CHAPTER 6 Security, Copyright and The Law

Overview

Security is a system of safeguards designed to protect a computer system and data from intentional and accidental damage or access by unauthorized persons.

How does a computer system detect whether you are the person who should be allowed access to it? Various means have been devised to give access to authorized people. For this, we have four approaches, as discussed below:

- **What you have:** *You may have a key, badge, token, or plastic card to give you physical access to the locked-up server room or computer building.*
- **What you know:** *Standard user-ids and passwords or some special combination of numbers are given to the users to logon the machine.*
- **What you do:** *Normally, the users put their* ***signatures*** *on the documents to confirm their legitimacy as an authorized user.*
- **What you are:** *Some security measures are* ***biometrics*** *- biological means of identification i.e. fingerprints, voice recognition, eye retina etc.*

6.1 Virus and Antivirus issues:

To fully understand the concept of a virus (or worm), first recall the concept of a computer program, what can a program do, and how a program is executed? A program is a sequence of instructions given to a computer. These instructions are for some sort of processing. By processing we mean performing arithmetic and logical operations on the data in the computer memory, manipulating data is storing and arranging two data item to see if they are equal or not, and transmitting data is sending data from one computer to some other computer on a network or via internet. A **virus** is a program that attaches itself with other executable files by modifying them so that the virus program is also loaded and executed with the execution of these programs. A virus usually

Note :
(i) Some systems use a combination of the above mentioned techniques for individual's identification.
(ii) Loss of hardware is not a major problem in itself; it can be recovered by insurance, and the hardware can be replaced. The loss of software is also not a big issue, as if it has been backed up properly, can be re-installed in case of loss. The actual problem lies in the loss of data. It is difficult (though not impossible) to recover it in time in case of transactions based computer systems.

performs destructive operation by deleting or modifying (unknowingly) data stored on the storage devices attached to the computer. It is very important to note that a virus is a set of instructions so it cannot physically destroy a hardware (a common misconception).

We can formally describe a virus as "A destructive program containing code that can generate copies of itself and attaches itself with other program so that it is automatically executed when those programs are executed".

It is important to know exactly how a virus reaches from one computer to another. As the virus attaches itself with files present on a system so the only way, a virus can reach from one computer to another, is when some data is exchanges between these computers either through usb, disks, or the network.

6.1.1 Causes of Viruses

Following are the means through which a virus reaches from one computer to another.

- **Email:** Now a days, most of the virus programs spread by attaching themselves with email messages. When a user opens such an infected message, the virus is also loaded into the computers memory and attaches copies of itself with many files. Then this virus gets itself attached with email message sent from the infected computer and infects other computers.
- **Networks:** Another way of spreading virus is by using Internet and other networks. For example when you download some executable file or data from the Internet or from a shared disk on the Network, the infected files may be attached with the downloaded data that ultimately infects the computer.
- **Removable storage media:** One important means of exchanging data is through the use of removable media like memory cards CDs and flash devices. So, when you copy the data from one computer to another by using a removable media, the infected files may get transferred.
- **Pirated Software:** Another important but not so common way the virus infects your computer is through the use of pirated software. Some companies may intentionally put some virus program into their software. This program will only activate when it does not find some special files like license files on your computer.

6.1.2 Types of Virus

Following are some important types of viruses:

- **Boot sector virus:** We know that the disk is divided into tracks and sectors. The disk on which the operating system has been loaded, has a special program in its first sector called the boot sector. When the computer is turned on, the program in the boot sector is automatically loaded into the memory. This program then loads the operating system into the memory after performing some initial tasks. The boot sector virus modifies the program in the boot sector and is loaded into memory whenever computer is turned on. The virus is attached with the executable files i.e. **.exe, .com** an **.dll** files. When the user uses these executable files, the virus attached with these files is also activated and then it infects other files and also performs destructive commands and destroys the data files also.
- **Chernobal Virus :** The famous **chernobal** virus deletes all the Microsoft office files and also the partition information form the disk hence causing a major loss of data.
- **Logic bomb:** Logic bomb, differ from other viruses in that they are set to go off at a certain date and time. A disgruntled programmer, for a defense contractor created a bomb in a program that was supposed to go off two months after he left. Designed to erase in inventory tracking system, the bomb was discovered only by chance.
- **Trojan horse:** the Trojan horse covertly places illegal, destructive instructions in the middle of a legitimate program, such as a computer game. Once you run the program, the Trojan horse goes to work, doing its damage while you are blissfully unaware. An example of a Trojan horse is FormatC.
- **Redlof:** The Redlof virus is a polymorphic virus, written in Visual Basic Script. The virus relies on the Microsoft ActiveX Component vulnerability to automatically execute itself. When executed the virus locates Folders.htt and infects that file, the Folder.htt is part of Microsoft Windows Active Desktop feature. It searches the users hard-drive and locates infectable files and appends itself to them.
- Some viruses may make unnoticeable changes hence corrupting the data being used and some viruses may even make data unusable.
- A virus program may detect some special information like passwords, or any sensitive data and send it to some other user on a network. For

example a virus program may read the Pin code or credit card number entered by a user and then send this information to another user.

- Another interesting thing a virus can do is that it may make resources unavailable to the users. For example, a virus after copying itself on all computers on a network will start sending data on the network so that other users cannot use the network.

6.1.3 How to safeguard against viruses?

Following are the few ways following which you can save your computers from getting infected by a virus. Never open unknown email messages, and also scan (for virus) all email messages even if you know the sender of the message. You should also minimize the data transfer between computers through the use of floppy disks and other removable media. While using the Internet, do not download free-ware programs without first checking it for virus. Always use a virus detecting software i.e. Norton, McAfee, Dr. Solomon's, toolkit or IBM's antivirus programs to detect and to delete the infected programs from your system. You should periodically update these programs as more and more viruses are discovered over the time, so older versions of these programs may not detect the new viruses. Another important way to save yourself from the destruction of virus attack is that you should always keep backup of your data. The backup will be useful if a virus attack deletes your data or modifies it.

6.2 DATA SECURITY

The organization obtaining the data is responsible for the security of data and will be liable to prosecution for the lapses in the security of data and updating it improperly.

You can use Internet to connect to a network in any part of the world and see any data on that network. Today many organizations heavily depend upon fast computer processing and if some one enters into their network and make it unavailable, the working of the entire organization will halt. Many organization store data of their customers online for providing fast services. For example a credit card company may put data of its customers online. A bank providing online services will be using online data storage for the records. A university may provide the facility of viewing results online. People take online exams like GRE, GAT etc. As it is clear from the above examples, some really sensitive data is available online. All these advances in data manipulation have given birth to a new issue known as **Data Security.** If some unauthorized user views or obtains this data, the whole organization may suffer irrepairable losses ultimately.

It is obvious from the above discussion that the security of data is necessary for the existence of many organizations and for all kinds of online services. To understand the process of making the data secure, let us first see in what ways the data can be misused if not secured properly. In recent years, the computer technology has become available to everybody at a very cheap cost. Also specialized software packages are producing all kinds of solution at a very low price. The result of all the advancement in the technology and its affordability has made it possible to use computers in all fields of life. For example computers are being used to monitor weather conditions, to monitor defense projects in controlling sensitive process like controlling atomic reactors etc. Business people are using computers for performing calculation, keeping records of employees, recording of customers transactions and provide them better services throughout the country or world. Hospitals are keeping patient records, sorted and updated by using different criteria. Schools and universities are keeping all records of students, examinations, accounts, libraries etc on a computer to provide instantaneous access of data to administrators and the students. You name any field of life and computers are there to be used, to efficiently process data accordingly.

Internet has connected millions of computers and people together and it has made possible the e-commerce, m-commerce etc. Now you can purchase books, clothes, and all kinds of stuff online, by using credit cards. In today's world, online markets are available for all kind of shopping like software, hardware, electronics, medical equipment etc.

In today's world, many networks are connected together and are sharing all kinds of information amongst the users, using email, SMS and other programs for instantaneous communication across the world.

6.2.1 Security Violations

Following are some of the ways in which the security of data may be violated.

- Someone may break into the computer room and take away all storage devices housing sensitive data.
- Unauthorized users may take access to personal data of someone and then use it to gain some advantage. For example if someone gets access to your credit card number then he can use it to do online shopping from your account.
- An unauthorized user may use an online mail server, like mail.yahoo.com to view email message of other users hence causing privacy issues.
- Someone can send a virus onto a network causing the network to become very slow or even unusable.

- Some users may gain unauthorized access to bank accounts and transfer a large amount of money from other accounts to his personal account.
- A person may make a computer so busy by sending many requests so that the computer becomes unavailable to authorized users. This is called denial of service situation.

6.2.2 Security Threats

Following are the main threats to Data Security:

- Some authorized user of the data may unintentionally delete or change sensitive data. There are two solutions to this problem. Firstly, the users must be assigned proper rights to minimize such events. Only the authorized users with certain rights may be allowed to delete or modify data after following a step-by-step process. Secondly, periodic backup of data should be taken to recover from this sort of situation.
- Another solution to these types of problems is that proper password protection should be used to use any resource. A log file should also be maintained to keep track of all the activities on the data/files.
- Some strong encryption algorithm should be used, so that if someone gets access to the data, he / she should not be able to make any sense out of it.
- The solution to infected data is that proper virus scanning software should be used to scan all data coming into the organization.
- Computers and all backing storage devices should be placed in locked rooms with only authorized access to these resources.
- Authorized users must be asked to change their passwords periodically. Very short and common passwords should be avoided.

6.2.3 Data Protection

As discussed in the beginning of this chapter, many organizations gathered data about their employees customers. Some of this data is needed for (purely) efficiently processing the business transactions. For example, a hospital having data about the disease history of patients. All the personal data kept by different organizations may by disclosed by the organization for some legal purposes. For example in the hospital case, the medical researches may use the patient personal data, like his medical history, or any other fields to draw some conclusions. But if the hospital management distributes that data somewhere else, then this may make the patient feel embarrassment e.g. in

case when the patient has some mental disorder or has a bad history. The data protection rules refer to such a case, it means that any personal data kept by some organization should never be disclosed to unauthorized persons / organization under any circumstances.

6.2.4 Privacy Issue

An individual has a right to see the data kept about him. For this, he has the right to submit an application to view that data any time.

He also has the right to stop the processing of his data by the organization. He also has a right to claim a compensation from the organization for any kind of disclosure of data disallowed by the law.

No worker of the organization is allowed to disclose or use the data kept by its organization and if he fails to abide by, he is committing a crime.

It is clear from this discussion that data protection act tries to minimize the misuse of personal information to provide a safeguard against such crime. Also an organization collecting data should collect only the data adequate necessary for its working and should not collect un-necessary data.

The following points should be considered to ensure the individual's privacy.

- The organization is responsible for keeping the data updated.
- The organization should keep data for the specified period of time only and can not keep it longer than necessary.
- At no point during the processing of data, the rights of the subject should be violated.
- The organization is responsible for all kinds of security of data.

6.3 Data Protection Legislation and Copyright Issues

The data legislation is being improved with the time and may include many more laws for the protection of data in future but the underlying basic principle (legislation) are same for all new laws.

6.3.1 Legislation

The data protection legislation defines the laws that ensure data protection. Many countries have defined the data protection legislation and in some advanced western countries; this law is enforced properly as well. The data protection legislation of different countries is based on same basic principles. In this section, we will discuss these basic principles so that you can get some idea of why data protection act is needed. The detailed Data Protection Acts will not be given here as it is beyond the scope of this course.

The principles of Data Protection Acts are as follows:

- The purpose of keeping and distrusting personal data must be clearly defined by organization obtaining that data.
- The individual about whom data is kept, must be informed about the identity of the organization / individual. The processing is necessary to fulfill of the contract between two parties. The processing is required by law or is necessary to carry out interest of the individual.

6.4 Important Privacy Acts

Note: In this regard Acts may also be consulted.

The **1980 Privacy Protection Act**, which prohibits agents of federal government from making unannounced, searches of press office if no one there is suspected of a crime.

The **1984 Cable Communications Policy Act**, which restricts cable companies in the collection and sharing of information about their customers. It was the first piece of legislation to regulate the use of information, which is processed on computer. The "Data Protection Act 1984" is intended to protect the individual from unauthorized use and disclosure of personal information held on a computer system. It consists of the following eight principles:

- The information to be contained in personal data shall be obtained and the data shall be processed, fairly and lawfully.
- Personal data shall be held only for one or more specified and lawful purposes.
- Personal data held for any purpose shall not be used or disclosed in any manner incompatible with that purpose or those purposes.
- Personal data held for any purpose shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- An individual shall be entitled, at reasonable intervals and without undue delay or expense, to be informed by any data user whether he holds personal data of which that individual is the subject, to have access to any such data, and where appropriate, to have such data corrected or erased.
- Appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure, accidental loss, or destruction of personal data

The **1987 Computer Security Act**, which makes actions that affect the computer security files and telecommunication illegal.

The **1988 Video Privacy Protection Act 1988,** which prevents retailers from disclosing a person's video rental records without a court order; privacy supporters want the same rule for medical and insurance files. Another step in that direction is the Computer **Matching and Privacy Protection Act of 1988,** which prevents the government from comparing certain records in an attempt to find a match. However, most comparisons are still unregulated.

The **Computer Misuse Act 1990** to make provision for securing computer material against unauthorized access or modification; and for connected purposes. The **Computer Misuse Act 1990** was passed to deal with the problem of hacking of computer systems. In the early days of hacking the problem wasn't taken very seriously – it was seen as mischievous behaviour, rather than as something, which could cause serious loss or problems to companies, organizations and individuals. However, with developments in technology the issue has become more serious and hence legislation was introduced to recognize three key offences:

- Unauthorized access to computer material.
- Unauthorized access with intent to commit or facilitate commission of further offences.
- Unauthorized modification of computer material.

The **1998 Data Protection Act** came into force early in 1999 and covers how information about living identifiable persons is used. It is much broader in scope than the earlier 1984 act, but does contain some provision for a transitional period for compliance with the new requirements. The 1998 Act applies to:

- computerised personal data ;
- personal data held in structured manual files .

It applies to anything at all done to personal data ("processing"), including collection, use, disclosure, destruction and merely holding personal data.

6.5 The Copyright Act

The principal law governing software piracy is the "Copyright Act 1976". Some amendments were made in this in 1983 and now **software piracy** is believed to be a punishable crime involving huge amounts of penalties. It is justified because software is believed to be an "intellectual property" that has been developed and brought into market after a lot of effort and cost. So, its future financial interests must be made sure by the concerned legal authorities.

Exercise 6C

1. Fill in the blanks:

(i) Making illegal copies of copyrighted software is called_____

(ii) A special program that can detect and remove viruses from computer is called _____

(iii) Software that is available free for a limited period is called_____

(iv) When the virus starts to impact on data, it is known as_____

(v) IR stands for_____

(vi) _____ is a software used for data compression

(vii) The right to use the software on the computer is called _____

(viii) Software is a _____ of person who developed it.

2. Choose the correct option:

(i) A virus program is usually hidden in

(a) The operating system only

(b) An application program only

(c) The disk drive

(d) The operating system or application programs

(ii) Most computer crimes are committed by

(a) Hackers

(b) International spies

(c) Highly trained computer consultants

(d) Company insiders who have no extraordinary technical ingenuity

(iii) Types of software that can be freely distributed without violating copyright laws are called

(a) Shareware (b) Public domain

(c) Copy protected (d) a and b

(iv) Information is

(a) A marketable commodity

(b) Can be stolen while leaving the original behind

(c) Should be free, according to the original hacker ethic

(d) All of above

(v) A virus that replicates itself is called a

(a) Bug (b) Worm

(c) Vaccine (d) Bomb

(vi) Another name for free software

(a) Encrypted software (b) Copy protected software

(c) Public domain software (d) Shareware

(vii) Another name for anti virus is

(a) Vaccine (b) Worm

(c) Trojan horse (d) DES

(viii) Security protection for personal computers include

(a) Internal components (b) Locks and cables

(c) Software (d) All of these

(ix) A secret word or numbers to be typed in on a keyboard before any activity can take place are called

(a) Biometric data (b) Data encryption

(c) Password (d) Private word

(x) What is the most common computer crime of these listed below

(a) Extortion of bank funds (b) IRS database sabotage

(c) Putting people on junk mailing lists (d) Software piracy

3. Write T for true and F for false statements:

(i) Software error can result in data loss

(ii) Any person can change password

(iii) All viruses activate in exactly the same manner

(iv) A full backup means that once a week you can perform a complete backup

(v) IR stands for intellectual rights

(vi) A computer virus is a part of hardware

(vii) Passwords, auditor checks and separation of employee functions are data protection techniques

(viii) No one has ever been able to read encrypted messages without key

(ix) It is legitimate to make a copy of software for backup purpose

(x) The computer fraud and abuse act of 1984 defines software piracy as crime

4. What is computer virus?

5. Define the anti-virus software.

6. How viruses may damage computer system?

7. Define Data protection Piracy acts.

8. Describe the Legislation and Copyright Issues.

9. Define the types of viruses.

10. What is a password?

11. Write the names and define briefly the antivirus.

12. Describe the exemption of 1990 act.

Answers

1. (i) piracy (ii) anti-virus (iii) shareware
(iv) virus attack (v) input request (vi) winzip
(vii) licence (viii) property

2. (i) d (ii) c (iii) b (iv) d (v) b
(vi) c (vii) a (viii) d (ix) c (x) c

3. (i) T (ii) F (iii) F (iv) F (v) F
(vi) F (vii) T (viii) F (ix) T (x) T