It works as an ordinary ODBC data source and monitor every SQL statements being executed.

4.11 Buffer Overflow

Buffer overflow, or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory the programmer has set aside for it. The extra data overwrites adjacent memory, which may contain other data, including program variables and program flow control data. This may result in erratic program behavior, including memory access errors, incorrect results, program termination (a crash) or a breach of system security.

Buffer overflows can be triggered by inputs that are designed to execute code or alter the way the program operates. They are, thus, the basis of many software vulnerabilities and can be maliciously exploited. Bounds checking can prevent buffer overflows.

Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type), which is within the boundaries of that array.[35]

Buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. As buffers are created to contain a finite amount of data, the extra information – which has to go somewhere – can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

The knowledge of C, C++ or any other high-level computer language (i.e., assembly language) is essential to understand buffer overflow, as basic knowledge of process memory layout is very important. A buffer is a contiguous allocated chunk of memory such as an array or a pointer in C. In C and C++, there are no automatic bounds checking on the buffer – which means a user can write past a buffer. For example,

```
int main () {
int buffer[10];
buffer[20] = 10;
}
```

This C program is a valid program and every compiler can compile it without any errors. However, the program attempts to write beyond the allocated memory for the buffer, which might result in an unexpected behavior.

4.11.1 Types of Buffer Overflow

Stack-Based Buffer Overflow

Stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside the intended data structure – usually a fixed length buffer. Here are the characteristics of stack-based programming:

1. "Stack" is a memory space in which automatic variables (and often function parameters) are allocated.
2. Function parameters are allocated on the stack (i.e., local variables that are declared on the stack – unless they are also declared as "static" or "register") and are not automatically initialized by the system, so they usually have garbage in them until they are initialized.

3. Once a function has completed its cycle, the reference to the variable in the stack is removed. (Therefore, if a function is called multiple times, its local variables and parameters are recreated and destroyed each time the function is called and exited.)

The attacker may exploit stack-based buffer overflows to manipulate the program in various ways by overwriting:

1. A local variable that is near the buffer in memory on the stack to change the behavior of the program that may benefit the attacker.
2. The return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input-filled buffer.
3. A function pointer, or exception handler, which is subsequently executed.

The factors that contribute to overcome the exploits are

1. Null bytes in addresses;
2. variability in the location of shellcode;
3. differences between environments.

A shellcode is a small piece of code used as a payload in the exploitation of software vulnerability. It is called "shellcode" because it starts with command shell from which the attacker can control the compromised machine.

NOPs

NOP or NOOP (short form of no peration or no operation performed) is an assembly language instruction/command that effectively does nothing at all. The explicit purpose of this command is not to change the state of status flags or memory locations in the code. This means NOP enables the developer to force memory alignment to act as a place holder to be replaced by active instructions later on in program development.

NOP opcode can be used to form an NOP slide, which allows code to execute when the exact value of the instruction pointer is indeterminate (e.g., when a buffer overflow causes a function's return address on the stack to be overwritten). It is the oldest and most widely used technique for successfully exploiting a stack buffer overflow. It helps to know/locate the exact address of the buffer by effectively increasing the size of the target stack buffer area. The attacker can increase the odds of findings the right memory address by padding his/her code with NOP operation. To do this, much larger sections of the stack are corrupted with the NOOP machine instruction. At the end of the attacker-supplied data, after the NOOP instructions, an instruction is placed to perform a relative jump to the top of the buffer where the shellcode is located. This collection of NOOP is referred to as the "NOP sled" because if the return address is overwritten with any address within the NOOP region of the buffer then it will "slide" down the NOOP until it is redirected to the actual Malicious Code by the jump at the end. This technique requires the attacker to guess where in the stack the NOP sled is compared with small shellcode.

Owing to the popularity of this technique, many vendors of intrusion prevention system will search for this pattern of NOOP machine instructions in an attempt to detect shellcode in use. It is important to note that an NOP sled does not necessarily contain only traditional NOOP machine instructions but also any instruction that does not corrupt the state of machine to a point where the shellcode will not run and can be used in place of the hardware-assisted NOOP. As a result, it has become common practice for exploit writers to compose the NOOP sled with randomly chosen instructions that will have no real effect on the shellcode execution.[35]

Heap Buffer Overflow

Heap buffer overflow occurs in the heap data area and may be introduced accidentally by an application programmer, or it may result from a deliberate exploit. In either case, the overflow occurs when an application copies more data into a buffer than the buffer was designed to contain. A routine is vulnerable to exploitation if it copies data to a buffer without first verifying that the source will fit into the destination. The characteristics of stack-based and heap-based programming are as follows:

1. "Heap" is a "free store" that is a memory space, where dynamic objects are allocated.
2. The heap is the memory space that is dynamically allocated new(), malloc() and calloc() functions; it is different from the memory space allocated for stack and code.
3. Dynamically created variables (i.e., declared variables) are created on the heap before the execution program is initialized to zeros and are stored in the memory until the life cycle of the object has completed.

Memory on the heap is dynamically allocated by the application at run-time and normally contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers. The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as malloc metadata) and uses the resulting pointer exchange to overwrite a program function pointer.

4.11.2 How to Minimize Buffer Overflow

Although it is difficult to prevent all possible attacks, the following methods will definitely help to minimize such attacks:

1. **Assessment of secure code manually:** Buffer overflow occurs when a program or process tries to store more data in a buffer than it was intended to hold. Developers should be educated about minimizing the use of vulnerable functions available in C library, such as strcpy(), strcat(), sprintf() and vsprintf(), which operate on null-terminated strings and perform no bounds checking. The input validation after scanf() function that reads user input into a buffer is very essential.
2. **Disable stack execution:** Malicious Code causes input argument to the program, and it resides in the stack and not in the code segment. Any code that attempts to execute any other code residing in the stack will cause a segmentation violation. Therefore, the simplest solution is to invalidate the stack to execute any instructions. However, the solution is not easy to implement. Although possible in Linux, some compilers [(including GNU Compliance Connection (GCC)] use trampoline functions to implement taking the address of a nested function that works on the system stack being executable. A trampoline is a small piece of code created at run-time when the address of a nested function is taken. It normally resides in the stack and in the stack frame of the containing function and thus requires the stack to be executable. However, a version of the Linux kernel that enforces the non-executable stack is freely available.
3. **Compiler tools:** Over the years, compilers have become more and more aggressive in optimizations and the checks they perform. Various compiler tools already offer warnings on the use of unsafe constructs such as gets(), strcpy(), etc. Developers should be educated to restructure the programming code if such warnings are displayed.
4. **Dynamic run-time checks:** In this scheme, an application has restricted access to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed. This preloaded component can either provide safer versions of the standard unsafe functions or

Table 4.17 | Tools used to defend/protect buffer overflow

Sr. No.	*Tool*	*Brief Description*
1	**StackGuard**	It was released for GCC in 1997 and published at USENIX Security 1998. It is an extension to GCC that provides buffer overflow protection. It was invented by Crispin Cowan. It is a compiler approach for defending programs and systems against "stack-smashing" attacks. These attacks are the most common form of security vulnerability. Programs that have been compiled with StackGuard are largely immune to stack-smashing attack. Whenever vulnerability is exploited, it detects the attack in progress, raises an intrusion alert and halts the victim program.
2	**ProPolice**	The "stack-smashing protector" or SSP, also known as ProPolice, is an enhancement of the StackGuard concept written and maintained by Hiroaki Etoh of IBM. Its name derives from the word propolis. The stack protection provided by ProPolice is specifically for the C and C++ languages. It is also optionally available in Gentoo Linux with the hardened USE flag.
3	**LibSafe**	It was released in April 2000 and gained popularity in the Linux community. It does not need access to the source code of the program to be protected. Libsafe protection is system wide and automatically gets attached to the applications. It is based on a middle-ware software layer that intercepts all function calls made to library functions known to be vulnerable. A substitute version of the corresponding function implements the original function in a way that ensures that any buffer overflows are contained within the current stack frame, which prevents attackers from overwriting the return address and hijacking the control flow of a running program. The real benefit of using libsafe is protection against future attacks on programs not yet known to be vulnerable.

it can ensure that return addresses are not overwritten. One example of such a tool is libsafe. The libsafe library provides a way to secure calls to these functions, even if the function is not available. It makes use of the fact that stack frames are linked together by frame pointers. When a buffer is passed as an argument to any of the unsafe functions, libsafe follows the frame pointers to the correct stack frame. It then checks the distance to the nearest return address and when the function executes, it makes sure that address is not overwritten.

5. **Various tools are used to detect/defend buffer overflow:** See Table 4.17 to know about few such tools.

4.12 Attacks on Wireless Networks

Even when people travel, they still need to work. Thus, work seems to be moving out of the traditional offices into homes, hotels, airport lounges and taxis. The employee is no longer tied to an office location and is, in effect, "boundaryless." When one talks to the young generation about their lifestyles, one realizes that gone are those days when an "office" conjured up the image of the four walls, set in the formal setting, typical office decor and with all the formality that one can imagine, which may perhaps be difficult for our new generation to appreciate. In the yesteryears, "working" meant leaving home, commuting to the workplace, spending those typical 9 a.m.–6 p.m. in the office and then shutting down the work and commuting back home or wherever that one wished to be after office hours. The "working" and "away from work" were cleanly delineated distinct states that one could be in. Gone are those days and now we are in the era of computing anywhere, anytime! There is no doubt that workforce "mobility" is on the rise (see Box 9.1, Chapter 9).

The following are different types of "mobile workers":

1. **Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems. This includes home workers, tele-cottagers and, in some cases, branch workers.
2. **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).
3. **Nomad:** This category covers employees requiring solutions in hotel rooms and other semi-tethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.
4. **Road warrior:** This is the ultimate mobile user and spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels. This type includes the sales and field forces.

Wireless technologies have become increasingly popular in day-to-day business and personal lives. Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and PDAs. Wireless networks are generally composed of two basic elements: (a) access points (APs) and (b) other wireless-enabled devices, such as laptops radio transmitters and receivers to communicate or "connect" with each other (see Fig. 4.6). APs are connected through physical wiring to a conventional network, and they broadcast signals with which a wireless device can connect.

Wireless access to networks has become very common by now in India – for organizations and for individuals. Many laptop computers have wireless cards preinstalled for the buyer, for example, in India, such cards are provided by TATA Indicom, Reliance and Airtel. There are many hotels and equivalent establishments all over the world (including India) where the rooms are "Wi-Fi enabled." There is no denying that the ability to enter a network while on the move (working away from home or in other locations that are not routine office locations, working while in hotels, etc.) has great benefits (see Box 4.10 for some interesting facts).

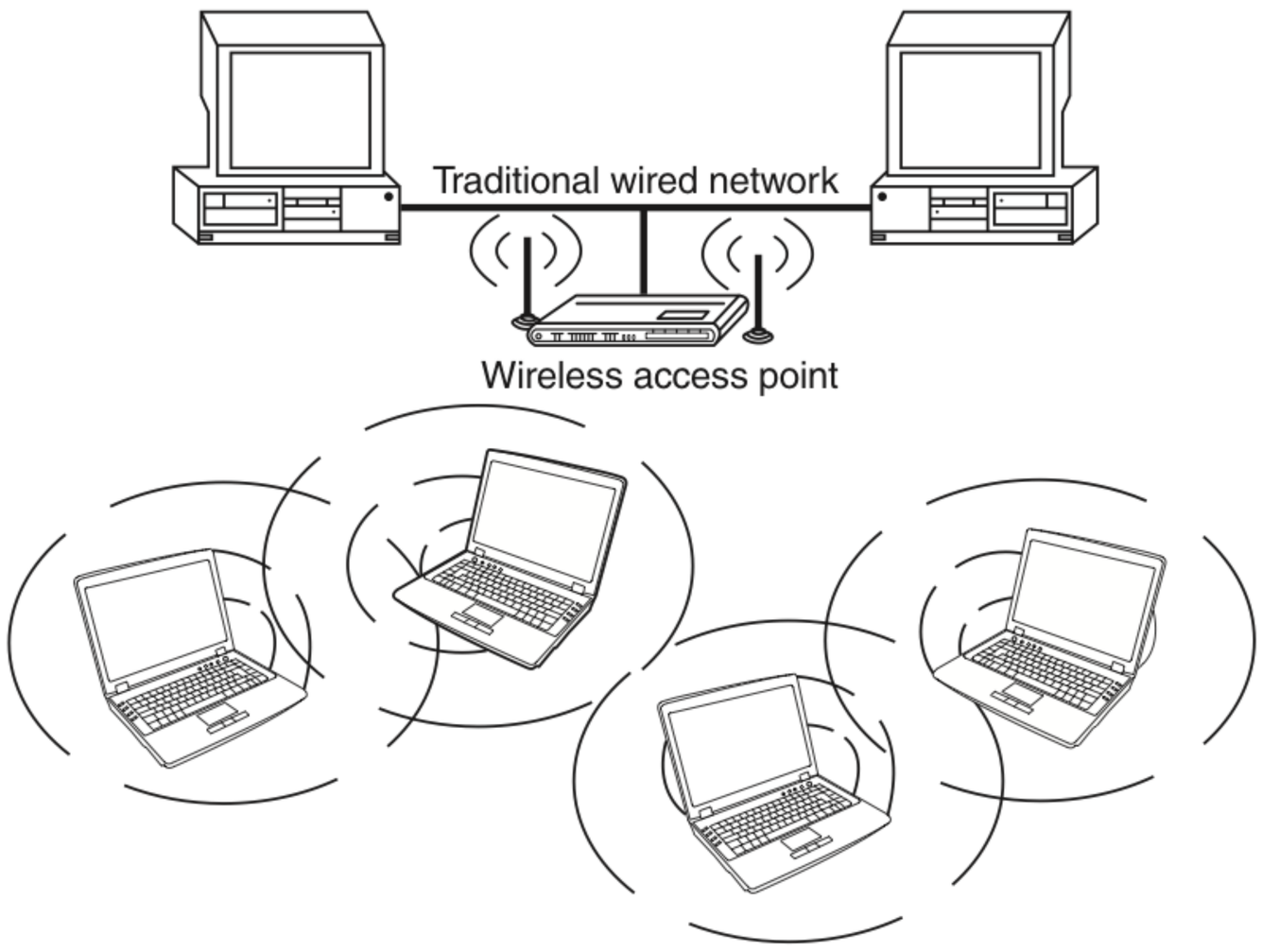

Figure 4.6 | Wireless networks.

Box 4.10 Going Wi-Fi

Start with a laptop computer or other portable device that could benefit from Internet access. Make sure it is wireless. Look for Intel's Centrino sticker or any sign that Wi-Fi is built into the device. If not, you need an external Wi-Fi Personal Computer Memory Card International Association (PCMCIA)-compliant card. Find a public hotspot by searching store windows for stickers that say Wi-Fi Zone, T-Mobile HotSpot or anything indicating a wireless service. Boot up your laptop and login, at home or at a hotel, or get a Wi-Fi router and plug one end into your cable or digital subscriber line (DSL) modem. The router will broadcast the wireless Internet signal in your house and you can sit on the couch and surf the Internet.

Although wireless technology is not new, it is now being used by families who need an easy way to share a fast Internet connection with two or more computers at home. It is helping almost anybody, that is, even the "non-techies," to get Internet access while they buy their daily cup of coffee at a Wi-Fi coffeehouse. This kind of scene is now very common in most Indian metros, including some small cities too.

Cell phones have become indispensable for many who use them to keep track of family members or to call for help in an emergency. Wi-Fi is not there yet, however, the idea of wireless Internet access on every corner is becoming a 24/7 possibility as more companies set up public hotspots. Like cell phones, Wi-Fi is not something you will use every minute, but it can be convenient when you need to check for an E-Mail message or compare the price of an online gift.

Readers may like to visit http://computer.howstuffworks.com/wifi-quiz.htm to test fundamental knowledge about wireless networks before going through this section.

Wireless technology is no more buzzword in today's world. Let us understand important components of wireless network, apart from components such as modems, routers, hubs and firewall, which are integral part of any wired network as well as wireless network.

1. **802.11 networking standards:** Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication in the 2.4, 3.6 and 5 GHz frequency bands.
   - *802.11:* It is applicable to WLANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency-hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
   - *802.11a:* It provides 54 Mbps transmission in the 5 GHz band and uses orthogonal frequency-division multiplexing (OFDM) which is more efficient coding technique compared with FHSS and DSSS.
   - *802.11b:* It provides 11 Mbps transmission in the 2.4 GHz band and uses complementary code keying (CCK) modulation to improve speeds. In 1999, ratification was made to the original 802.11 standard, and was termed as 802.11b, which allowed wireless functionality comparable to Ethernet. Although it was being a slowest standard, at the same time being the least expensive, the evolution led to the rapid acceptance of 802.11b across the world as the definitive WLAN technology and known as "Wi-Fi standard."
   - *802.11g:* It provides 54 Mbps transmission in the 2.4 GHz band and the same OFDM coding as 802.11a, hence it is a lot faster than 802.11a and 802.11b.
   - *802.11n:* It is the newest standard available widely and uses multiple-input multiple-output (MIMO) that enabled to improve the speed and range significantly. For example, although

802.11g provides 54 Mbps transmission theoretically, however, it can only achieve 24 Mbps of speed because of network traffic congestion. However, 802.11n can achieve speeds as high as 140 Mbps.

The other important 802 family members are as follows:

- *802.15*: This standard is used for *personal WLANs* and covers a very short range. Hence, it is used for *Bluetooth Technology*.
- *802.16*: It is also known as *WiMax*. It combines the benefits of broadband and wireless, hence it provides high-speed wireless Internet over very long distances and provides access to large areas such as cities. This standard is developed by IEEE working group established in 1999 to develop the standards for *Wireless Metropolitan Area Networks*.

2. **Access points:** It is also termed as AP. It is a hardware device and/or a software that acts as a central transmitter and receiver of WLAN radio signals. Users of wireless device, such as laptop/PDAs, get connected with these APs, which in turn get connected with the wired LAN. An AP acts as a communication hub for users to connect with the wired LAN.
3. **Wi-Fi hotspots:** A hotspot is a site that offers the Internet access by using Wi-Fi technology over a WLAN. Hotspots are found in public areas (such as coffee shops, public libraries, hotels and restaurants) and are commonly offered facility throughout much of North America and Europe.
   - *Free Wi-Fi hotspots:* Wireless Internet service is offered in public areas, free of cost and that to without any authentication. The users will have to enable the wireless on their devices, search for such hotspots and will have to say (*click*) connect. The Internet facility is made available to the user. As the authentication mechanism on the router is disabled, user gets connected to WLAN and cybercriminals get their prey. As, access to free hotspots cannot be controlled, cybersecurity is always questioned. Readers may visit www.hotspot-locations.com to find wireless hotspots into their area. Hotspot locations is the free global hotspot database of wireless access points made available to the general public.
   - *Commercial hotspots:* The users are redirected to authentication and online payment to avail the wireless Internet service in public areas. The payment can be made using credit/debit card through payment gateways such as PayPal. Major airports and business hotels are usually charged to avail wireless Internet service. Some Internet service providers offer virtual private network (VPN) as a security feature but found to be an expensive option.

   Although the user has been authenticated while connecting to a hotspot, it does not mean that he/she is on the secured communication channel. A "poisoned/rogue hotspot" is termed to be a free public hotspot set up by the cybercriminals, with the objective of sniffing the data sent by the user. They can easily obtain the User IDs (i.e., login names), decipher the passwords and/or other sensitive information by examining packets sent by the user (see Section 7.9, Chapter 7).
4. **Service set identifier (SSID):** It is the name of 802.11i WLAN and all wireless devices on a WLAN must use the same SSID to communicate with each other. While setting up WLAN, the user (or WLAN administrator) sets the SSID, which can be up to 32 characters long so that only the users who knew the SSID will be able to connect the WLAN. It is always advised to turn OFF the broadcast of the SSID, which results in the detected network displaying as an unnamed network and the user would need to manually enter the correct SSID to connect to the network. Hence, it is also advised to set the SSID manually rather than leaving it blank. Moreover, it is important to note that turning off the broadcast of the SSID discourages casual wireless snooping, however, it does not stop an attacker trying to attack the network.
5. **Wired equivalence privacy (WEP):** Wireless transmission is susceptible to eavesdropping and to provide confidentiality, WEP was introduced as part of the original 802.11i Protocol in 1997. It is

always termed as deprecated security algorithm for IEEE 802.11i WLANs. SSID along with WEP delivers fair amount of secured wireless network.

6. **Wi-Fi protected access (WPA and WPA2):** During 2001, serious weakness in WEP was identified that resulted WEP cracking software(s) being made available to enable cybercriminals to intrude into WLANs. WPA was introduced as an interim standard to replace WEP to improve upon the security features of WEP. WPA2 is the approved Wi-Fi alliance (www.wi-fi.org) interoperable implementation of 802.11i. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government agencies.
7. **Media access control (MAC):** It is a unique identifier of each node (i.e., each network interfaces) of the network and it is assigned by the manufacturer of a network interface card (NIC) stored in its hardware. MAC address filtering allows only the devices with specific MAC addresses to access the network. The router should be configured stating which addresses are allowed. Although this method appears to be very secure, the attacker can spoof a MAC address, that is, copy the known MAC address to entice the network that the device he/she is using belongs to the network , at the same time it is important to note that, in case you purchase a new device or if any visitors would like to connect to the network, you will need to add the MAC addresses of these new devices to the list of approved addresses.

How to find MAC Address?

Readers may visit www-dcn.fnal.gov/DCG-Docs/mac/ **OR** www.coffer.com/mac_info/ to know the steps to find the MAC address on the systems running on various operating systems (OS) as well as in case if no OS is installed.

While all this sounds very exciting, it is important to understand that wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into. They are known to use wireless technology to crack into non-wireless networks. Network administrators must be aware of these risks and should stay up to date on any new risks that arise. Users of wireless equipment must be aware of these risks so as to take personal protective measures. As the wireless service technology is getting improved and falling within an easy reach of information technology (IT) as well as non-IT workers, the risks to users of wireless technology have increased exponentially (see Section 9.3.1, Chapter 9).

There were relatively few dangers when wireless technology was first introduced. Although the attackers have no time to latch on to the new technology as wireless was not commonly found in the workplace, however, there are a great number of security risks associated with wireless technology. Some issues are obvious and some are not. At a corporate level, it is the responsibility of the IT department to keep up to date with the types of threats and appropriate countermeasures to deploy. Security threats are growing in the wireless arena. The attackers have learnt that there is much vulnerability in the current wireless protocols, encryption methods and the carelessness and ignorance that exist at the user and corporate IT levels. Cracking methods have become much more sophisticated and innovative with the availability of different tools used to search and hack wireless networks. Cracking has become much easier and more accessible with easy-to-use Windows- and Linux-based tools being made available on the Web at no charge (see Table 4.18).

The overall philosophy behind wired networks vs. wireless networks is "trust." On a wired network, the hardware is under the direct control of the network administrator, and therefore, the overall attitude toward

Table 4.18 | Tools used for hacking wireless networks

Website	*Brief Description*
http://www.netstumbler.com/	**NetStumbler:** This tool is based on Windows OS and easily identifies wireless signals being broadcast within range. It also has ability to determine signal/noise that can be used for site surveys.
http://www.kismetwireless.net/	**Kismet:** This tool detects and displays SSIDs that are not being broadcast which is very critical in finding wireless networks. NetStumbler do not have this key functional element – ability to display wireless networks that are not broadcasting their SSID.
http://sourceforge.net/projects/airsnort/files/	**Airsnort:** This tool is very easy and is usually used to sniff and crack WEP keys (http://airsnort.shmoo.com/).
http://wirelessdefence.org/Contents/coWPAttyMain.htm	**CowPatty:** This tool is used as a brute force tool for cracking WPA-PSK and is considered to be the "New WEP" for home wireless security. This program simply tries a bunch of different options from a dictionary file to see if one ends up matching what is defined as the preshared key.
http://www.wireshark.org/	**Wireshark (formerly ethereal):** Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff out 802.11 management Beacons and probes, and subsequently could be used as a tool to sniff out non-broadcast SSIDs.

Source: http://www.ethicalhacker.net/content/view/16/24/ (10 May 10).

the workstations tends to be one of trust. With a wireless network, it is possible that someone could sit in the parking lot with a laptop and access your wireless network. Therefore, the general attitude toward wireless workstations tends to be one of extreme distrust. However, this difference in attitude often causes the same administrators to take extreme positions when it comes to guarding network security. Although they tend to go to extreme lengths at securing a wireless network, at times they almost neglect wired network security. Things to watch out are the following: Are there any unused network jacks or unused switch ports in the office? This is important because if someone was able to sneak into the office and plug a laptop into one of these unused jacks, you may no more have the same level of trust in the hardware on your wired network.

4.12.1 Traditional Techniques of Attacks on Wireless Networks

In security breaches, penetration of a wireless network through unauthorized access is termed as *wireless cracking*. There are various methods that demand high level of technological skill and knowledge, and availability of numerous software tools made it less sophisticated with minimal technological skill to crack WLANs.

1. **Sniffing:** It is eavesdropping on the network and is the simplest of all attacks. Sniffing is the simple process of intercepting wireless data that is being broadcasted on an unsecured network. Also termed as reconnaissance technique, it gathers the required information about the active/available Wi-Fi networks. The attacker usually installs the sniffers remotely on the victim's system and conducts activities such as
   - Passive scanning of wireless network;
   - detection of SSID;
   - colleting the MAC address;
   - collecting the frames to crack WEP.

2. **Spoofing:** The primary objective of this attack is to successfully masquerade the identity by falsifying data and thereby gaining an illegitimate advantage. The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a legitimate network. It causes unsuspecting computers to automatically connect to the spoofed network instead of the real one. The attacker can conduct this activity easily because while setting up a wireless network, the computers no longer need to be informed to access the network; rather they access it automatically as soon as they move within the signal range. This convenient feature is always exploited by the attacker.
   - *MAC address Spoofing:* It is a technique of changing an assigned media access control (MAC) address of a networked device to a different one. This allows the attacker to bypass the access control lists on servers or routers by either hiding a computer on a network or allowing it to impersonate another network device.
   - *IP Spoofing:* It is a process of creating IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. To engage in IP Spoofing, the attacker uses a variety of techniques to find an IP address of a trusted host(s) and then modifies the packet headers so that it appears that the packets are coming from that host, that is, legitimate sender.
   - *Frame Spoofing:* The attacker injects the frames whose content is carefully spoofed and which are valid as per 802.11 specifications. Frames themselves are not authenticated in 802.11 networks and hence when a frame has a spoofed source address, it cannot be detected unless the address is entirely faked/bogus.
3. **Denial of service (DoS):** We have explained this attack in detail in Section 4.9.
4. **Man-in-the-middle attack (MITM):** It refers to the scenario wherein an attacker on host *A* inserts *A* between all communications – between hosts *X* and *Y* without knowledge of *X* and *Y*. All messages sent by *X* do reach *Y* but through *A* and vice versa. The objective behind this attack is to merely observe the communication or modify it before sending it out.
5. **Encryption cracking:** It is always advised that the first step to protect wireless networks is to use WPA encryption. The attackers always devise new tools and techniques to deconstruct the older encryption technology, which is quite easy for attackers due to continuous research in this field. Hence, the second step is to use a long and highly randomized encryption key; this is very important. It is a little pain to remember long random encryption; however, at the same time these keys are much harder to crack.

4.12.2 Theft of Internet Hours and Wi-Fi-based Frauds and Misuses

Information communication technology (ICT) is within reach of people nowadays and most of the new systems (i.e., computers) are equipped for wireless Internet access as more and more people are opting for Wi-Fi in their homes. Wireless network into homes is becoming common necessity because of lifestyle and availability of inexpensive broadband routers that can be configured easily and/or there is no need to configure these devices at all because of plug-and-play feature. This enables the Internet on the finger tip of home users and in case, unfortunately, he/she visits a malicious webpage, the router is exposed for an attack. Thus, as the networks become stronger and more prevalent, more of the signals are available outside the home of the subscriber, spilling over into neighbor's apartments, hallways and the street. In today's era of high dependability on the Internet for many aspects of our life and given that predators are lurking around as potential cybercriminals, they (criminals) often wonder how they can find out who they are stealing it from so that they can get an idea if that information is safe. According to a study by Jupiter Research, 14% of wireless

network owners have accessed their neighbor's connection.[36] It appears that more and more people are logging on for free.

Cybercriminals know that they should not steal Internet hours purchased by others but somehow they want to get their work done without paying for the Internet connection and they also want to know if anyone knows how to find out who they are stealing it from. Here is what they are mostly likely to do: (a) they find out the IP address of the router that you are using, (b) open up a command prompt (go to start click on run with; type cmd and press enter) at the command prompt and (c) type this command ipconfig/all and press enter. Look for the default gateway (this is the router); once you see the IP address type the routers IP address into your browser and you can find out some information about who you are stealing Internet from.

An interesting question is whether "stealing" wireless Internet is illegal. We have discussed it under a mini-case in Chapter 11 (in CD) and readers may visit the URL provided in Ref. #13, Additional Useful Web References, Further Reading. Here is one scenario, given that use of laptops is now common place. Suppose you figure out how to connect the laptop to one of the many wireless networks detected on your laptop. Is this illegal? As we shall learn in Chapter 6 the laws vary around the world. However, for the most part, logging and collecting information, such as surfing the Web or checking E-Mail, from wireless networks that are accessible to anyone with a receiver is OK. The act of wardriving is searching for wireless networks by a moving vehicle using a portable computer or PDA.[37] Readers may visit the URL mentioned in Ref. #3, Video Clips, Further Reading to watch a small video clip on how wardriving is conducted.

Software for wardriving is freely available and can be downloaded from the Internet – to name a few NetStumbler for Windows, Kismet or SWScanner for Linux, and FreeBSD, NetBSD, OpenBSD, DragonFly BSD, Solaris and KisMac for Macintosh. Wardrivers log and collect information from the wireless access points (WAP) they find while driving (see Box 4.11). Think about radio airwaves: as long as you have a radio, listening to a radio station broadcasting where you are driving is free (at least in the US).

Box 4.11 The New "Wars" in the Internet Era!

Basically, the term "wardriving" was derived from the term wardialing from the 1983 film WarGames, which involved searching for computer systems to connect to, using software that dialed numbers sequentially, to see which ones were connected to a fax machine or computer. Subsequently, many related terms came up:

1. **Warwalking:** It is also known as "warjogging" and is similar in nature to wardriving, except that it is done on foot rather than conducted from a moving vehicle. The disadvantages of this approach consist in slower speed of travel (resulting in fewer and more infrequently discovered networks) and the absence of a convenient computing environment. Consequently, hand-held devices, such as Pocket PCs that can perform tasks while one is walking or standing, have predominated in this area. The inclusion of integrated Wi-Fi (rather than a CompactFlash, i.e., CF is a mass storage device format used in portable electronic devices or PCMCIA add-in card) in Dell Axim, Compaq iPAQ and Toshiba pocket PCs in 2002 – and, more recently, an active Nintendo DS and Sony PSP enthusiast community possessing Wi-Fi capabilities on these devices — has expanded the extent of this practice as the newer Smartphones have also integrated Global Positioning System (GPS). Of recent note, the Nokia N770, N800 and N810 Internet Tablets have very good antennas and will pick up nearly anything in the area, even blocks away from the unit.
2. **Warbiking:** Although warbiking is same as wardriving, it involves searching for wireless networks while on a moving bicycle or motorcycle. This activity is facilitated by the mounting of a Wi-Fi-capable device on the vehicle itself.

Box 4.11 The New "Wars" . . . (*Continued*)

3. **Warkitting:** Warkitting was identified by Tsow, Jakobsson, Yang and Wetzel in 2006. This is a combination of wardriving and rootkitting – an attack in which the wireless access point's configuration or firmware is modified over the wireless connection. This allows the attacker to control all traffic for the victim and may even permit to disable Secure Socket Layer (SSL) by replacing HTML content, when it is being downloaded. The attacker first discovers vulnerable wireless routers through wardriving and/or by retrieving the necessary data from existing Wi-Fi access point databases such as WiGLE (www.wigle.net) or WiFiMaps (www.wifimaps.com) to carry out a warkitting attack.
4. **WAPKitting:** In this attack, external software clutches the control of router's firmware that can be easily accomplished by exploiting open administrative access. WAPkitting can theoretically proceed by more traditional means such as buffer overflow. The ability to install arbitrary control software on a wireless router opens unlimited possibilities to an attacker.
5. **WAPjacking:** This type of attack is very similar to DNS poisoning attacks. It changes the settings of existing firmware that helps an attacker to engage in malicious configuration of firmware settings; however, it makes no modification to the firmware itself, that is, allow connections to be hijacked and/or rerouted without the user's knowledge. WAPjacking is less powerful attack compared to WAPkitting.

WAPkitting and WAPjacking are independent of the means of infection, and specify the relative modifications done to a WAP upon corruption. Warkitting, on the other hand, does not specify the type of WAP alteration, but it does relate to how infection occurs.

Source: http://en.wikipedia.org/wiki/Wardriving (31 May 2010).

Be careful with use of WAPs; when you are using a WAP to gain access to computer on a network, be aware of the local laws/legislations where you are doing it because things can become dangerous from security and privacy as well legal perspective. Maybe if corporations were not in such a hurry to release this technology and thought about it more thoroughly, they would not have to deal with security breaches and creating superior protection for their own systems. The moral of the story is that you must secure your network.

4.12.3 How to Secure the Wireless Networks

Nowadays, security features of Wi-Fi networking products are not that time-consuming and non-intuitive; however, they are still ignored, especially, by home users. Although following summarized steps will help to improve and strengthen the security of wireless network, see Table 4.19 to know the available tools to monitor and protect the wireless networks:

1. Change the default settings of all the equipments/components of wireless network (e.g., IP address/user IDs/administrator passwords, etc.).
2. Enable WPA/WEP encryption.
3. Change the default SSID.
4. Enable MAC address filtering.
5. Disable remote login.
6. Disable SSID broadcast.
7. Disable the features that are not used in the AP (e.g., printing/music support).
8. Avoid providing the network a name which can be easily identified (e.g., My_Home_Wifi).
9. Connect only to secured wireless network (i.e., do not autoconnect to open Wi-Fi hotspots).
10. Upgrade router's firmware periodically.

Table 4.19 | Tools to protect wireless network

Website	*Brief Description*
http://www.zamzom.com/	**Zamzom Wireless Network Tool:** New freeware tool helps to protect wireless networks and maintain computer security, detects all computer names, Mac and IP addresses utilizing a single wireless network, reveals all computers – both authorized and unauthorized – who have access to any given wireless network. Thus, it helps users to take vital steps toward securing their wireless networks and acts as a measure that should not be overlooked or skipped.
http://www.airdefense.net/	**AirDefense Guard:** The tool provides advanced intrusion detection for wireless LANs and is based on signature analysis, policy deviation, protocol assessment policy deviation and statistically anomalous behavior. AirDefense detects responds to: • Denial-of-service (DoS) attacks; • man-in-the-middle attacks; • identity theft.
http://www.loud-fat-bloke.co.uk/tools.html	**Wireless Intrusion Detection System (WIDZ):** This is an intrusion detection for wireless LANs for 802.11. It guards APs and monitors local frequencies for potentially malevolent activity. It can detect scans, association floods and bogus APs, and it can easily be integrated with other products such as SNORT or Realsecure.
http://www.dachb0den.com/projects/bsd-airtools.html	**BSD-Airtools:** This tool provides a complete toolset for wireless auditing (802.11b). It contains AP detection application, Dstumbler – similar to Netstumbler. It can be used to detect wireless access points and connected nodes, view signal-to-noise graphs, and interactively scroll through scanned APs and view statistics for each. It also contains a BSD-based WEP cracking application (called as Dweputils).
http://wifi.google.com/	**Google Secure Access:** Google Wi-Fi is a free wireless Internet service offered to the city of Mountain View (California, USA). With your Wi-Fi-enabled device and a Google Account, one can go online for free by accessing the network name "GoogleWi-Fi," which is secured by Google's virtual private network (VPN). Google Secure Access encrypts the Internet traffic and sends it through Google's servers on the Internet.

11. Assign static IP addresses to devices.
12. Enable firewalls on each computer and the router.
13. Position the router or AP safely.
14. Turn off the network during extended periods when not in use.
15. Periodic and regular monitor wireless network security.

Summary

When information systems are the target of offense, the criminal's goal is to steal information from, or cause damage to, a computer, computer system or computer network. The perpetrators range from teenagers (script kiddies/cyberjoyriders) to organized crime operators and international terrorists. A computer can be the target of offense; tools may be used in an offense, or may contain evidence of an offense. An understanding of different uses of a computer will provide foundation of the application of the criminal statutes.

The computing technology may also be a tool of an offense. The criminal uses the computer to commit a traditional crime, such as counterfeiting. For example, a counterfeiter that used to engrave plates to create the counterfeit currency can now use sophisticated graphic computers with advanced color printers.

The criminals/attackers have in-depth knowledge about the technology and can use traditional methods/techniques or sophisticated means such as hacking tools to break into the systems. Everybody has to take care of their own systems and this should not be left over to any one person/group of persons (i.e., System Administrator, Chief Information Security Officer). Many scenarios and case illustrations are provided in Chapter 11 (in CD) explaining different techniques used in cyberattacks. Everybody should follow **R.U.N.S.A.F.E. guidelines:**

1. **R**efuse to download/install/execute any unknown utilities/tools.
2. **U**pdate vital utilities/tools (e.g., OS, antivirus, anti-Spywares, firewalls) regularly.
3. **N**ullify unnecessary risks.
4. **S**afeguard own user ID and password.
5. **A**ssure sufficient resources to take care of own systems appropriately.
6. **F**ace insecurity (i.e., what and how much to secure is always a question!).
7. **E**verybody should do their own job sincerely (i.e., information security is everybody's responsibility similar to "charity begins at home!").

Review Questions

1. What are the different phases during the attack on the network?
2. What is the difference between proxy server and an anonymizer?
3. What are the different ways of password cracking?
4. How can keyloggers be used to commit a cybercrime?
5. What is the difference between a virus and a worm?
6. What is virus hoax?
7. What is the difference between Trojan Horses and backdoors?
8. What is the difference between steganography and cryptography?
9. Are countermeasures employed against steganography? Explain.
10. What is the difference between DoS and DDoS?
11. What is SQL injection and what are the different countermeasures to prevent the attack?
12. What is Blind SQL injection attack? Can it be prevented?
13. What are different buffer overflow attacks?
14. What are the different components of wireless network?
15. What is the difference between WEP and WPA2?
16. How can wireless networks be comprised?
17. What is the difference between WAPkitting and WAPjacking?

References

[1] To know more about anonymizer, visit: http://en.wikipedia.org/wiki/Anonymizer (6 September 2009).

[2] To know more about Google cookie, visit: http://www.google-watch.org/bigbro.html (2 October 2009).

[3] To know more about DART cookie, visit: http://www.doubleclick.com/privacy/faq.aspx (2 October 2009).

[4] To know more on G-Zapper, visit: http://www.dummysoftware.com/gzapper.html (2 October 2009).

[5] To know more on Phishing, visit: http://computer.howstuffworks.com/phishing.htm (29 May 10).

[6] To know more about password, visit: http://en.wikipedia.org/wiki/Password_cracking (2 October 2009).

[7] To know more about MITM attacks, visit: http://en.wikipedia.org/wiki/Man-in-the-middle_attack (2 October 2009).
[8] To know more about strength of a password, visit: http://www.microsoft.com/protect/fraud/passwords/checker.aspx (2 October 2009).
[9] To know more about keyloggers, visit: http://en.wikipedia.org/wiki/Keystroke_logging (4 October 2009).
[10] To know more about software keyloggers, visit: http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci962518,00.html (4 October 2009).
[11] To know more about antikeylogger, visit: http://www.anti-keyloggers.com/products.html (4 October 2009).
[12] To know more about Spyware, visit: http://en.wikipedia.org/wiki/Spyware (5 October 2009).
[13] To know more about malware, visit: http://en.wikipedia.org/wiki/Malware (5 October 2009).
[14] To know more about Trojan Horses visit: http://en.wikipedia.org/wiki/Trojan_horse_(computing) (8 October 2009).
[15] To know more about rootkit, visit: http://en.wikipedia.org/wiki/Rootkit (8 October 2009).
[16] To know more about backdoor, visit: http://en.wikipedia.org/wiki/Backdoor_(computing) (8 October 2009).
[17] To know more about viruses, worms and Trojans, visit: http://en.wikipedia.org/wiki/Computer_virus (1 March 2010).
[18] To understand difference between computer virus and worm, visit: http://www.diffen.com/difference/Computer_Virus_vs_Computer_Worm (1 March 2010).
[19] To know types of viruses, visit: http://www.spamlaws.com/virus-types.html (1 March 2010).
[20] To know more on worm, visit: http://en.wikipedia.org/wiki/Computer_worm (1 March 2010).
[21] To understand various aspects of viruses, visit: http://www.kernelthread.com/publications/security/vunix.html (1 March 2010).
[22] To know more about Trojan Horse, visit: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html (11 January 2010).
[23] To know more about threats by Trojan Horses, visit: http://www.techsupportalert.com/best-free-trojan-scanner-trojan-remover.htm (11 January 2010).
[24] To know more about backdoor, visit: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci962304,00.html (10 January 2010).
[25] To know more about what a backdoor does, visit: http://www.2-spyware.com/backdoors-removal (10 January 2010).
[26] To know more about SAP backdoors, visit: http://blog.c22.cc/2010/04/14/blackhat-europe-sap-backdoors-a-ghost-at-the-heart-of-your-business-4/ (29 May 2010).
[27] To know more about what is P2P network, visit: http://en.wikipedia.org/wiki/Peer-to-peer (29 May 2010).
[28] To understand different levels of P2P networks, visit: http://disco.ethz.ch/theses/ss05/freenet.pdf (29 May 2010).
[29] To know more about steganography, visit: http://en.wikipedia.org/wiki/Steganography (11 October 2009).
[30] Visit New York Times reports usage of steganography at: http://en.wikipedia.org/wiki/Steganography (11 October 2009).
[31] To know more about DoS: Teardrop attack, visit: http://en.wikipedia.org/wiki/Denial-of-service_attack (11 May 2010).
[32] To know more about DoS: Nuke attack, visit: http://wapedia.mobi/en/Denial_of_Service (11 May 2010).

[33] To know how to prevent DoS attacks, visit: http://www.cert.org/tech_tips/denial_of_service.html#4 (11 May 2010).
[34] To know more about SQL injection and Blind SQL injection attacks, visit: http://en.wikipedia.org/wiki/SQL_injection (11 May 2010).
[35] To know more about buffer overflow: NOOP, visit: http://en.wikipedia.org/wiki/Buffer_overflow (11 May 2010).
[36] To know more about wireless network – frauds and misuses, visit: http://www.88450.com/redirect.php?tid=55751&goto=lastpost (11 May 2010).
[37] To know more about wardriving, visit: http://en.wikipedia.org/wiki/War_driving (11 May 2010).

Further Reading

Additional Useful Web References

1. To know how anonymizers work, visit: http://www.livinginternet.com/i/is_anon_work.htm (6 September 2009).
2. To know more about anonymizer FAQs, visit: http://www.anonymizer.com/company/about/anonymizer-faq.html (6 September 2009).
3. To understand a framework for classifying denial-of-service attacks, visit: http://isi.edu/div7/publication_files/tr-569.pdf (30 May 2010).
4. To understand wireshark frequently asked questions, visit: http://www.wireshark.org/faq.html (30 May 2010).
5. To understand classification of DoS attack, visit: http://www.technospot.net/blogs/types-of-dos-attacks-and-introduction-to-ddos/ (30 May 2010).
6. To understand types of DoS attacks, visit: http://www-rp.lip6.fr/~blegrand/cours/MIAIF/secu1.pdf (30 May 2010). http://www.topbits.com/denial-of-service-dos-attacks.html (30 May 2010).
7. To understand blind SQL injection, visit: http://www.net-security.org/dl/articles/Blind_SQLInjection.pdf (30 May 2010).
8. To know more about SQL injection protection, visit: http://www.owasp.org/images/7/7d/Advanced_Topics_on_SQL_Injection_Protection.ppt (30 May 2010).
9. To know how to protect from injection attacks in ASP.NET, visit: http://msdn.microsoft.com/en-us/library/ff647397.aspx (30 May 2010).
10. To know more about buffer overflow attacks and their countermeasures, visit: http://www.linuxjournal.com/article/6701?page=0,0 (30 May 2010).
11. To know more about article *Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade*, visit: http://www.ece.cmu.edu/~adrian/630-f04/readings/cowan-vulnerability.pdf (30 May 2010).
12. Stealing your neighbor's Net, visit: http://money.cnn.com/2005/08/08/technology/personaltech/internet_piracy/index.htm (30 May 2010).
13. Is "Stealing" Wireless Internet Illegal?, visit: http://journalism.nyu.edu/pubzone/wewantmedia/node/10 (30 May 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. Kimberly, G. (2007) *CEH: Official Certified Ethical Hacker Review Guide*, Wiley Publishing, Inc., IN, USA.
3. Milhorn, H.T. (2007) *Cybercrime: How to Avoid Becoming a Victim*, Universal Publishers, USA.

Video Clips

1. To know more about *Demonstration of Scareware*, visit: http://www.youtube.com/watch?v=nRgkFt0NLsw (16 February 2010).
2. To know more about *Crime: The Real Internet Security Problem*, visit: http://www.youtube.com/watch?v=rZ1rkIy0dMM (16 February 2010).
3. To know more on how wardriving is conducted, visit: http://www.metacafe.com/watch/1708061/i_quit_movie_scene_24_stealing_internet_access/ (16 September 2009).

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, C, D, E, J, L. These are provided in the companion CD.