crime is difficult. One definition that is advocated is, "*a crime conducted in which a computer was directly and significantly instrumental.*" This definition is not universally accepted. It, however, initiates further discussion to narrow the scope of the definition for "cybercrime": for example, we can propose the following alternative definitions of computer crime:

1. Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution.
2. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
3. Any financial dishonesty that takes place in a computer environment.
4. Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.

Here is yet another definition: "*cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.*" Note that in a wider sense, "computer-related crime" can be any illegal behavior committed by means of, or in relation to, a computer system or network; however, this is not cybercrime.

Statute and treaty law both refer to "cybercrime." The term "cybercrime" relates to a number of other terms that may sometimes be used interchangeably to describe crimes committed using computers. *Computer-related crime*, *Computer crime*, *Internet crime*, *E-crime*, *High-tech crime*, etc. are the other synonymous terms. Cybercrime specifically can be defined in a number of ways; a few definitions are:

1. A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs. Refer to Chapter 5.
2. Crimes completed either on or with a computer.
3. Any illegal activity done through the Internet or on the computer.
4. All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.

According to one information security glossary,[1] cybercrime is any criminal activity which uses network access to commit a criminal act. Opportunities for the exploitation due to weaknesses in information security are multiplying because of the exponential growth of Internet connection (see Ref. #26, Additional Useful Web References, Further Reading). Cybercrime may be internal or external, with the former easier to perpetrate. The term "cybercrime" has evolved over the past few years since the adoption of Internet connection on a global scale with hundreds of millions of users. *Cybercrime* refers to the act of performing a criminal act using cyberspace as the communications vehicle (the term "cyberspace" is explained in Box 1.1). Some people argue that a cybercrime is not a crime as it is a crime against software and not against a person or property. However, while the legal systems around the world scramble to introduce laws to combat cybercriminals (refer to Section 1.5), two types of attack are prevalent:

1. **Techno-crime:** A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. The 24×7 connection to the Internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving few, if any, "finger prints."

2. **Techno-vandalism:** These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. Tight internal security, allied to strong technical safeguards, should prevent the vast majority of such incidents.

There is a very thin line between the two terms "computer crime" and "computer fraud"; both are punishable (see Tables 1.1–1.4). Cybercrimes (harmful acts committed from or against a computer or network) differ from most terrestrial crimes in four ways: (a) how to commit them is easier to learn, (b) they require few resources relative to the potential damage caused, (c) they can be committed in a jurisdiction without being physically present in it and (d) they are often not clearly illegal.

The term cybercrime has some stigma attached and is notorious due to the word "terrorism" or "terrorist" attached with it, that is, cyberterrorism (see explanation of the term in Box 1.1). Cyberterrorism is defined as "*any person, group or organization who, with* ***terrorist intent****, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism.*" Cybercrime, especially through the Internet, has grown in number as the use of computer has become central to commerce, entertainment and government.

The term *cyber* has some interesting synonyms: fake, replicated, pretend, imitation, virtual, computer-generated. Cyber means combining forms relating to Information Technology, the Internet and Virtual Reality. This term owes its origin to the word "cybernetics" which deals with information and its use; furthermore, cybernetics is the science that overlaps the fields of neurophysiology, information theory, computing machinery and automation.[2] However, beyond this, there does not seem to be any further connection to the term "cybernetics" as per other sources searched.[3–5] According to Wikipedia,[6] cybernetics is the interdisciplinary study of the structure of regulatory systems. It is closely related to control theory and systems theory.

People are curious to know how cybercrimes are planned and how they actually take place (explained in Chapter 2). Worldwide, including India, cyberterrorists usually use computer as a tool, target or both for

their unlawful act to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information. [See Further Reading, Books, Ref. #3 for a pointer to data privacy and understanding terms such as sensitive information, personal information (PI) and sensitive personal information (SPI).] Internet is one of the means by which the offenders can gain priced sensitive information of companies, firms, individuals, banks and can lead to intellectual property (IP) crimes (such as stealing new product plans, its description, market program plans, list of customers, etc.), selling illegal articles, pornography/child pornography, etc. This is done using methods such as Phishing, Spoofing, Pharming, Internet Phishing, wire transfer, etc. and use it to their own advantage without the consent of the individual. "Phishing" refers to an attack using mail programs to deceive or coax Internet users into disclosing confidential information that can be then exploited for illegal purposes. Figure 1.2 shows the increase in Phishing hosts.

1.5.7 Forgery

Counterfeit currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges there are miscreants soliciting the sale of fake marksheets or even degree certificates. These are made using computers and high quality scanners and printers. In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

1.5.11 Hacking

Although the purposes of hacking are many, the main ones are as follows:

1. Greed;
2. power;
3. publicity;
4. revenge;
5. adventure;
6. desire to access forbidden information;
7. destructive mindset.

Every act committed toward breaking into a computer and/or network is hacking and it is an offense. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get enjoyment out of such destruction. Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information that is critical in nature. Government websites are hot on hackers' target lists and attacks on Government websites receive wide press coverage. For example, according to the story posted on December 2009, the NASA site was hacked via SQL Injection (see Ref. #22, Additional Useful Web References, Further Reading). SQL Injection is covered more in detail in Chapter 4. Examples of prominent websites hacked are shown in Figs. 1.6–1.10.

Hackers, crackers and phrackers[11] are some of the oft-heard terms. The original meaning of the word "hack" meaning an elegant, witty or inspired way of doing almost anything originated at MIT. The meaning has now changed to become something associated with the breaking into or harming of any kind of computer or telecommunications system. Some people claim that those who break into computer systems should ideally be called "crackers" and those targeting phones should be known as "phreaks" (see Chapter 17, Box 17.3 of Ref. #3, Books, Further Reading).

1.5.14 Software Piracy

This is a big challenge area indeed. (Readers may like to refer to Chapter 38 and other relevant pages of Ref. #3, Books, Further Reading.) Cybercrime investigation cell of India defines "software piracy" as *theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.* There are many examples of software piracy: *end-user copying* – friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses; *hard disk loading with illicit means* – hard disk vendors load pirated software; *counterfeiting* – large-scale duplication and distribution of illegally copied software; *illegal downloads from the Internet* – by intrusion, by cracking serial numbers, etc. Beware that those who buy pirated software have a lot to lose: (a) getting untested software that may have been copied thousands of times over, (b) the software, if pirated, may potentially contain hard-drive-infecting viruses, (c) there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users, (d) there is no warranty protection, (e) there is no legal right to use the product, etc.

Economic impact of software piracy is grave (see Fig. 1.11). According to the Fourth Annual BSA and IDC Global Software Piracy Study,[14] in Asia Pacific 55% of the software installed in 2006 on personal computers (PCs) was obtained illegally, while software losses due to software piracy amounted to US$ 11.6 billion. The Global Software Piracy Study mentioned covers all packaged software that runs on personal computers, including desktops, laptops and ultraportables. The study includes operating systems, systems software such as databases and security packages, business applications and consumer applications such as PC games, personal finance and reference software. Refer to Section 9.2.2, Chapter 9.

The BSA/IDC study of year 2006 did not include other types of software such as those which run on servers or mainframes or software sold as a service. It is shocking to know that 35% of the software installed in 2006 on PCs worldwide was obtained illegally, amounting to nearly $40 billion in global losses due to software piracy. Progress was seen in a number of emerging markets, most notably in China, where the piracy rate dropped 10 percentage points in 3 years, and in Russia, where piracy fell seven percentage points over 3 years. Figure 1.12 shows the regional scenario on piracy rate.

1.5.18 Computer Network Intrusions

Computer Networks pose a problem by way of security threat because people can get into them from anywhere. The popular movie "War Games" illustrated an extreme but useful example of this. "Crackers" who are often misnamed "Hackers"[11] can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan Horses or change user names and passwords. Network intrusions are illegal, but detection and enforcement are difficult. Current laws are limited and many intrusions go undetected.

The cracker can bypass existing password protection by creating a program to capture logon IDs and passwords. The practice of "strong password" is therefore important (password strength is explained in Chapter 4). Importance of passwords and password rules is explained in Chapter 11 (Network Security in Perspective) in Ref. #3, Books, Further Reading. In Ref. #3, Books, Chapter 35 (Auditing for Security) explains about password cracking tools in the context of vulnerability scanning and penetration testing. Refer to Ref. #3, Books, Chapter 17 (Security of Wireless Networks and Box 17.3 in particular) for crackers and hackers and Chapter 14 (Intrusion Detection for Securing Networks) for Trojans.

2.2 How Criminals Plan the Attacks

Criminals use many methods and tools to locate the vulnerabilities of their target. The target can be an individual and/or an organization. (The custodian of a property can be an individual or an organization; for discussion purpose not mentioned here.) Criminals plan passive and active attacks (see Sections 2.2.2 and 2.2.3 for more details on these topics). Active attacks are usually used to alter the system (i.e., computer network) whereas passive attacks attempt to gain information about the target. Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to breaches of confidentiality.

In addition to the active and passive categories, attacks can be categorized as either inside or outside. An attack originating and/or attempted within the security perimeter of an organization is an inside attack; it is usually attempted by an "insider" who gains access to more resources than expected. An outside attack is attempted by a source outside the security perimeter, maybe attempted by an insider and/or an outsider, who is indirectly associated with the organization, it is attempted through the Internet or a remote access connection.

The following phases are involved in planning cybercrime:

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

2.2.1 Reconnaissance

The literal meaning of "Reconnaissance" is *an act of reconnoitering – explore, often with the goal of finding something or somebody (especially to gain information about an enemy or potential enemy)*.

In the world of "hacking," reconnaissance phase begins with "*Footprinting*" – this is the preparation toward preattack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment. Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities. The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack.

Thus, an attacker attempts to gather information in two phases: passive and active attacks. Let us understand these two phases.

2.2.2 Passive Attacks

A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge. It can be as simple as watching a building to identify what time employees enter the building premises. However, it is usually done using Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information.

1. Google or Yahoo search: People search to locate information about employees (see Table 2.1).
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
3. Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target (see Section 2.3).
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

2.2.3 Active Attacks

An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase. It involves the risk of detection and is also called "*Rattling the doorknobs*" or "*Active reconnaissance*."

Active reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.

Table 2.2 gives the list of tools used for active attacks – some of the tools are also used during "vulnerability assessment" and/or "penetration testing." Refer to Appendix E in CD.

2.2.4 Scanning and Scrutinizing Gathered Information

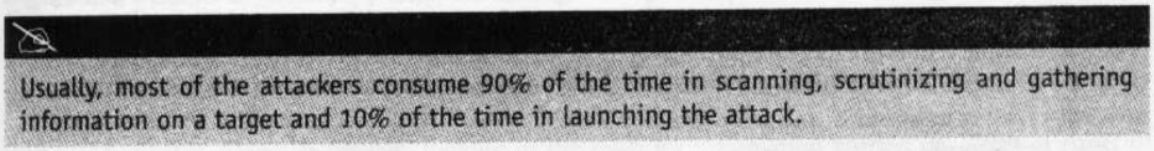
Scanning is a key step to examine intelligently while gathering information about the target. The objectives of scanning are as follows:

1. **Port scanning:** Identify open/close ports and services. Refer to Box 2.5.
2. **Network scanning:** Understand IP Addresses and related information about the computer network systems.
3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

The scrutinizing phase is always called "enumeration" in the hacking world. The objective behind this step is to identify:

1. The valid user accounts or groups;
2. network resources and/or shared resources;
3. OS and different applications that are running on the OS.

Most of the tools listed in Table 2.2 are used for computer network scanning as well.



2.2.5 Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password (we will address it in Chapter 4);
2. exploit the privileges;
3. execute the malicious commands/applications;
4. hide the files (if required);
5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

2.4 Cyberstalking

The dictionary meaning of "stalking" is an "*act or process of following prey stealthily – trying to approach somebody or something.*" Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group

of individuals, or organization. The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.[3]

Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person. It involves harassing or threatening behavior that an individual will conduct repeatedly, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person's property. As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

3.5 Security Challenges Posed by Mobile Devices

Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. When people are asked about important issues in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in Fig. 3.6.

As the number of mobile device users increases, two challenges are presented: one at the device level called "microchallenges" and another at the organizational level called "macrochallenges." Of these, some microchallenges are discussed in this section and macrochallenges in the next section.

Some well-known technical challenges in mobile security are: *managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API) security, etc.* In this section, we provide a brief discussion on these cybersecurity aspects. For most of the discussion here, the reference point is Windows mobile development given that the developers of the Windows OS are on the forefront of the technology in terms of their mobile computing technological initiatives. In view of the discussion in Section 3.4, the ID theft (we will address it in Chapter 5) is now becoming a major fraud in credit card business domain, wherein individual's *Personally Identifiable Information* (PII) is misused to open new credit accounts, take new loans or engage in other types of frauds, such as misuse of the victim's

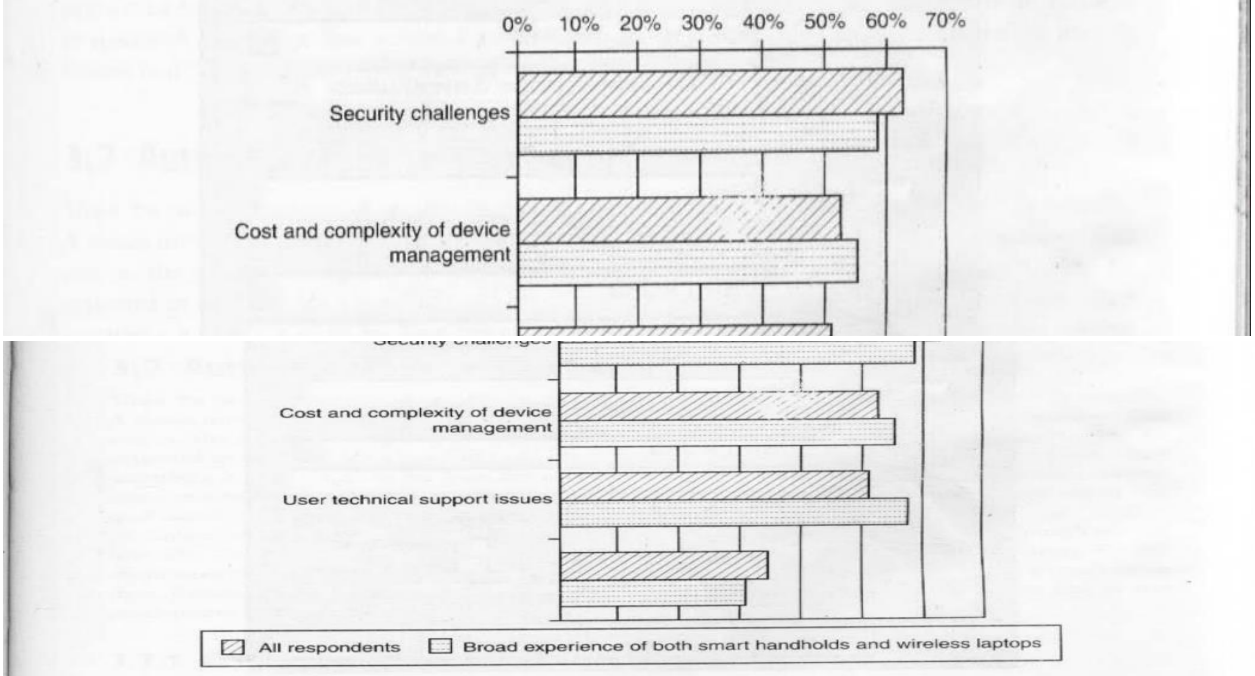
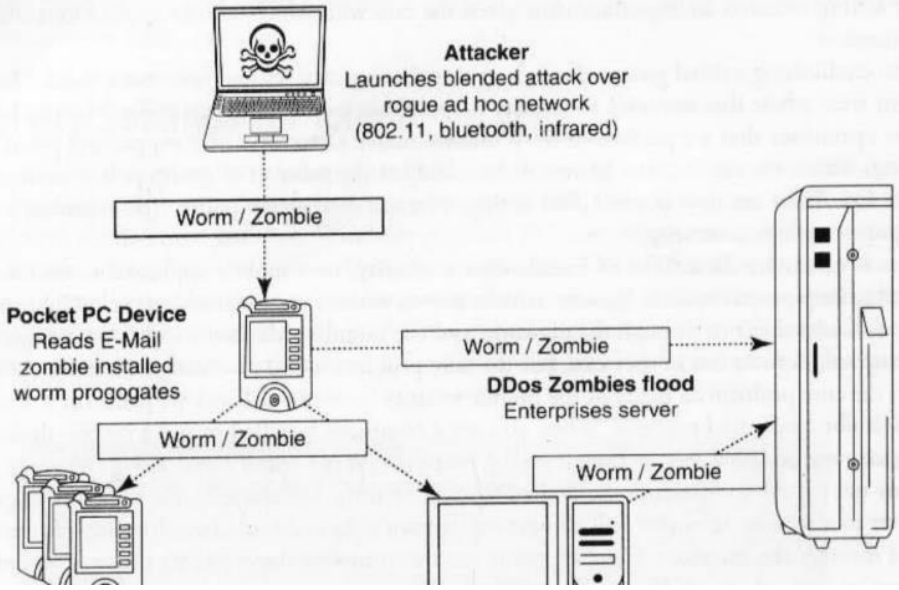


Figure 3.6 Important issues for managing mobile devices.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

name and identifying information when someone is charged with a crime, when renting an apartment or when obtaining medical care.

3.7.1 Cryptographic Security for Mobile Devices

In this section we will discuss a technique known as *cryptographically generated addresses* (CGA). CGA is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address. The address the owner uses is the corresponding private key to assert address ownership



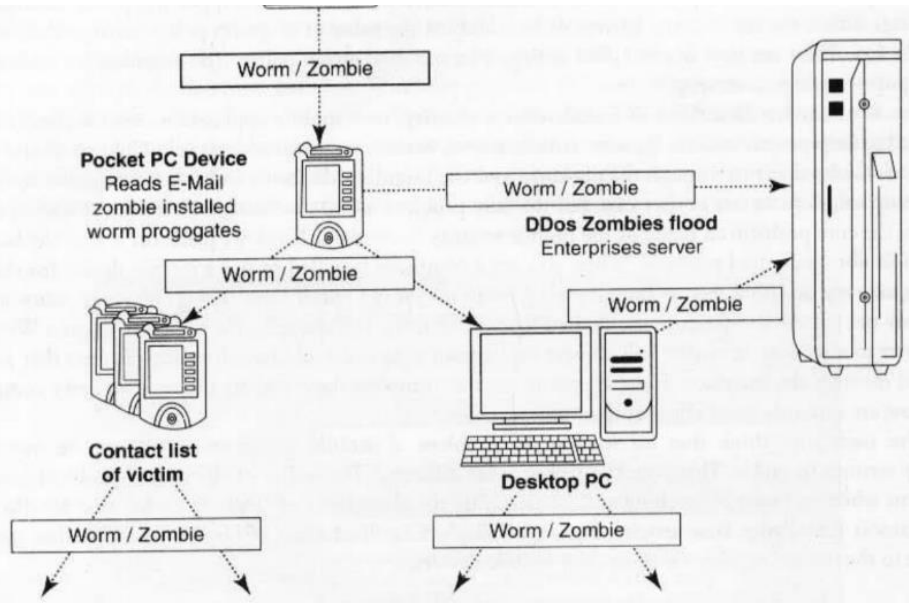


Figure 3.8 | Push attack on mobile devices. DDoS implies distributed denial-of-service attack. *Source:* Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure. Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices. CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery (as in *context-aware mobile computing applications*) and mobility protocols. It can also be used for key exchange in opportunistic Internet Protocol Security (IPSec). Palms (devices that can be held in one's palm, illustrated in Fig. 3.1) are one of the most common hand-held devices used in mobile computing. *Cryptographic security controls* are deployed on these devices. For example, the *Cryptographic Provider Manager* (CPM) in Palm OS5 is a system-wide suite of cryptographic services for securing data and resources on a palm-powered device. The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

3.8 Attacks on Mobile/Cell Phones

3.8.1 Mobile Phone Theft

Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals. Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims. When anyone looses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information (PII)" (refer to Chapter 5), that really matter, are lost. Refer to Box 3.6 to learn about tips on securing mobile phone from being stolen and/or lost.

One might have just thought that his/her cell phone is much safer than a PC that is very often attacked by viruses; however, criminals made this thought as false statement. After PC, the criminals' (i.e., attackers')

Box 3.6 Tips to Secure your Cell/Mobile Phone from being Stolen/Lost

Nowadays, mobiles/cell phones are becoming fancier and expensive hence increasingly liable to theft. Criminals are interested in accessing wireless service and seek potential possibility to stealing the ID.

Ensure to note the following details about your cell phone and preserve it in a safe place[12]:

1. Your phone number;
2. the make and model;
3. color and appearance details;
4. PIN and/or security lock code;
5. IMEI number.

The International Mobile Equipment Identity (IMEI)

It is a number unique to every GSM, WCDMA and iDEN cell phone. It is a 15-digit number and can be obtained by entering *#06# from the keypad.

The IMEI number is used by the GSM network to identify valid devices and therefore can be used

new playground has been cell phones, reason being the increasing usage of cell phones and availability of Internet using cell phones. Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.

The following factors contribute for outbreaks on mobile devices:

1. **Enough target terminals:** The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.
2. **Enough functionality:** Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.
3. **Enough connectivity:** Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

3.8.2 Mobile Viruses

A mobile virus is similar to a computer virus that targets mobile phone data or applications/software installed in it. Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays. In total, 40 mobile virus families and more than 300(+) mobile viruses have been identified. First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.

Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS. Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth-activated phones (i.e., if Bluetooth is always ENABLED into a mobile phone) whereas MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book. Readers may visit http://symbianpoint.com/types-latest-list-mobile-viruses.html to know the list of latest mobile viruses (few viruses have been discussed in Section 3.3 Trends in Mobility).

It is interesting to note that, like Computer Virus Hoax, variants of Mobile Phone Virus Hoax[13] have been circulating since 1999. These hoax messages either will be sent through E-Mail or through SMS to the mobile users. The example of such hoax is given.

"All mobile users pay attention!!!!!!!!!

If you receive a phone call and your mobile phone displays (XALAN) on the screen don't answer the call, END THE CALL IMMEDIATELY, if you answer the call, your phone will be infected by a virus. This virus WILL ERASE all IMEI and IMSI information from both your phone and your SIM card, which will make your phone unable to connect with the telephone network. You will have to buy a new phone. This information has been confirmed by both Motorola and Nokia. There are over 3 Million mobile phones being infected by this virus in all around the world now. You can also check this news in the CNN website.

PLEASE FORWARD THIS PIECE OF INFORMATION TO ALL YOUR FRIENDS HAVING A MOBILE PHONE."

How to Protect from Mobile Malwares Attacks

Following are some tips to protect mobile from mobile malware attacks[14]:

1. Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
2. If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
3. If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
4. Download and install antivirus software for mobile devices.

3.8.6 Hacking Bluetooth

Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances (i.e., using short length radio waves) between fixed and/or mobile devices (see Box 3.9). Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication. The older standard – Bluetooth 1.0 has a maximum transfer speed of 1 Mbps (megabit per second) compared with 3 Mbps by Bluetooth 2.0.

When Bluetooth is enabled on a device, it essentially broadcasts "I'm here, and I'm able to connect" to any other Bluetooth-based device within range. This makes Bluetooth use simple and straightforward, and it also makes easier to identify the target for attackers. The attacker installs special software [see Table 3.1 for list of software(s) which are termed as *Bluetooth hacking tools*] on a laptop and then installs a Bluetooth antenna. Whenever an attacker moves around public places, the software installed on laptop constantly scans the nearby surroundings of the hacker for active Bluetooth connections. Once the software tool used by the attacker finds and connects to a vulnerable Bluetooth-enabled cell phone, it can do things like download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls and much more.

Box 3.9 Bluetooth

The word Bluetooth is an anglicized form of Danish *Blåtand* – Harald Bluetooth was king of Denmark in the 10th century, who managed to unite Denmark and parts of Norway into a single kingdom. The king was killed in 986 AD during a battle with his son. Choosing this name indicates how important companies from the Nordic region (nations including Denmark, Sweden, Norway and Finland) are to the communications industry, even if this name says little about the way the technology works. The implication is that Bluetooth does the same with communication protocols, uniting them into one universal standard. *blå* in modern Scandinavic languages means blue and (historically) correct translation of Old Norse *Harald Blátǫnn* could be Harald Bluetooth.

The Bluetooth logo is a bind rune merging the Germanic runes ᚼ (Hagall) and ᛒ (Berkanan).

Bluejacking, *Bluesnarfing*, *Bluebugging* and *Car Whisperer* are common attacks that have emerged as Bluetooth-specific security issues.

1. **Bluejacking:** It means *Bluetooth* + *Jacking* where Jacking is short name for *hijack* – act of taking over something. Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or computers (within 10-m radius), for example, sending a visiting card which will contain a message in the name field. If the user does not recognize/realize what the message is, he/she might allow the contact to be added to her/his address book, and the contact can send him messages that might be automatically opened because they are coming from a known contact. Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.
2. **Bluesnarfing:** It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers. This enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.
3. **Bluebugging:** It allows attackers to remotely access a user's phone and use its features without user's attention. During initial days, the attacker could simply listen to any conversation his/her victim is having; however, further developments in Bluebugging tools have enabled the attacker with the ability to take control of the victim's phone and to conduct many more activities such as initiate phone calls; send and read SMS; read and write phonebook contacts; eavesdrop on phone conversations and connect to the Internet.
4. **Car Whisperer:** It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo. Further reasearch is underway to know whether Bluetooth attackers could do anything more serious such as disabling airbags or brakes through this kind of attack. The reasearchers are also investigating about possibility of an attacker accessing a telephone address book once the connection gets established with the Bluetooth system through this kind of attack.

Among the four above-mentioned attacks, Bluesnarfing is claimed to be much more serious than Bluejacking. These vulnerabilities are an inevitable result of technological innovation, and device manufacturers' continuously research and release firmware upgrades to address new challenges/problems as they arise.

3.12 Laptops

As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable.

Box 3.13 Spy Phone Software!!!

Spy Phone software is installed on the mobile/cell phone of employees, if the employers wants to monitor phone usage. The Spy Phone software is completely hidden from the user, once it is intsalled and collects all the available data such as SMS messages, ingoing/outgoing call history, location tracking, GPRS usage and uploads the collected data to a remote server.

The employer can simply access the designated website hosted by Spy Phone vendor, and after entering his/her account details, he/she can have full access to all the data collected 24 hours a day, 7 days a week. The employer can access this website through the Internet; hence, he/she can keep an eye on their employees, regardless where he/she is in the world. The employer can read all SMS messages (both incoming and outgoing), know who they (employees) are calling or who is calling them and where they were when the call was received.

Following are few Spy Phone Software(s) available in the market:

1. **SpyPhonePlus:** http://www.spyphoneplus.com/
2. **FlexiSpy:** http://www.flexispy.com/
3. **TheSpyPhone:** http://www.thespyphone.com/spyphone.html
4. **Mobile Spy:** http://www.mobile-spy.com/

Wireless capability in these devices has also raised cybersecurity concerns owing to the information being transmitted over other, which makes it hard to detect. In this section, we provide an elaborate discussion as to what measures the organizations can take in the face of cybersecurity threat brought by the wide-

as to what measures the organizations can take in the face of cybersecurity threat brought by the widespreading use of laptops.

The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive.

Such information can be misused if found by a malicious user. Senior executives commonly believe that the information stored on their laptops is only useful for them and would not be of any interest to others. Owing to this belief, most senior executives in an organization feel that it is unnecessary to protect the information stored on these laptops. However, this is not true. The following section provides some countermeasures against the theft of laptops, thereby avoiding cybersecurity exposures.

3.12.1 Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees' laptops and to reduce the likelihood that employees will lose laptops. Management also has to take care of creating awareness among the employees about physical security countermeasures by continuous training and stringent monitoring of organizational policies and procedures about these physical security countermeasures.[21]

1. **Cables and hardwired locks:** The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cables [see Figs. 3.14 (a) and (b)]. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms. However, the downside of the security cables lies in the fact that one can easily remove detachable bays such as CD-ROM bay, Personal Computer Memory Card Industry Association (PCMCIA) cards (see Ref. #10, Additional Useful Web References, Further Reading), hard disk drive (HDD) bay and other removable devices from the laptop as the cable only secures the laptop from being stolen. The other disadvantage of security cables is when the laptop is locked to an object that is not fixed or is weak enough for anyone to break it. In certain cases of laptop thefts, the thief dismantled or smashed the fixed item to which the laptop was attached to.

enough for anyone to break it. In certain cases of laptop thefts, the thief dismantled or smashed the fixed item to which the laptop was attached to.

2. **Laptop safes:** Safes made of polycarbonate – the same material that is used in bulletproof windows, police riot shields and bank security screens – can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.
3. **Motion sensors and alarms:** Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to

their loud nature, they help in deterring thieves. Modern alarm systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop. The owner of the laptop has a key ring device that communicates with the laptop alarm device. The alarm is triggered when the distance between the laptop alarm device and the key ring device crosses the specified range. Also available are security PCMCIA cards that act as a motion detector, an alarm system, and also have the capability to lockdown the laptop if the laptop is moved out of the designated range. They also secure the passwords and encryption keys and prevent access to the OS. These cards have batteries that keep them powered on even when the system is shutdown. Figure 3.15 shows some laptop alarm systems with sensors.

4. **Warning labels and stamps**: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which in turn makes the resale of stolen laptops a difficult process. Such lables are highly recommended for the laptops issued to top executives and/or key employees of the organizations.
5. **Other measures for protecting laptops are as follows:**
   - Engraving the laptop with personal details;
   - keeping the laptop close to oneself wherever possible;
   - carrying the laptop in a different and unobvious bag making it unobvious to potential thieves;
   - creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop;
   - making a copy of the purchase receipt, laptop serial number and the description of the laptop;
   - installing encryption software to protect information stored on the laptop;
   - using personal firewall software to block unwanted access and intrusion;
   - updating the antivirus software regularly;
   - tight office security using security guards and securing the laptop by locking it down in lockers when not in use;
   - never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an antitheft device;
   - disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

So far, we have discussed protection of corporate laptops in terms of physical access control. However, information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/open access.
3. Monitoring application security and scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not pose threats.
5. Proper handling of removable drives/storage mediums/unnecessary ports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing security patches and updates.
9. Installing antivirus software/firewalls/intrusion detection system (IDSs).
10. Encrypting critical file systems.
11. Other countermeasures:
    - Choosing a secure OS that has been tested for quite some time and which has a high security incorporated into it.
    - Registering the laptop with the laptop manufacturer to track down the laptop in case of theft.
    - Disabling unnecessary user accounts and renaming the administrator account.
    - Disabling display of the last logged in username in the login dialog box.
    - Backing up data on a regular basis.

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

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.

process is established into the system

in a list. This is still considered manual cracking, is time consuming

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.

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).

4.7 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 [illegible] Most backdoors are autonomic

A backdoor works in background and ... 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

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

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).

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.

	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.

4.9.5 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

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.

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 user-name 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

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.

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.

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 pro-

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

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.

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.

5.2.2 Phishing Techniques

In this section we will discuss common ways, the techniques[17] used by phishers to launch Phishing attacks.

1. **URL (weblink) manipulation:** URLs are the weblinks (i.e., Internet addresses) that direct the netizens/users to a specific website. In Phishing attack, these URLs are usually supplied as misspelled, for example, instead of www.abcbank.com, URL is provided as www.abcbank1.com. Phishers use Lobsterpot method of Phishing and make the difference of one or two letters in the URLs, which is ignored by netizens. This makes a big difference and it directs users to a fake/bogus website or a webpage. See Box 5.6 to know about an advanced Phishing attack known as homograph attack.
2. **Filter evasion:** This technique use graphics (i.e., images) instead of text to obviate from netting such E-Mails by anti-Phishing filters. Normally, these filters are inbuilt into the web browsers. For example,
   - Internet Explorer version 7 has inbuilt "Microsoft phishing filter." One can enable it during the installation or it can be enabled post-installation. It is important to note that it is *not enabled* by default.
   - Firefox 2.0 and above has inbuilt "Google Phishing filter," duly licensed from Google. It is enabled by default.
   - The Opera Phishing filter is dubbed Opera Fraud Protection and is included in version 9.5+.
3. **Website forgery:** In this technique the phisher directs the netizens to the website designed and developed by him, to login into the website, by altering the browser address bar through JavaScript commands. As the netizen logs into the fake/bogus website, phisher gets the confidential information very easily. Another technique used is known as "cloaked" URL – domain forwarding and/or inserting control characters into the URL while concealing the weblink address of the real website.
4. **Flash Phishing:** Anti-Phishing toolbars are installed/enabled (see Table 5.2) to help checking the webpage content for signs of Phishing, but have limitations that they do not analyze flash objects at all. Phishers use it to emulate the legitimate website. Netizens believe that the website is "clean" and is a real website because anti-Phishing toolbar is unable to detect it.
5. **Social Phishing:** Phishers entice the netizens to reveal sensitive data by other means and it works in a systematic manner.
   - Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.
   - The victim calls the bank on the phone numbers displayed in the mail.
   - The phone number provided in the mail is a false number and the victim gets redirected to the phisher.

5. **Social Phishing:** Phishers entice the netizens to reveal sensitive data by other means and it works in a systematic manner.
   - Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.
   - The victim calls the bank on the phone numbers displayed in the mail.
   - The phone number provided in the mail is a false number and the victim gets redirected to the phisher.
   - Phisher speaks with the victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank. For example, "Sir, we need to make sure that you are indeed our customer. Could you please supply your credit card information so that I can verify your identity?"
   - Phisher gets the required details swimmingly.
6. **Phone Phishing:** We have explained "Mishing" – mobile Phishing attacks ("Vishing" and "Smishing") in Chapter 3. Besides such attacks, phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the users to reveal their personal information such as account numbers and passwords. See Box 5.7 to understand the innovative Phishing attack launched on "Android Market" website.

Phishers usually take a broad approach by sending millions of E-Mail messages that appear to come from popular banks, online auction houses and other business houses. These E-Mail messages, pop-up windows and the websites appear to be official so that they can deceive many netizens to believe that they are legitimate. Unsuspecting netizens often respond to these requests for credit card numbers, passwords, account information or other personal and financial data. According to the 2009 Consumer Reports State of the Net Survey,[18] Phishing scams cost US$ 483 million in the US. Thus, we see that Phishing scams involve fraudulent E-Mail messages or fake websites designed to steal identity. Scam artists "phish" in an attempt to persuade millions of netizens/Internet users to disclose sensitive information. Now there is a new version of

an old scam called "Spear Phishing," a targeted E-Mail attack that a scammer sends only to people within a small group, which is explained in the next section.

5.2.3 Spear Phishing

"Spear Phishing" is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering. Here is how Spear Phishing scams work; Spear Phishing describes any highly targeted Phishing attack. Spear phishers send E-Mail that appears genuine to all the employees or members within a certain company, government agency, organization or group. The message might look like as if it has come from your employer, or from a colleague who might send an E-Mail message to everyone in the company (such as the person who manages the computer systems); it could include requests for usernames or passwords. Unfortunately, through the modus operandi of the Spear phishers, the E-Mail sender information has been faked or "spoofed." While traditional Phishing scams are designed to steal information from individuals, Spear Phishing scams work to gain access to a company's entire computer system. If you respond with a username or password, or if you click on the links or open the attachments in a Spear Phishing E-Mail, pop-up window or website, then you might become a victim of ID theft and you might put your employer or group at risk.

Spear Phishing also describes scams that target people who

phishers, the E-Mail sender information has been faked or "spoofed." While traditional Phishing scams are designed to steal information from individuals, Spear Phishing scams work to gain access to a company's entire computer system. If you respond with a username or password, or if you click on the links or open the attachments in a Spear Phishing E-Mail, pop-up window or website, then you might become a victim of ID theft and you might put your employer or group at risk.

Spear Phishing also describes scams that target people who use a certain product or website. Scam artists use any information they can to personalize a Phishing scam to as specific a group as possible. Thus, "Spear Phishing" is a targeted E-Mail attack that a scammer sends only to people within a small group, such as a company. The E-Mail message might appear to be genuine, but if you respond to it, you might put yourself and your employer at risk. You can help avoiding Spear Phishing scams by using some of the same techniques you have already used to help avoid standard Phishing scams (see Box 5.8).

Whaling

This is a specific form of "Phishing" and/or "Spear Phishing" – targeting executives from the top management in the organizations, usually from private companies. The objective is to swindle the executives into revealing confidential information. Whaling targets C-level executives sometimes with the help of information gleaned through Spear Phishing, aimed at installing malware for keylogging or other backdoor access mechanisms.

The names given to various *Internet scams* are found to be amusing. *Whaling* may have been derived from the fact that the people targeted are *top-ranking executives*. The difference between Spear Phishing and whaling appears to be a bit cloudy. It seems, whaling involves more extensive reconnaissance about the target rather than the target being enticed to be a victim of Spear Phishing attack.

E-Mails sent in the whaling scams are designed to masquerade as a critical business E-Mail sent from a legitimate business body and/or business authority. The content of an E-Mail usually involves some kind of falsified industry-wide concern and is meant to be tailored for executives.

Whaling phishers have also forged official looking FBI subpoena E-Mails and claimed that the manager needs to click a link and install special software to view the subpoena. In the case of the recent 2008 FBI subpoena whaling scam, 20,000 corporate CEOs were attacked. Approximately 2,000 of them fell for it and clicked on the whaling link, believing it would download a "special" browser add-on to view the entire subpoena document. In truth, the linked software was a keylogger that secretly recorded the CEOs passwords

5.3 Identity Theft (ID Theft)

This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits (introduced in Section 1.5.21, Chapter 1). The person whose identity is used can suffer various consequences when he/she is held responsible for the perpetrator's actions. In many countries, specific laws make it a crime to use another person's identity for personal gain.[34] As mentioned in the "introduction" section, ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 66D).

Visit the weblink http://njaes.rutgers.edu/money/identitytheft/default.asp to undergo a quiz on identity theft to test your awareness and to get tips to avoid to be victim of identity theft.

The statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as Identity Theft Resource Center (ITRC), with the objective to extend the support to the society to spread awareness about this fraud (see Box 5.14).

According to 2010 Report published by Javelin Strategy & Research[35] the number of "identity fraud victims" were increased by 12% during 2009 and "amount of fraud" increased by 12.5%. Key statistics noted about total identity frauds in the US are as mentioned below:

1. The total fraud amount was US$ 54 billion.
2. The average amount spent by the victim was US$ 373 and the time of 21 hours to resolve the crime.
3. In total, 11.1 million adults were found to be victims of ID theft, which amounts to 4.8% of the population being a victim of identity fraud in 2009.
4. 13% of identity frauds were committed by someone who the victim knew.

According to 2010 Report published by Javelin Strategy & Research[36] the number of "identity fraud victims" were increased by 12% during 2009 and "amount of fraud" increased by 12.5%. Key statistics noted about total identity frauds in the US are as mentioned below:

1. The total fraud amount was US$ 54 billion.
2. The average amount spent by the victim was US$ 373 and the time of 21 hours to resolve the crime.
3. In total, 11.1 million adults were found to be victims of ID theft, which amounts to 4.8% of the population being a victim of identity fraud in 2009.
4. 13% of identity frauds were committed by someone who the victim knew.
5. Online methods accounted for only 11% of ID theft in 2009.
6. Offline methodology such as stolen wallets and paperwork account for almost half (43%) of all ID thefts.

Federal Trade Commission (FTC) has provided the statistics about each one of the identity fraud mentioning prime frauds presented below.[36]

1. **Credit card fraud (26%):** The highest rated fraud that can occur is when someone acquires the victim's credit card number and uses it to make a purchase. Chapter 11 (see Section 11.4.2) provides many illustrations on credit card frauds.
2. **Bank fraud (17%):** Besides credit card fraud, cheque theft and Automatic Teller Machines (ATM) pass code theft have been reported that are possible with ID theft. Chapter 11 (see Section 11.4.1) provides many illustrations on banking-related frauds.
3. **Employment fraud (12%):** In this fraud, the attacker borrows the victim's valid SSN to obtain a job.
4. **Government fraud (9%):** This type of fraud includes SSN, driver license and income tax fraud.
5. **Loan fraud (5%):** It occurs when the attacker applies for a loan on the victim's name and this can occur even if the SSN does not match the name exactly.

Readers may like to visit Section 11.7, Chapter 11, where many forms of online scams are described. It is important to note the various usage of ID theft information.[37]

1. 66% of victims' personal information is used to open a new credit account in their name.
2. 28% of victims' personal information is used to purchase cell phone service.
3. 12% of victims end up having warrants issued in their name for financial crimes committed by the identity thief.

The statistics proves the importance of ID theft and the frauds related with ID theft are increasing day-by-day. ITRC, in the US, is putting enormous efforts to create awareness among the society to reduce such

5.3.1 Personally Identifiable Information (PII)

The fraudster always has an eye on the information which can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual. PII has four common variants based on personal, personally, identifiable and identifying.

The fraudsters attempts to steal the elements mentioned below, which can express the purpose of distinguishing individual identity:

1. Full name;
2. national identification number (e.g., SSN);
3. telephone number and mobile phone number;

4. driver's license number;
5. credit card numbers;
6. digital identity (e.g., E-Mail address, online account ID and password);
7. birth date/birth day;
8. birthplace;
9. face and fingerprints.

The fraudster may search for following about an individual, which is less often used to distinguish individual identity; however these can be categorized as potentially PII because they can be combined with other personal information to identify an individual.

1. First or last name;

5.3.2 Types of Identity Theft

Identity is stolen in order for someone to commit the crime. ID theft is related to many areas:

1. Financial identity theft;
2. criminal identity theft;
3. identity cloning;
4. business identity theft;
5. medical identity theft;
6. synthetic identity theft;
7. child identity theft.

Financial Identity Theft

Financial ID theft includes bank fraud, credit card fraud, tax refund fraud, mail fraud and several more. In total, 25 types of financial ID thefts are investigated by the US Secret Service. Financial identity occurs when a fraudster makes a use of someone else's identifying details, such as name, SSN and bank account details, to commit fraud that is detrimental to a victim's finances. For example, the fraudster fraudulently can open a new credit card account in the victim's name and the card charges up, payment is neglected, leaving the victim with bad credit history (i.e., horrible credit score) and a world of debt. In some cases, the fraudster will completely take over a victim's identity, which enables the fraudster to easily open bank accounts, multiple credit cards, purchase a vehicle, receive a home mortgage or even find employment in the victim's name.

The process of recovering from the crime is often expensive, time-consuming and psychologically painful. Many a times, before a crime is detected, the fraudster is capable of running up hundreds to thousands of dollars worth of debt in the victim's name. This type of fraud often destroys a victim's credit and it may take weeks, months or even years to repair. As technology moves along and fraudsters become more advanced, financial ID theft will continue to pose a great threat to many individuals.

Criminal Identity Theft

It involves taking over someone else's identity to commit a crime such as enter into a country, get special permits, hide one's own identity or commit acts of terrorism. These criminal activities can include:

1. Computer and cybercrimes;
2. organized crime;

3. drug trafficking;
4. alien smuggling;
5. money laundering.

Individuals who commit ID theft are not always out to steal the victim's money or ruin victim's credit. This type of fraud/theft occurs when a fraudster uses the victim's name upon an arrest or during a criminal investigation. The personal information given by a fraudster to a law enforcement officer may include counterfeited document such as driver's license, birth certificate, etc. Unfortunately, the victim of criminal ID theft may not know what warrant has been issued under his/her name for quite some time. The victim will only come to know in case of being detained on a routine traffic stop and arrested due to outstanding and overdue debts. In some cases, the fraudster will appear in court for the violation and enter a guilty plea without the victim's knowledge. This may place the victim's name into countywide or state-wide criminal database with a huge blemish language on the record.

There have been several instances where victims of criminal ID theft do not learn of an impersonation until being denied for employment or terminated from a job. This occurs when an employer conducts a criminal background search and finds that the victim has a criminal history that he/she lied about or charges that forbid him/her from working in that particular environment. When this happens, there is very little a victim can do to salvage the job, as an employer has the right to proceed with termination over entering false information on an application.

The victims of this crime are left with the burden to clear their own name in the eyes of the criminal justice system. It is very important to act quickly in order to minimize the damage and get your life back in order. What makes the process so difficult is the fact that officials working within the criminal justice system are the only ones capable of correcting the data. It is very crucial and important to contact local police department immediately in case of becoming a victim of criminal ID theft. This should be the first step in building a case and clearing your name.

Identity Cloning

Identity cloning may be the scariest variation of all ID theft. Instead of stealing the personal information for financial gain or committing crimes in the victim's name, identity clones compromise the victim's life by actually living and working as the victim. ID clones may even pay bills regularly, get engaged and married, and start a family. In summary, identity cloning is the act of a fraudster living a natural and usual life similar to a victim's life, may be at a different location.

An identity clone will obtain as much information about the victim as possible. They will look to find out what city and state the victim (he/she) was born in, what street he/she grew up on, where he/she attended school and what relationships he/she may have been involved in. They will also want to know information concerning the victim's parents and other family members. In a nutshell, identity clones want as much personal information about the victim as they can attain. This enables them to answer questions in an informative manner when they are on the move or asked about the victim's life.

Business Identity Theft

"Bust-out" is one of the schemes fraudsters use to steal business identity; it is paid less importance in comparison with individual's ID theft. A fraudster rents a space in the same building as victim's office. Then he applies for corporate credit cards using victim's firm name. The application passes a credit check because the company name and address match, but the cards are delivered to the fraudster's mailbox. He sells them on the street and vanishes before the victim discovers the firm's credit is wrecked.[40] Hence, it is extremely important to protect business sensitive information (BSI) to avoid any further scams.

BSI is the information about the business/organization, privileged in nature and/or proprietary information which, if it is compromised through alteration, corruption, loss, misuse or unauthorized disclosure, could cause serious damage to the organization. Such information is like a "sensitive asset" for the organization.[41]

Identity theft in the business context occurs most often when someone knocks off the victim's product and masquerades their shoddy goods as victim's. It is a kind of intellectual property theft. Nowadays, technology has made it easier for the trademarks and security devices such as holograms to be knocked off swimmingly. The consumers should no longer rely on trademarks alone to certify the authenticity of the goods and should verify their source of origin.

Medical Identity Theft

India is known to have become famous for "medical tourism." Thousands of tourists, every year visit India with dual purpose – touring the country plus getting their medical problems attended to (surgeries, total health check, Kerala massage, etc.) because India has made name for good quality and yet reasonable priced (compared with Europe and the US) in medical services. In the process thousands of medical records of foreigners as well as locals who avail medical facility get created. This has created a boom for cybercriminals.

Healthcare facilities now are very different compared to how they were used a decade back. There are greate opportunities for protected health information (PHI) changing hands when multiple agencies are connecte over computer networks and the Internet – for example, medical representatives, health officers, doctors medical insurance organizations, hospitals, etc. to name a few (see Fig. 5.2).

Medical facility providers are moving from cumbersome paper records to faster and easier file and trac electronic records; however, the concern over medical ID theft[43] is growing. The stolen information ca be used by the fraudster or sold in the black market to people who "need" them. This could lead to man more cases. For example, invoice of thousands of dollars of emergency medical services was received by man situated in Houston (Texas), who had never had any health issues, as reported in the New York Times A fraudster had used this man's identity for the fraudster's emergency medical needs.

Medical ID theft can be dangerous not only from a financial perspective as explained in the case above but also from a medical perspective. If the fraudster has successfully stolen the victim's identity and receive treatment, the record can become part of a victim's permanent medical record. For example, a patient coul be unconscious after an accident. The emergency room reads that during a previous admission the "patient" indicated he/she is not allergic to the medication the doctor believes will be most beneficial for the unconscious patient. Relying on the prior medical record, the doctor administers that drug which, in reality, th patient is severely allergic to.

According to a 2008 Identity Theft Resource Center survey, some of the reasons why medical ID theft is particularly damaging the victims include:

1. Approximately one-third of victims of medical ID theft surveyed had someone else's medical information or medical history on their medical record, increasing the possibility of patients being treated incorrectly because of incorrect medical records.
2. More than 10% of victims of medical ID theft surveyed were denied health or life insurance for unexplained reasons.
3. More than two-third of victims surveyed receive a bill for medical services that were provided to an imposter.

ModernHealthcare.com reported a noticeable spike in attempted medical ID theft. This has been confirmed during June 2008 wherein the University of Utah Hospital announced that the personal information of 2.2 million patients had been stolen.

The World Privacy Forum estimates that there are more than 250,000 cases of medical ID theft each year and acknowledges that medical ID theft is a crime that can cause great harm to the victims. Medical ID theft has been addressed by HIPAA and HITECH Acts in the US (see Box 5.16 as well as Fig. 5.2).

Synthetic Identity Theft

This is an advanced form of ID theft in the ID theft world. The fraudster will take parts of personal information from many victims and combine them. The new identity is not any specific person, but all the victims can be affected when it is used.

Child Identity Theft

Parents might sometimes steal their children's identity to open credit card accounts, utility accounts, bank accounts and even to take out loans or secure leases because their own credit history is insufficient or too damaged to open such accounts.

2. age;
3. country, state or city of residence;
4. gender;
5. name of the school/college/workplace;
6. job position, grades and/or salary;
7. criminal record.

The information can be further classified as (a) non-classified and (b) classified. [Classification scheme is also explained in Chapter 9 (Section 9.11) in the context of media and asset protection.]

1. **Non-classified information**
   - **Public information:** Information that is a matter of public record or knowledge.
   - **Personal information:** Information belongs to a private individual but the individual commonly may share this information with others for personal or business reasons (e.g., addresses, telephone numbers and E-Mail addresses).
   - **Routine business information:** Business information that do not require any special protection and may be routinely shared with anyone inside or outside of the business.
   - **Private information:** Information that can be private if associated with an individual and individual can object in case of disclosure (e.g., SSN, credit card numbers and other financial information).
   - **Confidential business information:** Information which, if disclosed, may harm the business (e.g., sales and marketing plans, new product plans and notes associated with patentable inventions).
2. **Classified information**
   - **Confidential:** Information that requires protection and unauthorized disclosure could damage national security (e.g., information about strength of armed forces and technical information about weapons).
   - **Secret:** Information that requires substantial protection and unauthorized disclosure could seriously damage national security (e.g., national security policy, military plans or intelligence operations).
   - **Top secret:** Information that requires the highest degree of protection and unauthorized disclosure could severely damage national security (e.g., vital defense plans and cryptologic intelligence systems).

ID theft fraudsters and/or industrial/international spies target to gain the access to private, confidential, secret and top secret information.

6.3 Why Do We Need Cyberlaws: The Indian Context

Cyberlaw is a framework created to give legal recognition to all risks arising out of the usage of computers and computer networks. Under the purview of cyberlaw, there are several aspects, such as, *intellectual property, data protection and privacy, freedom of expression* and *crimes committed using computers*. The Indian Parliament passed its first cyberlaw, the ITA 2000, aimed at providing the legal infrastructure for E-Commerce in India. ITA 2000 received the assent of the President of India and it has now become the law of the land in India. The Government of India felt the need to enact relevant cyberlaws to regulate Internet-based computer-related transactions in India. It manages all aspects, issues, legal consequences and conflict in the world of cyberspace, Internet or WWW. In the Preamble to the Indian ITA 2000, it is mentioned that it is an act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as *electronic commerce*. The reasons for enactment of cyberlaws in India are summarized below:

1. Although India possesses a very well-defined legal system, covering all possible situations and cases that have occurred or might take place in future, the country lacks in many aspects when it comes to newly developed Internet technology. It is essential to address this gap through a suitable law given the increasing use of Internet and other computer technologies in India.
2. There is a need to have some legal recognition to the Internet as it is one of the most dominating sources of carrying out business in today's world.
3. With the growth of the Internet, a new concept called *cyberterrorism* came into existence. Cyberterrorism includes the use of disruptive activities with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives in the world of cyberspace. It actually is about committing an old offense but in an innovative way.

Keeping all these factors into consideration, Indian Parliament passed the Information Technology Bill on 17 May 2000, known as the ITA 2000. This law is based on Model UNCITRAL law for E-Commerce (see Ref. #11, Articles and Research Papers, Further Reading). It talks about cyberlaws and forms the legal framework for electronic records and other activities done by electronic means. There are strengths as well as limitations in the ITA 2000; they are explained in Sections 6.4.2 and 6.4.3. A legal framework for the cyberworld was conceived in India, in the form of a draft E-Commerce Act 1998 – thereafter, the subject of cyberlaws started haunting the government. The basic law for the cyberspace transactions in India has emerged in the form of the ITA 2000. With that background, the Indian IT Act is briefly discussed in the following section.

6.4 The Indian IT Act

As mentioned above, this Act was published in the year 2000 with the purpose of providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as *electronic commerce*. Electronic communications involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies. Another purpose of the Indian IT Act was to amend the Indian Penal Code (IPC),[11] the Indian Evidence Act 1872,[12] the Bankers' Books Evidence Act 1891,[13] the Reserve Bank of India Act 1934[14] and matters connected therewith or incidental thereto. Cybercrimes punishable under various Indian laws are mentioned in Box 6.10. The Reserve Bank of India Act has got Section 58B about Penalties. Subsequently, the Indian IT Act underwent some important changes to accommodate the current cybercrime scenario; a summary of those changes is presented in Table 6.7 – note specially the changes to Section 66 and the corresponding punishments for cyberoffenses. Readers should also refer to Section 6.8.1 (Overview of Changes Made to the Indian IT Act) where the changes are explained in details.

Cybercrimes and Other Related Crimes Punishable

Table 6.6 | The Indian ITA 2000: Summary of contents (main elements only)

From Table 6.6, we can see that in particular, Sections 65, 66, 67, 71, 72, 73 and 74 in CHAPTER XI (Offences) of the Indian ITA 2000 are relevant to the discussion of cybercrime in legal context. The relevant portion from that is as follows:

1. **Section 65: Tampering with computer source documents**
   Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer

programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to 3 years, or with fine which may extend up to 2 lakh rupees (₹ 2,00,000), or with both.
Explanation: For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

2. **Section 66: Computer-related offences**
   (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
   (2) Whoever commits hacking shall be punished with imprisonment up to 3 years, or with fine which may extend up to 5 lakh rupees (₹ 5,00,000), or with both.

3. **Section 67: Punishment for publishing or transmitting obscene material in electronic form**
   Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter

3. **Section 67: Punishment for publishing or transmitting obscene material in electronic form**
Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to 3 years and with fine which may extend to 5 lakh rupees (₹ 5,00,000) and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to 3 years and with fine which may extend to 5 lakh rupees (₹ 5,00,000) and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to 5 years and also with fine which may extend to 10 lakh rupees (₹ 10,00,000).

4. **Section 71: Penalty for misrepresentation**
Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

5. **Section 72: Penalty for breach of confidentiality and privacy**
Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there-under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

6. **Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars**
(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that:
(a) The Certifying Authority listed in the certificate has not issued it; or
(b) the subscriber listed in the certificate has not accepted it; or
(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of subsection (1) shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

6. **Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars**

(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that:

(a) The Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of subsection (1) shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with both.

7. **Section 74: Publication for fraudulent purpose**

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees (₹ 1,00,000), or with

Both.

6.7 Digital Signatures and the Indian IT Act

In this section, some potential problems regarding the terms *digital signatures* and *electronic signatures* are discussed. Public-key certificate and the role of public-key infrastructure (PKI) are also explained. Impact of oversights in ITA 2000 regarding digital signatures is also discussed. For the benefit of readers without technical backgroud, the PKI and related terms are explained. For the discussion in this section, we will refer to Table 1.1 of Chapter 1 (Cybercrimes/Cases Registered and Persons Arrested under IT Act during 2004–2007); there is a mention of "publishing false digital signature certificate," that is, item No. 7 in that table. CHAPTER XI (Offences) of the Indian IT Action mentions "penalty for publishing false digital signature certificate in certain particulars." With those threads, in this section we will discuss particularly about digital signatures in context of the Indian IT Act. Before we do that, we need to understand a few technical concepts.

6.7.1 Public-Key Certificate

A public-key certificate is a digitally signed statement from one entity, saying that the public key (and some other information) of another entity has some specific value. A digital signature is a type of electronic signature that is used to guarantee the integrity of the data. When linked to the identity of the signer – using a security token such as X.509 Certificates – a digital signature can be used for non-repudiation, since it links the signer with the signed document. An X.509 Certificate contains information about the certificate subject and the certificate issuer (the CA that issued the certificate). A certificate is encoded in Abstract Syntax Notation One (ASN.1), a standard syntax for describing messages that can be sent or received on a network. The role of a certificate is to associate an identity with a public-key value. A certificate includes:

1. X.509 version information;
2. a serial number that uniquely identifies the certificate;
3. a common name that identifies the subject;
4. the public key associated with the common name;
5. the name of the user who created the certificate, known as the subject name;
6. information about the certificate issuer;
7. signature of the issuer;
8. information about the algorithm used to sign the certificate;
9. some optional X.509 version 3 extensions. For example, an extension exists that distinguishes between CA certificates and end-entity certificates.

Some of the most widely visible application of X.509 Certificates today is in Web browsers (such as Netscape Navigator and Microsoft Internet Explorer) that support the Secure Socket Layer (SSL) Protocol. SSL is a security protocol that provides privacy and authentication for your network traffic. These browsers can only use this protocol with webservers that support SSL. Other technologies that rely on X.509 Certificates include:

1. Code-signing schemes, such as signed Java Archives and Microsoft Authenticode;
2. Secure E-Mail standards, such as privacy-enhanced mail (PEM) and secure/multipurpose Internet mail extensions (S/MIME);
3. E-Commerce protocols, such as secure electronic transactions (SET).