CHAPTER 7

SECURITY COPYRIGHT & THE LAW

Q1. What is Security? Discuss its different approaches or How the security maintained on a computer?

SECURITY:

- It is a system of safeguards designed to protect a computer system and data from intentional and accidental damage or access by unauthorized persons.
- A computer system must be protected from unauthorized persons. Different methods have been planned to give access to authorized persons. For this purpose there are four approaches.
- **What you have:**

  You may have a key, token, or a card to give you physical access to the server room or computer building.
- **What you know:**

  IDs and Passwords are given to users to access the computers.
- **What you do:**

  Authorized users put their signatures on the documents to confirm their authority.
- **What you are:**

  Some security measures are biometrics-biological means of identification e.g. fingerprints, voice recognition, eye retina etc.

Q2. What is a Virus? What are the causes of Virus?

VIRUS:

- A virus is a program that disturbs the normal execution of the programs.
- 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.
- Virus is a destructive program containing code that can generate copies of it and attaches itself with other programs so that it is automatically executed when those programs are executed.
- A virus is a program designed by a computer programmer to do a certain unwanted function.
- The virus program can be simply annoying like displaying a happy face on the user's screen at a certain time and date.
- A virus usually performs destructive operations by deleting or modifying the data on storage devices attached to the computer.
- Virus cannot physically destroy the hardware.
- Some virus may make invisible changes in the user's data.
- A virus may make network resources unavailable to the users.
- A virus may detect some special information e.g. password, pin code etc. and transfers it to other users on the network.
- Virus infects computers data and can costs a lot of time and money to correct it.

CAUSES OF VIRUSES:

- Emails, Networks, Removable Storage media, Pirated software are ways through which a virus reaches from one computer to another.

Emails:

- Computers are infected due to receiving of emails containing virus programs.
- When a user opens an infected email, the virus is also loaded into the memory and attaches itself with other programs.
- You cannot get a virus from a plain email message. Modern email programs provide the ability to allow users to format email messages with HTML and attach scripts to them for various purposes and it is possible for a hacker to attempt to spread a virus by building a virus script into an HTML type of email message.

Networks:

- Virus is also spreading by using Internet and other networks
- When you are accepting software or scripts on Internet sites or reading mail from unknown senders it is wrong to run a program from that site or sender without checking it with an **anti-virus program**.
- When you download a file 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:

- You can transfers the data from one computer to another through some removable media like floppy disks, CDs, or flash drives; therefore, when you copy the data using removable storage, the infected files can be transferred to your computer.

Pirated software:

- The virus can also infect your computer by the use of pirated software (The software without license is called pirated software).
- Some companies may intentionally attach some virus programs into their software. This program will only activate when it does not find licensed files on the computer.

Q3. What are the different types of Virus?

TYPES OF VIRUSES:

- Boot Sector Virus, Chernobal virus, Logic Bomb, Trojan Horse, RedLof etc.

Boot Sector Virus:

- Boot sector virus modifies the boot sector (the first sector which contains the instructions to automatically load OS in memory) program and is loaded in the computer memory whenever the computer is turned on.
- This virus is attached with system executable files i.e. .exe, .com and .dll files.
- When the user uses these files, the virus performs destructive operations and destroys all the data files.

Chernobal virus:

- It deletes all the Microsoft office files.
- It also deletes the partition information from the disk.
- User cannot access files from the disk because of this virus.

Logic Bomb:

- It is a virus that is activated on the basis of a logical condition.
- The virus instruction is executed if the logical condition is true.
- It is activated on a certain date and time.

- The bomb can be discovered by chance.

Trojan horse:

- It is a part of some computer programs e.g. destructive instructions inside the game programs.
- When the infected program (game) runs on the system, then this virus is activated.
- An example of Trojan horse is FORMAT C instruction which is executed with the execution of a game.

RedLof:

- It is polymorphic virus written in VB Script.
- It infects the Folder.htt file which is the part of Windows Active desktop.
- It appends itself to other infected files on the hard disk and causes destruction.

Some viruses make unnoticeable changes. They corrupt data being used. Some viruses may make data unusable. A virus may detect some special information like passwords or sensitive data. It may send the data to some other user on a network. For example a virus may read the pin code or credit card number and then send it to another user. A virus may also make some resources unavailable to the users. For example, a virus may start sending data on a network. The network may become unavailable for the users.

Q4. What are the different safety measures against virus?

SAFEGUARD AGAINST VIRUSES:

Following are the few steps to save your computer from viruses.

- Never open unknown emails.
- Scan all emails even if you know the sender.
- Minimize the data transfer from one computer to another through removable media.
- Avoid downloading freeware programs without checking it for virus.
- Always use latest version of antivirus software and remove the infected files from the system.
- Always keep copy (backup) of your data on removable media.

Q5. What is a importance of data security?

DATA SECURITY:

It is the most important issue in any organization. The organization is responsible for the security of data so that unauthorized persons cannot access and modify the data. Many organizations store data of their customers online for providing fast services e.g.

- A credit card company stores data of its customers online.
- A bank providing online services will be using online data storage for the customers.

- A university may provide online results of examinations.
- People take online exams like GRE, GMAT etc.

These developments generate a new problem called **“Data Security”**. As the sensitive data of people is available online therefore security of data is necessary. If an unauthorized person gets this data, the whole organization may suffer irreparable or permanent loss.

Q6. What are Security Violations and Security Threats?

SECURITY VIOLATIONS:

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

- Unauthorized persons may get into the computer room and takes away all storage devices containing sensitive data.
- Unauthorized users may get access to personal data and use it to get some benefits.
- Unauthorized users may use an online mail server to view email messages of other users hence causing privacy issues.
- Unauthorized users may get access to the 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 computer is unavailable to authorized users. This is called **denial of service situation**.

SECURITY THREATS:

Following are the main threats to data security.

Intentional Threats:

- A user can intentionally delete important data. The intentional threats may occur for the following reasons.
    - A hacker can delete data on a computer.
    - An angry employee of the organization can delete the data.

Un-Intentional Threats:

- Some authorized user of the data may unintentionally delete or change sensitive data.

Solutions:

User Rights:

- 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.

Periodic Backup:

- Periodic backup of data should be taken to recover from this sort of situation.

Password Protection:

- Password protection should be used to use any resource.
- Authorized users must be asked to change their passwords periodically.
- Very short and common passwords should be avoided.

Encryption Algorithms:

- Encryption algorithms should be used, so that if anyone gets access to the data, he should not be able to make any sense out of it.

Anti-Virus:

- Anti-virus software should be used to scan all data coming into the organization.

Lock Room:

- Computers and all backing storage devices should be placed in lock rooms with only authorized access to these resources.

Q7. What is meant by DATA Protection?

DATA PROTECTION:

Data protection means make sure that personal data of any organization or a person is kept hidden from unauthorized users. The organizations collect required data of the customers for business transactions and these pieces of data contains the personal information of a customer e.g. a hospital having data about the disease history of patients.

All the data kept by different organizations may be disclosed by the organization for some legal purpose e.g. the medical researches may use the patient's history or any other data to draw some conclusions. If the hospital management distributes this data to someone else then this may make the patient feel embarrassment. The data protection legislation consider such cases.

Q8. What are DATA Privacy Issues?

PRIVACY ISSUES:

- It is the right of a person to keep his personal information away from other people.
- A person has a right to see his data and he has to submit an application to view that data any time.
- He has to stop the processing of his data by the organization.
- He has a right to claim 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 the above points that:

- Data protection act tries to minimize the misuse of personal information.
- Data protection act provides a safeguard against such crimes.

An organization collecting data should collect relevant data for its working and should not collect unnecessary information. The following points should be considered to ensure the individual's privacy issues.

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

Q9. What is Data Protection Legislation?

DATA PROTECTION LEGISLATION:

Data protection legislation defines the laws that ensure data protection. The principles of Data Protection Act are as follows:

- The purpose of keeping and using of 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 the contract between two parties. The processing is required by law or is necessary to carry out the interest of the individual.

Q10. What are Important Privacy Acts?

IMPORTANT PRIVACY ACTS:

- 1980 Privacy Protection Act
- 1984 Cable Communication Policy Act
- Data Protection Act 1984
- 1987 Computer Security Act
- 1988 Video Privacy Protection Act
- 1988 Matching and Privacy Protection Act
- 1990 Computer Misuse Act

- 1998 Data Protection Act

1980 PRIVACY PROTECTION ACT:

- It prohibits agents of federal government from making unannounced, searches of press office if no one there is suspected of crime.

1984 CABLE COMMUNICATION POLICY ACT:

- This act 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.

Data Protection Act 1984:

It consists of eight points and the main purpose of this Act is to protect the personal data from unauthorized access held on computer systems.

- The information and personal data shall be obtained and 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.
- 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, where necessary, kept up to date.
- Personal data held for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.
- An individual should be allowed at reasonable intervals, without expense and delay, to have access to his/her data, and where appropriate, to have such data corrected or erased.
- Appropriate security measure shall be taken against unauthorized access to, or alteration, accidental loss, or destruction of personal data.

1987 COMPUTER SECURITY ACT:

- This Act makes actions that affect the computer security files and telecommunication illegal.

1988 VIDEO PRIVACY PROTECTION ACT:

- This Act 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.

1988 Matching and Privacy Protection Act:

- It prevents the government from comparing certain records in an attempt to find a match; however most comparisons are still unregulated.

1990 Computer Misuse Act:

This Act makes provision for securing computerized material against unauthorized access and modification; and for connected purposes. This Act was passed to deal with the problem of hacking of computer system. With the developments in technology the issue has become more serious and therefore 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.

1998 DATA PROTECTION ACT:

It came into force early in 1999 and covers how information about living identifiable person is used. It is much broader in scope than the earlier 1984 Act but it contains some provision for a transitional period for compliance with the new requirements. The 1998 Act applies to:

- Computerized personal data.
- Personal data held in structured manual files.

Q11. What is the Copyright Act?

THE COPYRIGHT ACT:

Software is like a property and copyright is a right to copy software. The principal law governing software piracy is the "Copyright Act 1976". Some amendments were made in 1983. Software piracy is believed to be punishable crime involving huge amount of penalties. Software is an "Intellectual Property" that has been developed and brought to market after a lot of efforts and cost. So is future financial interest may be sure by the concerned legal authorities.

Q.12 Explain anti virus software with examples. Write some benefits of using anti virus software.

Ans. Antivirus Software:

A type of software that is used to detect and remove viruses is called antivirus software. Antivirus programs contain information about different known viruses. They can detect viruses and remove them.

Many Antivirus programs are available in the market. But no single software can detect and remove all viruses. Many new viruses are invented and spread through Internet continuously. Antivirus programs are also upgraded continuously to detect these new viruses. Antivirus program not only detects viruses from computer but also prevent new viruses from entering into the computer.

Examples:

Some important Antivirus programs are as follows:

- Norton Antivirus
- McAfee

- NOD32
- Kaspersky
- AVC

Benefits:

Some important benefits of using antivirus programs are as follows:

- Antivirus program protects important data from virus.
- It checks all files before they enter computer system.
- It alerts the user about the virus before it causes any damage to computer.
- It quarantines or eliminates a virus so that it may not harm computer.

Q.13 What is password?

Ans. Password:

- Pass is a secret word that is used to protect a computer system or program. It may consist of numbers, alphabets or both. The user has to type the password to access the computer system.
- The purpose of password is to protect data stored on a computer. It protects data from being lost, misused or deleted by any person.
- A person who knows the password can access the system.
- Only authorized person can change password.
- An unauthorized person cannot access a computer system or program that is protected by a password. So the computer and the data stored on it will be safe and protected.
- Every computer provides an option for setting password. If the computer is protected with password, it will ask for that password to login.
- Email facility on the Internet is also protected with password. Every user has to give email ID and password to check emails.
- Internet Service Providers provide user accounts with passwords. The user ID and password is used to connect to the Internet.

Q.14 What is backup of data? What are reasons of backup and types of backup?

Ans. Backup of Data:

- An additional copy of data or information stored on secondary storage media is called the backup of data. The common media for backup are zip disk, magnetic tap, floppy disk, CD-ROM and hard disk etc.
- The computer system can be damaged due to many reasons. The data stored on the system may also be lost, deleted or altered. Sometimes the data is very important and

it cannot be created again. For example, computer in a bank may contain the records of all money transactions. The backup of data is used if your system crashes accidentally and the data stored in it is lost.

Reasons of Backup:

The purposes of taking backup of data are as follows:

- An important file can be deleted accidentally.
- The user may overwrite a part or whole of an existing file.
- A mechanical failure in computer may result in loss of data.
- A virus may damage the data stored on the computer.
- Computer system may be stolen by anybody.
- Computer system may be damaged due to fire or power failure.
- It is very important to take the backup of data regularly.
- It should be stored at a safe and protected place. In big organization, the backup is normally stored on a centralized networked computer.
- In small organization, the backup is stored on floppy disks, Zip disks or CD-ROM.

Types of Backup:

There are two ways to take the backup of data. These are complete backup and incremental backup.

Complete Backup:

- Backup of all data on the hard disk is called complete backup.
- The advantage of this backup is that the entire hard disk is backed-up.
- The data can be restored from this backup in case of a problem in system.
- It takes more time and storage capacity because the entire data of hard disk is copied.

Incremental Backup:

- Incremental backup creates a copy of only the data that is newly created or modified since the last backup.
- This process is performed automatically in some software. In this type of backup, the entire disk is not copied.
- It takes less time and space than complete backup.