Preface

Information technology (IT) is the buzzword of the 21st century. It uses computers to store, retrieve, transmit, and manipulate data. Today, computers are used to perform every other task such as publishing a newspaper, designing a building, training an athlete, practising landing of an airplane, etc. The use of computers has become so widespread that almost every electrical and electronic device (such as washing machines, air conditioners, etc.) has a small embedded computer in it. In India, computers are now a part of millions of households. Even the mobile phones that we use are smartphones (phones with computing technology) that are connected to the Internet.

Information technology has revolutionized our lifestyle. Banking and shopping are done online. Employees work from home to save the time spent in going to offices. Therefore, in today's scenario learning about computers is meant not just for students pursuing a career in engineering and technology but is also mandatory for students in other professions such as journalism, nursing, archaeology, construction, commerce, and management, to name a few. Computing skills always help one to be more productive and self-sufficient. Therefore, a basic knowledge of computers and its technology will certainly pay dividends in future.

About the Book

Information Technology and Its Applications in Business has been specifically designed as per the latest syllabus of University of Calcutta. The book has been written for commerce students and is an ideal text for self-learning basic computer concepts (such as organization, architecture, input–output devices, and memory of computer) as well as advanced topics (such as operating systems, computer networks, and databases). The book also offers a hands-on experience of MS-Word, PowerPoint, Excel, Access, and Tally.

Key Features

Pictorial approach Numerous well-labeled diagrams are provided throughout the text for clear understanding of the concepts.

Practical orientation A number of examples and chapter-end exercises in the form of review questions are provided, which enables the students to check their understanding of the concepts.

Comprehensive coverage The book provides comprehensive coverage of important topics ranging from basic computers to advance technologies.

Glossary A list of key terms is provided at the end of each chapter that facilitates revision of the important topics learned.

Notes Important concepts are provided in between the text for a quick recap.

Lab exercises The book has a separate section on lab activities that includes practicals in MS-Office and Tally.

Solved question papers Solutions to previous years' university questions papers have been included in the book.

One-to-one mapping with syllabus The content of the book has a direct mapping with the syllabus prescribed by the University of Calcutta for commerce students.

Organization of the Book

The first part of the book, divided into seven chapters, deals with theoretical concepts. A brief overview of each chapter is provided here.

Chapter 1 clarifies the difference between data, information, and knowledge. It discusses the impact of IT in business, recent trends, and different types of information systems.

Chapter 2 describes the binary number system representation and discusses the binary, octal, and hexadecimal number systems. The chapter enables the reader to perform arithmetic operations such as addition, subtraction, multiplication, and division on binary numbers. Important binary codes such as American Standard Code for Information Interchange (ASCII), Extended Binary Coded Decimal Interchange Code (EBCDIC), binary coded decimal (BCD), and gray codes are also discussed in the chapter.

Chapter 3 provides an introduction to computers. This chapter gives the characteristics, applications, classifications, basic organization of the computer system, and a detailed description of different types of input and output devices. It explains the significance of memory hierarchy and discusses the different types of primary, secondary, and tertiary memory, which are widely used to store data. It also brings forth the basic processor architecture (including RISC and CISC), the instruction set and concepts such as hardware, software, operating system, and programming languages.

Chapter 4 gives a brief introduction to the traditional file-oriented approach of data management and introduces the concept of databases, their architecture, models, and components. It also illustrates how data can be fetched from tables using query language. This chapter introduces two important technologies—data warehousing and data mining—which has revolutionized the way in which massive amounts of data are stored and analysed.

Chapter 5 discusses computer networks, its applications, the connecting media, data transmission mode, network topologies, area networks, wireless networks, Bluetooth, and the devices used to form a network.

Chapter 6 introduces the concept, evolution, and different services provided by the Internet. It also includes discussions on Intranet, Extranet, IP address, DNS, URL, IP, TCP, FTP, UDP, TELNET, HTML, DHTML, and XML.

Chapter 7 brings forward threats to data security and the preventive measures that can be undertaken for protection. It also discusses the utility and working of antivirus software, firewalls, data encryption, digital certificates, digital signature, and digital envelope.

The second part of the book includes *Lab Exercises* that will prove very beneficial for having hands-on experience while working with computer systems. These activities cover five modules—MS-Word, Excel, PowerPoint, Access, and Tally.

Online Resources

The online resource centre provides the following resources for the faculty and students using this text:

- Objective type questions with answers
- Solutions to chapter-end exercises
- Solutions to model question papers

Acknowledgments

Many people have helped me in writing this book. Fortunately, I have had the fine support of my family, friends, and fellow members of the teaching staff at Shyama Prasad Mukherji College for Women, University of Delhi.

My special thanks would always go to my father Mr Janak Raj Thareja, my mother Mrs Usha Thareja, my brother Pallav, and sisters Kimi and Rashi, who are a source of inspiration and divine blessings for me. I am especially thankful to my son Goransh who has been very patient and cooperative in letting me realize my dreams. My sincere thanks go to my uncle Mr B.L. Theraja for his inspiration and guidance in writing this book.

I would also like to express my gratitude to Prof. Ramit Kumar Roy (St Xavier's College, University of Calcutta) for his valuable inputs. Without his guidance and support, it would have been very difficult to complete this book.

Last but not least, my acknowledgements will be incomplete if I do not thank the editorial team at Oxford University Press, India for their help and support.

Reema Thareja

Brief Contents

Detailed Contents

CHAPTER

7 Security Issues

7.1 INTRODUCTION

Data security is a broad issue that encompasses security for all the data and information that an organization stores on the computer and security of all the transactions that are made using the Internet. It ensures authenticated access of data. The term 'data security' is gaining topmost priority, especially in financial and government institutions as lack of security is a serious threat to the integrity and privacy of any organization.

Since the Internet is an insecure channel for exchanging private data or messages and intrusion or frauds like phishing (discussed later) are very common, some methods must be implemented to protect data. In this chapter, we will read about the threats to security and learn about the protective measures that can help the users protect their data from unwanted access. Before delving into these issues, let us try to find answers to some important questions.

How can Security of Data be Compromised?

Security of data may be compromised in the following ways:

- Unauthorized users from within or from outside the organization may access the data.
- Authorized or unauthorized users may modify the existing data, add wrong data, or delete some important data.

Figure 7.1 reveals the sources that can cause threat to security of data. While we cannot control damage to data because of natural disasters, damage due to humans can always be controlled by implementing sound security mechanisms. A hacker is someone who either breaks into the system for which he has no authorization or goes beyond his limits of legitimate access. A hacker can be a cracker; a cracker means a person who breaks into the system by password cracking or by cracking the security measures implemented to protect the data.

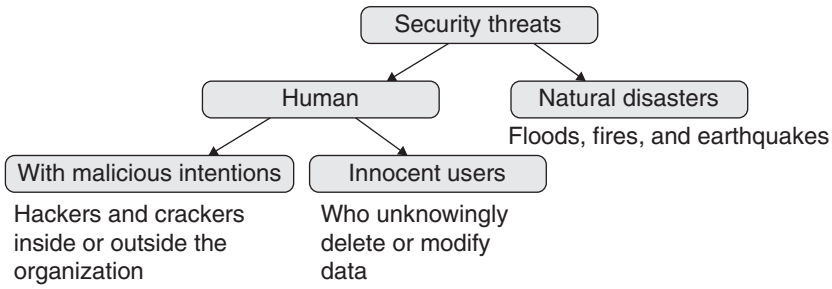


Figure 7.1 Types of security threats

However, a big threat to data security can be employees within the organization who do not have any malicious intention, but they either unknowingly alter data themselves or leave the data vulnerable to be accessed by attackers. For example, a programmer can write a code that can result in system crash. Another example is a clerk who saves an important file on the desktop. This file can then be accessed by any other user with malicious intentions.

How is Confidential Data Tampered?

Confidential data may be tampered in the following ways:

- Delete vital information from the database—for example, if someone deletes the records of your customers, there is no means to contact them.
- Steal information—for example, if your competitor steals information about your customers and offer them goods and services at a heavy discount, then you will have to bear a great loss.
- Modify data—for example, if a student gets access to the master computer of your school and modifies his marks, then the whole concept of taking exams and evaluating students will become a wasteful exercise. Another example could be that an employee can gain access to the attendance records and mark himself present on days when he had not gone to office.

How can we Protect Confidential Data?

The following are the ways to protect confidential data:

- Prevent the data from being altered or accessed by people with malicious intentions by implementing sound security policies.
- Detect any attempt to damage, modify, or steal data. Various tools are available in the market that detect and reveal any attempt made to breach data security.
- Recover lost or damaged data if someone has already tampered with it.

7.2 THREATS TO DATA SECURITY

The most common threats to data security come either from use of malwares or through fraud like phishing. The common threats to security can be classified as follows.

7.2.1 Malware

Malware or malicious software (meaning software designed with wrong intentions) is software specifically designed to gain access to a computer either to disrupt its operation or gather sensitive data from it. It is a big threat to Internet security and includes computer virus, spyware, worms, Trojan horse, etc. Malwares are usually embedded within legitimate software that is either useful or attractive.

Virus

A computer virus is a small program that gets loaded in the computer without the user's knowledge and replicates itself repeatedly. Such a piece of code is dangerous because it will quickly use all available memory and finally halt the system. An even more dangerous type of virus may corrupt or delete files from the computer and may spread itself to other computers by using the user's email program. Sources of computer virus include the following:

- Attachments in email messages or instant messaging messages
- Attachments of funny images, greeting cards, or audio and video files
- Downloads from the Internet

Computer viruses are thus always undesirable as they slow down the computer's performance, cause erratic behaviour, loss of data, and frequent crashes.

Features The features of virus are as follows:

- It replicates itself.
- It requires a host file to spread.
- It is activated by an external action.

Types of virus Viruses are of the following types.

Boot viruses These viruses were used to infect floppy disks. However, as floppy disks are no longer used, the boot virus infects only the master boot records of the hard disk. The boot record is a program that loads the operating system in the memory when the computer is turned on.

Boot record viruses either overwrite or replace the boot record and move it to a different location in the hard disk. When the operating system is loaded in memory, the virus also gets loaded along with the operating system.

Once the virus gets loaded in the memory, it performs its intended task. The only way to protect the computer in case of boot virus is to boot the operating system from another hard drive or a bootable CD or DVD. Examples of boot viruses include Polyboot.B, AntiEXE, Disk Killer, and Stoned.

The master boot record is the first sector on a partitioned storage device.

Program viruses or file infector viruses These viruses infect only executable files with extensions such as .BIN, .COM, .EXE, .OVL, .DRV, and .SYS. When an infected file is executed, the file along with the virus gets loaded in the memory. The virus is then free to

perform its intended task. The virus may overwrite the infected file or replace some parts of the file in such a way that every time the program or file is intended to execute, the virus gets executed. Most of the viruses belong to this category. However, program viruses are better than boot viruses as they can be removed easily, for example, Snow.A, Jerusalem, and Cascade.

The program or file virus uses a file as its host as it sticks to a file.

Multipartite viruses These viruses are a combination of two types of viruses—boot viruses and program viruses. Like program viruses, they infect an executable file and when the infected file is executed, the multipartite virus infects the master boot records (as the boot virus). For example, Emperor, Anthrax, Tequilla, and One_Half.

Stealth viruses These viruses use several techniques to avoid their detection. For example, stealth virus will remove the virus code from an infected file when antivirus software is examining the system so that the file is not detected as infected.

Some stealth viruses redirect the hard disk head so that the next read operation is done from another memory sector instead of the correct one. Some may alter the attributes of the infected file.

Polymorphic viruses These viruses create copies during replication. These replicated copies are functionally equivalent but have different codes. The difference in codes is intentionally induced by randomly inserting superfluous instructions, changing the order of instructions, or by choosing a different encryption algorithm each time a copy of the virus is created.

The real power of this virus lies in the fact that since each infection is different from the other, it is very difficult for an antivirus software to identify, locate, and remove them. Examples include Elkern, Marburg, Satan Bug, and Tuareg.

Macro viruses A macro virus infects documents that contain macros (a special type of program that performs a series of operations with a single action). A wide variety of programs, including Microsoft Word and Excel, support macros, and are thus, vulnerable to macro viruses.

For example, many a time, when working with Microsoft Word, you must have encountered a message as 'Problem in Normal.dot'. Macro virus infects `normal.dot` which is a file used by all the documents. Whenever users open any document (by indirectly using Normal.dot), the uninfected document also gets infected. When a macro virus-infected file is opened on another computer, the virus spreads on that computer too. Examples of macro viruses are Relax, Melissa.A, Bablas, O97M/Y2K, and WM.NiceDay.

ActiveX viruses Most Internet users do not know how to configure ActiveX and Java controls and thus leave a security hole in their computer. Many times, while surfing the Internet, we get a pop-up message saying 'Applets are not able to run', and asking 'allow or disallow?' Sometimes, certain websites ask users to download certain ActiveX or Java controls and we quickly download them.

By allowing these applications to run freely on our machines, we permit them to deliver all ActiveX viruses. Therefore, by simply turning off some ActiveX and Java controls in the browser, computers can be protected from such macro viruses.

Resident viruses A resident virus inserts itself in the computer's memory (RAM). From the memory itself, it performs all its intended tasks such as interrupting the system's operations and corrupting files and programs that are opened. A resident virus runs independently of the file that was originally infected. Examples include Randex, CMJ, Meve, and Mr Klunky.

Direct action viruses This type of virus replicates itself and performs its intended action only when the infected file is being executed. When the file is not being executed, the virus becomes dormant. Direct action viruses take action when a specific condition is met. When the virus becomes active, it infects all the files in its directory as well as in the directories specified in the AUTOEXEC.BAT file PATH. An example is the Vienna virus.

AUTOEXEC.BAT is a batch file stored in the root directory of the hard disk. It is used to perform some vital operations when the computer is booted.

Overwrite viruses This virus deletes the data stored in the infected files leaving them partially or totally useless. To clean a file infected by an overwrite virus, users have no option but to delete the file completely, thereby losing all its contents. Examples are Way, Trj. Reboot, and Trivial.88.D.

Directory virus A directory virus changes the paths that indicate the location of a file. When the user executes a directory virus-infected file (having extension as .EXE or .COM), he unknowingly runs the virus since the original file has been moved to another location by the virus.

Network virus These viruses rapidly spread through a LAN or through the Internet. Network viruses multiply through shared resources such as shared drives and files. When a computer gets infected, it searches through the network to attack another computer. When the other computer gets infected, it moves on to the next, and so on. Examples are Nimda and SQL Slammer.

Space filler (Cavity) viruses We have seen in Chapter 4 that many a time, some parts of a file are empty. The space filler virus use this empty space to house (or install) its code. It does not affect or damage the contents of the actual program itself. An example is the Lehigh virus.

FAT virus File allocation table (FAT) is a table maintained by the operating system to store information about location, size, and other details of files on the disk. The FAT virus attacks on the file allocation table.

The FAT virus makes it impossible for a computer to locate files. The virus spreads to the files when the FAT attempts to access them, thereby penetrating into the entire computer. When a file gets infected, to the users, it seems as if the file is missing or inaccessible.

The FAT virus disrupts a system completely by destroying data and forcing the user to reformat the system.

Worms

Like viruses, worms are programs written with malicious intentions that can replicate themselves and spread across a computer network. However, unlike viruses, most worms do not

interfere with the normal use of a computer. Moreover, they exist as separate entities and do not attach themselves with other files or programs.

However, worms may also take control over the computers on which they get installed and steal confidential data. Once a worm gets installed, it uses the email program of the user to send a copy of itself to everyone listed in his email address book. Then, it replicates itself to send itself out to everyone listed in each of the receiver's address book, and continues the replication process indefinitely. Worms use a lot of network bandwidth and memory which causes web servers, network servers, and individual computers to stop responding.

Once installed, a worm can connect to a remote computer over the Internet to download a more substantial piece of malicious software.

How a worm works A worm is a malicious code that locates vulnerabilities on a computer to exploit them. Once a computer gets infected, the worm will find other computers on its network with vulnerabilities so that they can also be accessed and infected.

Worms also spread through email attachments. To users, it seems as if the email has come from a known trusted person and the moment the user opens the email, the worm uses the user's email account and address book to copy itself and spread to other email recipients.

Worms can also attack applications such as Microsoft Word and Excel by inserting malicious code in documents and then use them as an attachment with email. The most destructive feature of a worm is that it can replicate itself 2,50,000 times over a period of several hours. Besides looking for other computers, worms also scan for unsecured servers and then replicate themselves on each server. Some worms are specifically designed to replicate themselves on specific days for making targeted attacks on special occasions.

The main aim of worms is to slow down the Internet due to the massive amount of traffic it creates. Worms can also gain unauthorized access to a website to attack it by sending thousands of requests in order to crash the site.

Worms also spread through pirated movies.

How to protect your computer from worms? The following are the ways to protect the computer from worms:

- Always use the latest operating system.
- Install antivirus software to remove the worm.
- Install a firewall that will guard against the downloading of the worm.
- Update your antivirus software on a regular basis.

Trojan Horse

A Trojan horse is a non-self-replicating malicious software that pretends to be harmless so that users can easily download it on the computer. It is usually contained inside a harmless program. Once executed, a Trojan may slow down the computer, cause loss or theft of data, give unauthorized access to its controller, ruin the FAT, and install a virus.

Types of Trojan horses Once a Trojan horse gets installed on your computer, its range of actions can vary from being harmless to destructive. For example, a Trojan can cause the following:

- It might display annoying messages on the screen.
- It can delete all vital files.
- It can steal confidential information like passwords.
- It may install viruses or another Trojan horse on the computer.
- It may allow the computer to be accessed from a remote machine.

The following are some common types of Trojan horses.

Remote administration Trojan horse This type of Trojan horse gives control of the infected computer to a hacker who can alter the registry, rearrange folders, change the login password, upload or download files, interrupt the infected computer's communication with other machines, erase files, type messages in a program that the user is currently running, open the CD-ROM drive door, play strange noises through the speaker, and even reboot the computer.

File serving Trojan horse This type of Trojan horse creates a file server (similar to the FTP server) on the infected machine. With this file server, the intruder (attacker) can control network connections, upload, and download files.

The file serving Trojan horse is so small in size (may be not more than 10 Kb) that it is difficult to be detected. It is often hidden in online games, funny forwarded messages, attachments in emails, or in other files that users may download from the Internet.

Denial of service attack Trojan horse This type is usually targeted to a primary server to enable a hacker gain control over one, several, or all computers in its network. After gaining the control, hackers flood the target server with traffic, thereby making it impossible for users to access certain websites.

Keylogging Trojan horse Keyloggers record every step of the user's activity on the infected computer (with regard to the mouse clicks and keys pressed). It emails the recorded information about keystrokes to the hacker. Hackers use this information for performing card fraud and identity theft. For example, hackers get information about username, password, credit card number, pins, and other valuable data to commit online thefts.

Password stealing Trojan horse This type of Trojan horse is used to steal passwords. Like keyloggers, this Trojan also transmits information about passwords to the hacker through email.

System killing Trojan horse These Trojans destroy everything in the system. Examples include Trojan.Killfiles.904 and Trojan.KillAV.

Trojan dropper This type of Trojan horse drops or downloads additional malicious files to the computer. These malicious files further infect the computer.

Joke Trojans Such a Trojan horse causes no damage to the computer but plays an annoying sound from the speaker or displays irrelevant messages on the screen like 'Now formatting hard drive'.

Icondance Trojan This Trojan horse causes no harm to the computer but minimizes all application windows and then starts rapidly scrambling all the desktop icons.

Some more Trojan horses Here are some more types of Trojan horses:

- Rootkit prevents malicious programs from getting detected.
- Trojan-FakeAV simulates the activity of antivirus software and aims at extorting money from innocent users for detecting and removing threats that are not even present on their computer.
- Trojan-Game Thief steals user account information from online gamers.
- Trojan-IM steals user's login details and passwords for instant messaging programs such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, and Skype.
- Trojan-Ransom prevents the users from accessing data stored on their computers. The attacker unblocks the data only after users pay them the ransom money demanded.
- Trojan-SMS sends text messages to premium rate phone numbers from the user's mobile phone.
- Trojan-Spy spies the user's activities on the computer using keyloggers by taking screenshots or getting a list of running applications.

Most antivirus software can detect and remove Trojan horses.

7.2.2 Spyware

A spyware is a malicious program that surreptitiously monitors the activity on a computer and reports that information to others without the user's consent. Spyware is usually used for tracking and storing the user's Internet browsing patterns, gaining information about user logins, bank, or credit card information; serving up pop-up ads to Internet users; installing additional software; redirecting web browsers to untrusted sites; modifying software settings; reading cookies; reducing network connection speeds; and causing slowdown or even crashing a computer system.

Spywares are bundled as a hidden piece of code in a freeware or shareware program, which can be difficult to remove once downloaded from the Internet.

7.2.3 Adware

Also known as advertising-supported software, adware is any software that is given to the user with advertisements embedded in the application. When users download a freeware or a shareware from the Internet that has an adware embedded in it, the adware gets installed in the user's computer. They can also spread through email attachments and shared files.

Adware comes under the category of malware because most of the times, they are unwanted. They are a form of spyware that tracks the user's Internet surfing habits and collects information about the user to display advertisements related to them. Users try to avoid them as they see it as a threat to their privacy and security over the Internet and also get annoyed due to the distraction caused by them.

Adware displays advertisements automatically without the user's permission.

Unlike spyware, adware does not transfer the user's personal information to another location. Both, however, slow down the computer speed and allow constant pop-up advertisements to plague the user.

7.2.4 Browser Hijacking

When a browser is hijacked, the attacker modifies the browser to permanently change the home page. This is basically done to boost web traffic hits or just to be asinine. Browser hijacking attacks are really irritating and most of the times, even good antivirus software take a long time to detect and free innocent users from such attacks.

7.2.5 Network Attacks

We will discuss some network attacks in this section.

Denial of service (DoS) attack It is an attempt to make a computer resource unavailable to its intended users. Generally, DoS attacks (Figure 7.2) target high-profile web servers such as banks, credit card payment gateways, government organizations, media, and root name servers. The common ways in which DoS attacks can be made are as follows.

Ping of flood In this scheme, the attacker sends numerous external communication requests to the target machine so that either it is unable to respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable.

Ping of death Normally, a ping packet in the network should not exceed 65,535 bytes. A packet greater than this is not only difficult to handle but may also cause the system to crash. Therefore, in this type of attack, ping packets of size greater than 65,535 bytes are deliberately sent.

Teardrop attack In routing, we have learnt that a message is split into packets. Each packet contains a sequence number so that the receiver can reassemble the message accurately. In the teardrop method of DoS, the attacker puts a confusing sequence number in the packets, thereby making it difficult for the receiver to reassemble the message. This may finally result in system crash.

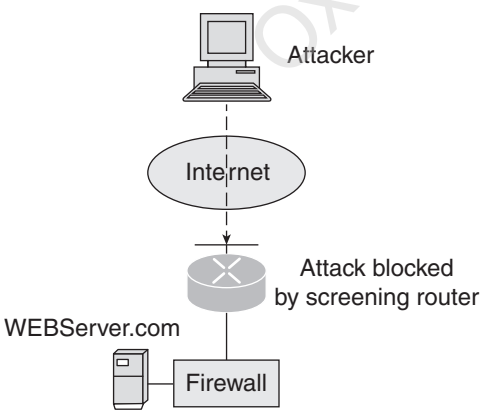
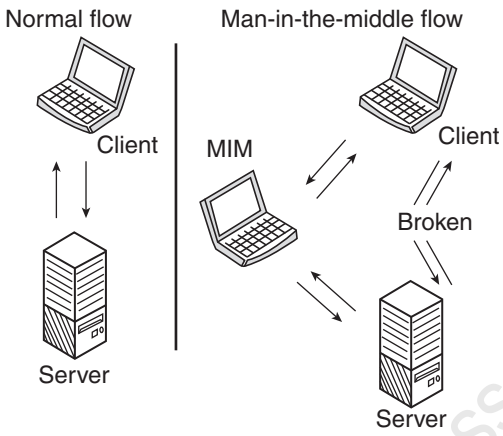


Figure 7.2 Denial of service attack

Mail bombs Unauthorized users may send a large number of email messages with large attachments to a particular mail server to fill its disk space so that other users are denied email services.

In other types of DoS attacks, the attacker identifies serious bugs in the target computer system and causes the target system to crash by sending an input that takes advantage of bugs. These bugs may lead to system crash or severely destabilize the system to an extent that it becomes unable to be accessed or used by other users.

Although DoS attacks do not cause loss or theft of confidential data, it can cost the victim a great deal of time and money.



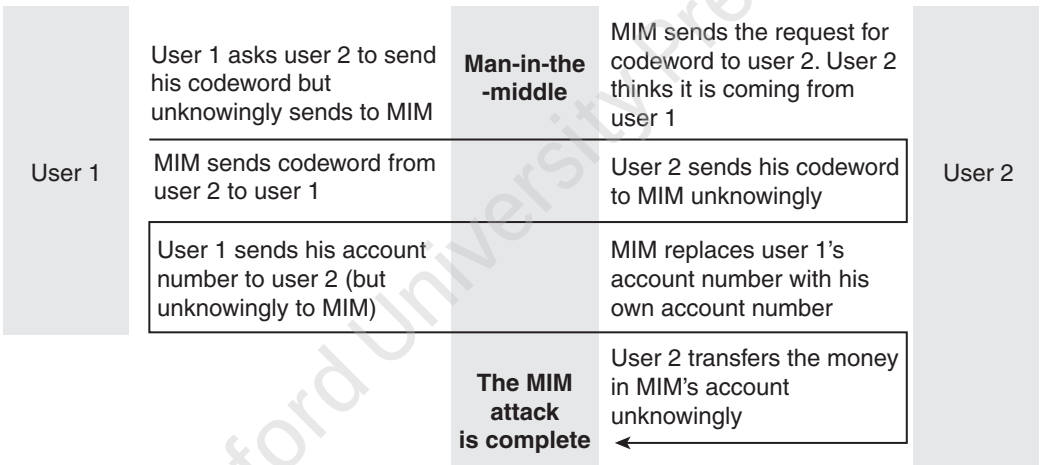


Figure 7.3 MIM attack

7.2.6 Man-in-the-middle Attack

In a man-in-the-middle (MIM) attack or network spoofing attack, the attacker intentionally inserts himself into a conversation between two persons. Besides deliberately getting in between the persons, the attacker impersonates the people in the conversation (acts as proxy to persons) and gains access to the information that they were sending to each other.

Figure 7.3 shows how an attacker intercepts, sends, and receives data which is meant for someone else. MIM attacks are commonly made for financial gains.

How to Prevent Man-in-the-middle Attacks

The following are the ways to prevent MIM attacks:

- Implement packet filters to inspect packets that are exchanged over the network. Such filters can block packets coming from suspicious IP addresses.
- Avoid trust relationships because such relationships only use IP addresses for authentication. The attacker can run spoofing attacks very easily.

- Implement spoofing detection software.
- Use cryptographic network protocols like using HTTPS rather than HTTP. Such protocols send encrypted data and, while receiving, authenticates the data. Other such protocols are transport layer security (TLS) and secure shell (SSH).

7.2.7 Internet Fraud

The downside of using Internet services include stealing personal information, conducting fraudulent transactions, or transmitting the proceeds of fraud to financial institutions. Such frauds can occur in chat rooms, emails, message boards, or on websites. Some common Internet frauds are discussed here:

- *Purchase fraud* occurs when a criminal purchases a product or service online and pays for it through fraudulent means; for example, using a stolen or a fake credit card. As a result, merchants do not get paid for the transaction and lose money as a result.
- *Online auction fraud* occurs when a fraudster starts an online auction of high-priced items on a website. He accepts payment from the auction winner, but either does not deliver the product or delivers a product that is less valuable than the one offered.
- *Work from home scam* occurs when the scammer accepts services from victims (such as writing directories, data entry, and reading books) but refuses to reimburse them by rejecting their work considering it sub-standard.
- *Phishing* is done to acquire sensitive information such as passwords, account numbers, and credit card details. In this technique, the fraudster constructs a fake website that looks similar to the legitimate site and asks for the user's personal information to steal his information and misuse it.
- *Stock market fraud* includes attempts to manipulate prices of securities on the market for the personal profit of the scammer. For example, the scammer spreads false information to cause a dramatic increase in price of thinly traded stocks and the moment prices reach the desired level, the scammer sells his stocks to innocent victims, thereby making a substantial profit.
- *Online intellectual property theft* is also common these days. Individuals all over the world who share their notes and information on the Internet have exclusive rights on their material. However, many people or students just copy and use it without taking permissions from the author.
- *Spam emails* is a common form of fraud in which the fraudster sends bulk emails to millions of email addresses to corrupt the receivers' computers, steal their identity, or fool them to pay for fraudulent products or services. These emails offer false dealings to recipients such as low-interest loans, winning lotteries, fancy business proposals, free credit report checks, and relationships with local singles. Spam emails require recipients to open the email and click on a link which may also open up the computer to a virus, worm, or other bug that will corrupt the computer.

7.3 PREVENTIVE MEASURES

As there is a rise in the number of people using the Internet for their businesses, entertainment, and socializing, the concern for privacy on the Internet is constantly growing.

Given here are some measures which the users can take to preserve their privacy in the public domain:

- To avoid cases of non-delivery of products or services or delivery of inferior products, buy only from trusted and reputed websites. Before doing any transaction, users should also read other user's feedback and comments on the products sold.
- Emails saying 'You have won money…' should be ignored. If it were true, then users will never get such emails through Yahoo or Gmail. They will be sent through the official email of that organization.
- Sometimes, we get spam emails from a friend claiming to have been mugged while on vacation overseas and asking for money. Ignore such emails because that friend's email account may have been hijacked. In such cases, confirm such types of request for money through phone or any other way of communication.
- Install anti-spyware, antivirus, anti-scamware, and anti-malware software on your computer and update them regularly. Most software are now available for free on the Internet. They are basically used to detect and eliminate attacks of malware.
- Do not click on links given in emails received from unknown senders.
- Review your monthly credit card statements to ensure that they are accurate. In case of any discrepancy or doubt, immediately contact the issuer of the credit card.
- If there is a spam mail asking for bank details, do not reply immediately; rather, call the bank to confirm the request. Make sure you do not call on any phone number included in the email as they can be fake.
- Do not use an obsolete operating system.
- Increase the browser's security settings.
- Use a pop-up blocker software to avoid pop-ups. Do not click on pop-up alerts, not even on the cross to delete the pop-up alert because this may result in getting more pop-ups. A better option in this case is to close the browser application.
- Use strong passwords so that it is not easy for the hacker to guess it. Never select an obvious password like your name, names of family members, date of birth, or simple sequences like abcdef or 123456. A good password should have at least six to eight characters that are a good mix of uppercase letters (e.g., A, B, C), lower case letters (e.g., a, b, c), numbers (e.g., 1, 2, 3), and punctuation symbols (e.g., ~!@#$%^&*()+−=). Moreover, passwords should be changed frequently and must not be shared with friends and family members.
- Do not reveal too much private details on the Internet, especially on the social networking sites. If it is necessary to disclose them, then ensure that the website is secured. The address of a secured site begins with https:// where 's' signifies secure. Remember that once an information is posted on the Internet, it is difficult to take it back because even after deleting it, the copy of the information can still be available with other websites or search engines.
- When accessing the Internet, do not forget to delete cookies, temporary files, or history of web pages browsed.
- When accessing the Internet over a wireless network, take for granted that the network is not secure even if its access is protected through passwords. In order to ensure that the devices do not get unknowingly connected to such networks, set devices to 'ask' before joining networks.

- To go to a website, type its address in the address bar. Do not click on any link or cut and paste its address from unsolicited emails or web pages. Remember that links that look legitimate and genuine may be actually bogus, specifically designed to steal private information.
- Do not forget to sign out from email, Facebook, or other accounts after using them.
- Most organizations ensure confidentiality by encrypting their messages or files before transmitting them over the Internet.
- Organizations also install firewalls to ensure data privacy.
- Before opening any attachment, scan it for malware using an antivirus program or email scanner.
- Update the operating system as well as the antivirus program on a regular basis.
- Scan the computer using an antivirus program regularly.
- Not all Trojan horses can be detected by antivirus software, so it is always better to install anti-Trojan software such as TrojanHunter and The Cleaner.

7.4 WORKING OF ANTIVIRUS SOFTWARE

An antivirus is a software that prevents, detects, and removes malicious software programs such as virus, worms, Trojan horses, spywares, and adwares that are harmful for the computer systems. It shields computers from most digital threats at the cost of negligible impact on the system's performance. Nowadays, many types of antivirus software are available in the market, which implement different strategies to perform the intended task. However, two main techniques to prevent, detect, and remove such malicious code from the computer are shown in Figure 7.4. These are explained here.

Signature-based approach In this technique, the antivirus software searches for matches in a virus dictionary (a file which contains a list of viruses that are identified by the antivirus software). While examining a file for presence of virus, if a piece of code matches any code in the virus dictionary, then the antivirus software may take any one of the following actions:

- Delete the file.
- Quarantine the file so that it is inaccessible to other programs. This will prevent the virus from spreading. Quarantine is like a sealed glass jar that disallows anything to enter or escape but the user can just look inside to see if it is a virus or not.
- Remove the virus from the file.

Signature or dictionary-based antivirus software examines files when a file is created, opened, closed, or attached with an email. Besides this, users can also schedule a complete hard disk scan to examine all the files for detecting any kind of virus.

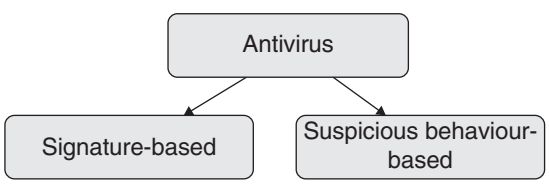


Figure 7.4 Types of antivirus

Although this approach has been very effective in detecting and removing viruses from files, virus authors always keep themselves a step ahead by encrypting parts of the virus code so that they are not detected by signature-based technique.

Suspicious behaviour or heuristic-based approach In this technique, the antivirus monitors the behaviour of all programs. In case a program tries to write

Antivirus software must be updated regularly, so that the virus dictionary can incorporate the definition of the recently identified viruses.

to an executable program, it is flagged as suspicious behaviour and the user is informed about it and asked for his permission to allow or disallow the write operation.

Unlike the previous technique, the suspicious behaviour approach protects the computer from brand-new viruses that have not yet been incorporated in the virus dictionary. The heuristic approach works as a doctor who examines a person's behaviour before diagnosing and curing him.

However, the drawback of this approach is that it may report a large number of write operations and after a certain period, users start ignoring such warning messages. If the user starts clicking 'Accept' on every such warning, then the utility of the antivirus software dwindles. Therefore, this technique is not used widely.

Most antivirus software use a hybrid approach that is a combination of the signature-based and heuristic-based techniques.

Miscellaneous techniques Some types of antivirus software emulate the beginning of the code of each executable that is being executed. The antivirus software then checks if the program is trying to modify the executable file or if it is immediately searching for other executable files, then it may be a virus and control is not transferred to the program. This check is made before transferring control to the executable file. However, it may also report false scenarios.

Some antivirus use a sandbox approach which emulates the operating system and runs the executable programs in the simulated environment. Once the program execution is completed, the sandbox examines the changes made by it to know if it was a virus. Though this technique is effective for performance issues, this type of detection is performed only during on-demand scans.

Some types of antivirus software work in the interactive mode. In this mode, the antivirus software works in the background and monitors the computer's activity. It checks for any virus getting downloaded from the Internet or from a removable storage device.

If you have more than one antivirus software installed in your computer, then make sure that only one of them works in the interactive mode because if both work in interactive mode, it will slow down the computer.

Avoid using web-based antivirus scans as most of them are either spyware or Trojan horses.

7.5 FIREWALLS

You must have heard people saying, 'We cannot access Facebook in our office.' How is it possible that a website available all over world cannot be accessed in a particular location? The answer to this question is the presence of firewall. A firewall that may be a piece of

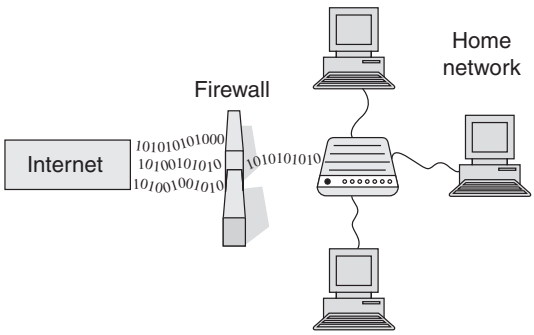


Figure 7.5 Firewall

hardware, software, or both is installed to prevent unauthorized access to computers or networks. It exercises full control over data packets coming in and going out of the computer to the Internet. All data traffic passes through the firewall as shown in Figure 7.5.

The firewalls are configured with a set of rules that decide the packets to be accepted that will be transmitted or received across the network. Although firewalls are already programmed with a sensible set of rules by the manufacturing company, users can also configure them. Basically, a firewall is designed to act as a barrier to keep destructive or unwanted forces away from your property.

Firewalls have become so important today that every operating system including Windows, Mac, Linux, etc. offer built-in support for maintaining and testing firewalls on the computer and the firewall is turned on by default. Besides the built-in support, users can also use third-party firewalls to protect their computers. Some examples of third-party tools are Zone Alarm, Norton Personal Firewall, Tiny, Black Ice Protection, McAfee Personal Firewall, and Trend Micro PC-cillin. Many of these tools either offer a free or a trial version of their commercial versions.

Firewall helps to screen out hackers and malicious software that tries to reach a computer.

7.5.1 Types of Firewalls

The different types of firewalls are explained in this section.

Packet filtering This technique examines each data packet that either enters or leaves the network. Based on the result of examination, it accepts or rejects the packet depending on user-defined rules. Packet filters work mainly on the first three layers of the OSI model. Although packet filtering is a fast, efficient, and effective technique, it is difficult to configure and is susceptible to spoofing. Moreover, packet filter firewalls cannot tell whether a packet is part of an existing data exchange or a new one. This is because each packet is treated in isolation.

Stateful firewalls Stateful firewall overcomes the drawback of packet filters by recording all connections passing through it. This gives enough information to determine whether a packet is the start of a new connection, an existing connection, or not a part of any connection. When the state of the packet is known, the firewall can speed up packet processing by allowing a packet of an existing connection without further analysis and evaluating only those packets (based on rules) that are coming through a new connection.

Circuit-level gateway implementation In this type of firewall, security mechanisms are implemented only when a TCP or UDP connection is established. Once the connection is established, packets can flow between the hosts without further checking.

A proxy service must be implemented for each type of Internet application the firewall will support. For example, there is an HTTP proxy for web services.

Proxy firewalls Proxy firewalls act as an intermediary for requests from one network to another to disallow any direct connections between either sides of the firewall. This enables the proxy firewall to block or allow traffic based on its rule set. A proxy service must be run for each type of Internet application the firewall will support, like an HTTP proxy for web services.

Application-layer firewalls With increasing attacks against web servers, a firewall is required to protect servers and the applications running on them. For this, application firewalls are implemented that inspect and filter packets on any OSI layer (up to the application layer). Such a firewall can block specific content (such as malware or certain websites) and report when applications and protocols (such as HTTP, FTP, and DNS) are misused.

However, practically speaking, most firewalls use more than one technique to implement security mechanisms.

7.5.2 Firewall Rules

Firewalls can be configured based on user-defined rules. These rules can be based on the following features.

IP addresses Block data coming from or going to a certain IP address or a range of IP addresses.

Domain names Allow or disallow data from certain specific domain names or domain name extensions such as .edu or .mil.

Protocols Allow or disallow data that uses protocols such as IP, SMTP, FTP, UDP, ICMP, and Telnet.

Keywords Allow or disallow data flow that contains certain keywords or phrases. This is done to block offensive or unwanted data from flowing in.

7.6 CONCEPT OF ENCRYPTION AND DECRYPTION

Encryption (Figure 7.6) is the process of converting data into a cipher text (random data which is meaningless). Here, cipher text means scrambled data, which cannot be easily understood by anyone except authorized parties. For example, if I want to send a message HELLO to my friend and I do not want anyone else to read my message, then I can encrypt this message and send the encrypted text across the network. The corresponding cipher text for HELLO could be KHOOR. KHOOR is not understood by anyone.

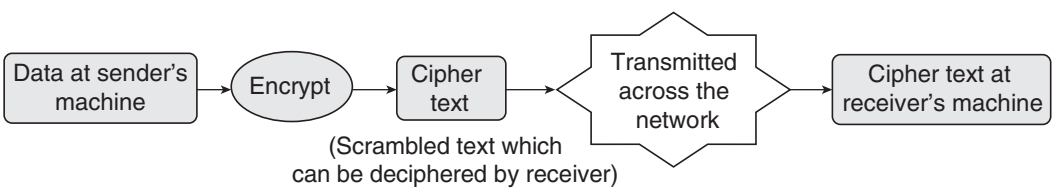


Figure 7.6 Data encryption

Advantage Encryption is done to protect the confidentiality of digital data that is either stored on the computer or is transferred across the network. Many companies store encrypted data in their database to ensure that even if an attacker gets illegal access to the confidential data, then at least he is not able to understand it.

Nowadays, many encryption algorithms are used; besides providing confidentiality, a sound encryption algorithm has the following features:

- Authentication to verify the originator of the message.
- Integrity to ensure that the message has not been modified or tampered during transmission.
- Non-repudiation to make sure that the sender cannot deny sending the message.

Decryption is the reverse of encryption. It is the process of converting encrypted data back into its original form so that receiver can correctly interpret its meaning. Until decrypted, the cipher text appears as garbage. To protect data from being decrypted by just anybody on the network, only those users who have the decryption key (3 in our example) can decrypt the data and make it useful. For example, only the intended receiver knows that while encrypting the data, the third character (in the forward direction) was replaced by the original character. Therefore, to decrypt the message the third character (in the backward direction) is written.

If the decryption key is not known, even then the attacker may decrypt the message by applying several decryption algorithms.

7.7 SYMMETRIC AND ASYMMETRIC ENCRYPTION

Encryption is done using two main techniques (Figure 7.7)—symmetric (also known as secret-key, single-key, shared-key, one-key, or private-key) encryption and asymmetric (public key) encryption.

7.7.1 Symmetric Encryption

This type of encryption is basically done on small amount of data. It uses a symmetric key which is applied on plain text (data) to convert it into cipher text. Similarly, during decryption, the symmetric key is applied to convert the cipher text into original data.

Strength A good symmetric encryption algorithm is one that makes it very difficult, if not impossible, for attackers to decrypt the generated cipher text without knowing the key used for encryption.

Requirements The following are the requirements of systematic encryption:

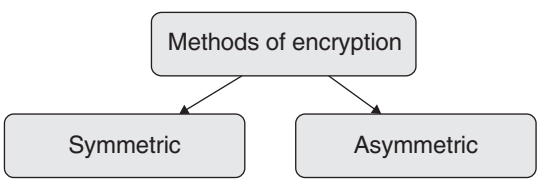


Figure 7.7 Encryption methods

- The longer the key, the more difficult it will be to decrypt the message. Most symmetric encryption algorithms use a key of 64 bits, 128 bits, 256 bits, and even 512 bits.
- It is always better to use an encryption algorithm that has been used for several years and has successfully resisted all attacks.

- The secret key can be a number, a word, or just a string of random letters. For example, 'hello' can be encrypted as 'hzexlqlhog' by inserting a character randomly between any two characters in the original message.
- Both the sender and the receiver know about the secret key.
- The secret key must be changed on a regular basis.

Drawbacks The following are the drawbacks of systematic encryption:

- While exchanging the secret key with the receiver across the network, it may get into the hands of an attacker. Once the key is known to him, he can decrypt all the messages very easily, thereby defeating the whole idea of ensuring data confidentiality.
- There is no provision for authenticating the sender. There is no way for the receiver to know whether the message has been sent by the intended sender.
- Data integrity cannot be assured—whether the received message is the one that was sent.

7.7.2 Asymmetric Encryption

Asymmetric encryption algorithm overcomes the limitations of symmetric encryption algorithm by using a pair of keys. The two keys in asymmetric encryption are related to each other in such a way that a message encrypted by one key can be decrypted only by the second key.

The two keys are known as public key and private key. While the public key is given to anyone who wants to send a message, the private key on the other hand is kept secret and is known only to its owner.

Technique A message (which may include a small text or a file) can be encrypted by using the public key. Similarly, any message encrypted by using the public key can be decrypted only by applying the equivalent private key on the cipher text. This process is shown in Figure 7.8.

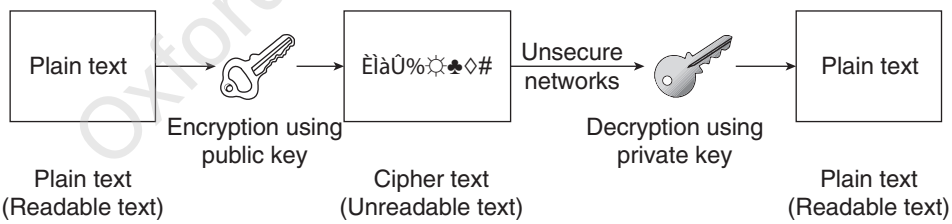


Figure 7.8 Asymmetric encryption

Public and private keys are allotted by a certificate authority.

As per Figure 7.8, the sender uses the receiver's public key to encrypt the message. The encrypted text then travels across the network. The receiver decrypts the cipher text with his private key to read the confidential message.

Example If my public key is P1 and my private key is P2, then the key P1 is known to everyone who wants to exchange data with me. Only I know my private key P2. A user X who wants to send me a confidential data will encrypt the data using P1. The data encrypted by P1 can be transformed into original text only by applying P2. This ensures that the message intended to be read by me is actually read only by me.

Key features The key features of asymmetric encryption are as follows:

- The two keys are mathematically related to each other.
- The algorithm used for encryption is universally known.
- It is impossible to compute the private key if the public key is known.

Table 7.1 differentiates between symmetric and asymmetric encryption techniques.

Table 7.1 Differences between symmetric and asymmetric encryption

Symmetric encryption	Asymmetric encryption
A single secret key is used.	A pair of keys is used.
Secret key is known to sender and receiver.	Public key is known but private key is kept secret.
It is used by the Digital Encryption Standard.	It is used by Pretty Good Privacy.
It is computationally faster.	It is slower than symmetric encryption.
It is less complicated.	It is more complex.
Secret key is shared.	Public key is available to everyone; private key is kept secret; and no key is shared.

7.8 DIGITAL SIGNATURE, DIGITAL CERTIFICATE, AND DIGITAL ENVELOPE

The concept of public key encryption or asymmetric encryption can be extended further to authenticate the sender. The sender can sign his message by encrypting it with his private key. This message can now be decrypted only by applying his public key (refer to Figure 7.9).

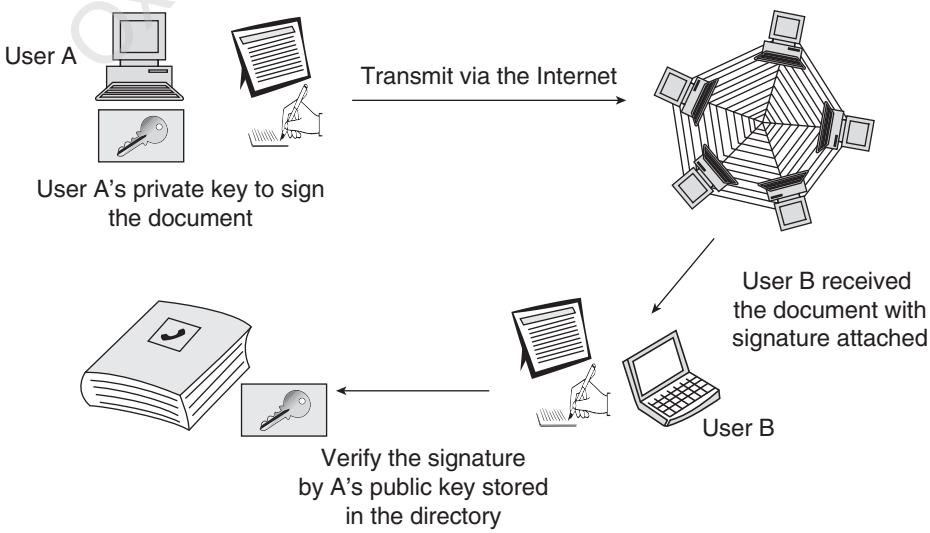


Figure 7.9 Digital signature

Since public and private keys are related to each other, the process proves that if the message is decrypted by X's pubic key, then it was encrypted only by X's private key.

Therefore, we see that digital signature is an equivalent of hand-written signatures. In many countries, digital signatures have the same legal significance as that of documents with handwritten signatures.

A digital signature can be used with encrypted as well as ordinary (plain) messages.

Uses

The uses of digital signature are as follows:

- It ensures the sender's identity.
- It makes it difficult for the sender to deny the transaction (non-repudiation).

Digital Envelope

Whenever you get a letter through registered post, before opening the letter, you need to sign after receiving it to notify the sender that it was received. The same level of security can be applied to digital messages as well. The sender can create a digital envelope using the following steps:

- Encrypt the message with a symmetric key.
- Encrypt the symmetric key with the public key of the receiver.

When the receiver receives this digital envelope, the same steps are performed in the reverse order:

- The receiver uses his private key to decode the symmetric key.
- The symmetric key is applied to decode the message.

Digital Certificate

By applying digital signature, the sender assures that the document was sent by him. However, it does not prove whether he is the person from whom the message was expected or not. For example, you know that Mr X will come to repair your computer. Now, if someone comes to your house and says that he is Mr X and has come to repair the computer, how will you know that he is actually Mr X and not a fraud? Of course, you will check his identity card issued by the organization in which he works or his licence, PAN card, voter card, etc. issued by the government.

The same situation exists in the digital world too. If you have received a digital document from a person or an entity, you need to assure yourself that the message is coming from the legitimate sender (as private key can also be stolen so anyone else can send a message using the legitimate user's identity). The solution to this problem is a digital certificate.

A digital certificate is an electronic document that certifies that the holder of the certificate (person or organization) is trusted by an independent source called the certificate authority. The certificate is issued after verifying the credentials of the entity.

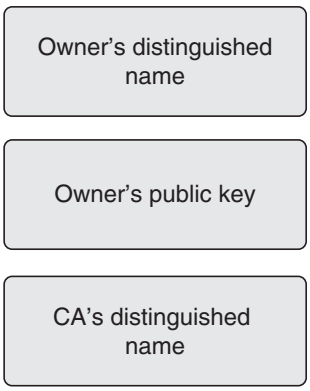


Figure 7.10 Digital certificate

A digital certificate (Figure 7.10) contains the following information:

- It has the digital signature of the certificate-issuing authority.
- It has the public key of the owner of the certificate.
- It has the owner's identity.

Uses

The uses of digital signature are as follows:

- It verifies that a public key belongs to a particular person or entity.
- Most email applications use digital signatures and digital certificates to sign any outgoing emails and validate digitally signed incoming messages.

The certificate authority issues, distributes, and revokes digital certificates.

Summary

- As the Internet is an insecure channel for exchanging private data or messages and intrusion or frauds like phishing are very common, some methods must be implemented to protect the data.
- Internet security ensures authenticated access of data that is exchanged over the Internet.
- Authorized or unauthorized users may modify the existing data, add wrong data, or delete some important data.
- The most common threats to data security comes either from use of malwares or through fraud like phishing.
- A worm, once installed, can connect to a remote computer over the Internet to download a more substantial piece of malicious software.
- Users must always use the latest operating system and antivirus software.
- In browser hijacking, the attacker modifies the browser to permanently change the home page.
- In a man-in-the-middle (MIM) attack or network spoofing attack, the attacker intentionally inserts himself into a conversation between two persons.
- A good symmetric encryption algorithm is one that makes it very difficult, if not impossible, for attackers to decrypt the generated cipher text without knowing the key used for encryption.

Glossary

Antivirus A software that prevents, detects, and removes malicious software programs such as virus, worms, Trojan horses, spywares, adwares, and so on that are harmful to computer systems

Cookie Small-sized files that store information about an Internet user on her own computer

Cracker A person who breaks into the system by password cracking or by cracking the security measures implemented to protect the data

Decryption The process of converting encrypted data back into its original form so that the receiver can correctly interpret its meaning

Denial of service An attempt to make a computer resource unavailable to its intended users

Digital certificate An electronic document that certifies that the holder of the certificate is trusted by the certificate authority

Domain hijacking The process of making the victim's computer to communicate with the wrong server

Domain name server A system used to translate word-based addresses of websites like www.abc.com into its equivalent numerical (IP) address. All computers on the Internet are allotted a numerical address like 3.7.14.19.

Encryption The process of converting data into a cipher text

File allocation table A table maintained by the operating system to store information about location, size, and other details about files on the disk

Firewall A piece or hardware, software, or both that is installed to prevent unauthorized access to computers or networks

Hacker A person who either breaks into the system for which they have no authorization or goes beyond their limits of legitimate access

Keyword The words that the user types in the search box of a search engine

Malware Software designed with wrong intentions, usually embedded within legitimate software that is either useful or attractive

Online intellectual property theft The process of copying and using someone else's online material

Spamming The process of flooding the Internet with many copies of the same message for commercial advertising, usually for dubious products like get-rich schemes or loan at low interest rates

Spyware A malicious program that surreptitiously monitors activity on a computer and reports that information to others without the user's consent

Trojan horse A non-self-replicating malicious software that pretends to be harmless so that users can easily download it on the computer

Virus A small program that gets loaded in the computer without the user's knowledge and replicates itself repeatedly

Virus dictionary A file which contains a list of viruses that are identified by the antivirus software

Exercises

Group A [2 marks each]

1. What is a virus? [C.U. 2012]
2. What is a firewall? [C.U. 2012]
3. What is an anti-virus? [C.U. 2013]
4. How can confidential data be protected?
5. What is digital signature? [C.U. 2013]
6. What do you mean by spyware?
7. Discuss any two features of a computer virus.
8. What do you mean by malwares?
9. What do you understand by a digital certificate?
10. What do you mean by spam emails?
11. Discuss any two ways of selecting passwords.
12. What do you understand by man-in-the-middle (MIM) attack?

Group B [4 marks each]

1. Write short notes on (i) Asymmetric encryption, (ii) Worm, (iii) Trojan, and (iv) Adware.
2. How can security of data be compromised?

3. Discuss the concepts of data encryption and decryption. [C.U. 2012]
4. Discuss the different types of firewall.
5. Point out the difference between symmetric and asymmetric encryptions.

Group C [8 marks each]

1. Discuss the different types of viruses.
2. How does a worm work?
3. Discuss the different types of Trojan horse.
4. Discuss the different types of network attacks.
5. How does an antivirus software work?
6. Discuss the different firewall rules.