Chapter 6

Computer Security

Introduction to Computer Security

Security: The prevention and protection of computer assets from unauthorized access, use, alteration, degradation, destruction, and other threats.

- Computer systems should have a set of protection policies to restrict and control the system resources
- Considering:
  - Unauthorized access
  - Malicious modification or destruction
  - Accidental introduction of inconsistency

Security Goals

- **Data Confidentiality**
  - It is concerned with having secret data remain secret
- **Data Integrity**
  - Unauthorized users should not be able to modify any data without the owners permission
  - Includes removing data and adding false data
- **System Availability**
  - Means nobody can disturb the system to make it unusable

Security is thus based on the following independent issues:

- **Privacy** - the ability to keep things private/confidential
- **Trust** - do we trust data from an individual or a host? Could they be used against us?
- **Authenticity** - are security credentials in order? Are we talking to whom? We think we are talking to, privately or not.
- **Integrity** - has the system been compromised/altered already?

Why Computer Security?

Computer security is required because computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. There may be several forms of damage, which are obviously interrelated. These include:

- Damage or destruction of computer systems.
- Damage or destruction of internal data.
- Loss of sensitive information to hostile parties.
- Use of sensitive information to steal items of monetary value.
- Use of sensitive information against the organization's customers, which may result in legal action by customers against the organization and loss of customers.
- Damage to the reputation of an organization.
- Monetary damage due to loss of sensitive information, destruction of data, hostile use of sensitive data, or damage to the organization's reputation.
- Losing the ability to use the system

Security Threats

A *threat* is a potential violation of security. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system.

A computer security threat can be any person, act, or object that poses a danger to computer security. Generally, environments can be hostile because of

- **Physical threats** - weather, natural disaster, bombs, power failures, etc.
- **Human threats** - stealing, trickery, bribery, spying, sabotage, accidents.
- **Software threats** - viruses, Trojan horses, logic bombs, denial of service, trap door.

1. **Fraud and Theft**

Computer systems can be exploited for both fraud and theft both by "automating" traditional methods of fraud and by using new methods. For example, individuals may use a computer to skim small amounts of money from a large number of financial accounts, assuming that small discrepancies may not be investigated. Financial systems

are not the only ones at risk. Systems that control access to any resource are targets (e.g., time and attendance systems, inventory systems, school grading systems, and long-distance telephone systems). Insiders or outsiders can commit computer fraud and theft. Insiders (i.e., authorized users of a system) are responsible for the majority of fraud.

Since insiders have both access to and familiarity with the victim computer system (including what resources it controls and its flaws), authorized system users are in a better position to commit crimes. Insiders can be both general users (such as clerks) and technical staff members. An organization's former employees, with their knowledge of an organization's operations, may also pose a threat, particularly if their access is not terminated promptly.

2. Loss of Physical and Infrastructure Support

The loss of supporting infrastructure includes power failures (outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes.

3. Malicious Hackers

The term malicious hackers, sometimes called crackers, refer to those who break into computers without authorization. They can include both outsiders and insiders. Much of the rise of hacker activity is often attributed to increases in connectivity in both government and industry. One 1992 study of a particular Internet site (i.e., one computer system) found that hackers attempted to break in at least once every other day. The hacker threat should be considered in terms of past and potential future damage. Although current losses due to hacker attacks are significantly smaller than losses due to insider theft and sabotage, the hacker problem is widespread and serious.

4. Threats to Personal Privacy

The accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies, combined with the ability of computers to monitor, process, and aggregate large amounts of information about individuals have created a threat to individual privacy. The possibility that all of this information and technology may be able to be linked together has arisen as a specter of the modern information age.

5. Malicious Code

Malicious code refers to viruses, worms, Trojan horses, logic bombs, and other "uninvited" software. Sometimes mistakenly associated only with personal computers, malicious code can attack other platforms.

- **Viruses**
  - "A small program that replicates and hides itself inside other programs usually without your knowledge."
  - It gets attached to some part of an operating system or any other computer program.
  - It may attach itself to any executable code, including but not limited to boot sectors and /or partition sectors of hard and/or floppy disks.
  - A computer virus can perform:
    - corrupt or destroy data
    - increase file size
    - format the hard disk
    - degrade system performance
    - manipulate the directory contents
    - rename all files with different name

Types of viruses

A. Multi-Partite

- A virus that attempts to attack both the boot sector and the executable, or program, files at the same time.
- When the virus attaches to the boot sector, it will in turn affect the system's files, and when the virus attaches to the files, it will in turn infect the boot sector.
- Such viruses are highly infectious.

B. Companion Virus

- A virus which infects executable files by creating a 'companion' file with the same name but an .COM extension.
- Since DOS executes .COM files, followed by .EXE files, and finally .BAT files, the virus loads before the executable file.

C. Boot sector or MBR virus

- A virus which infects the boot sector of disks

Boot sector

- Hard disk drives, floppy diskettes, and logical drives (partitions) all have boot sectors where critical drive information is stored.

Master Boot Record

- On all PC fixed disks, the first physical sector is reserved for a short bootstrap program. This sector is the master Boot (MBR).

D. Stealth Virus

- A computer virus that actively hides itself from antivirus software by either masking the size of the file that it hides in or temporarily removing itself from the infected file and placing a copy of itself in another location on the drive, replacing the infected file with an uninfected one that it has stored on the hard drive.
- A stealth virus is one that conceals the changes it makes
- A stealth virus is programmed as such that it is able to conceal itself from discovery or defends itself against attempts to analyze or remove it

E. Macro Virus

- A macro virus is a virus written in one of the many macro languages.
- The macro viruses spread via infected files, which can be documents, spreadsheets, databases, or any computer program which allows use of a macro language.
- At present these viruses can infect Microsoft Word and Lotus Ami Pro documents.
- This virus attaches itself to a word processing or spreadsheet file(mainly Microsoft Word or Excel file)

F. Trojan (Trojan Horse)

- A Trojan (or Trojan Horse) is a program which carries out an unauthorized function while hidden inside an authorized program.
- It is designed to do something other than what it claims to, and frequently is destructive in its actions

- Seemingly innocent program contains code to perform an expected and undesirable action
- Code segment that misuses its environment
- Exploits mechanisms for allowing programs written by users to be executed by other users

G. Worm

- An independent program that reproduces by copying itself from one computer to another
- Worms are self-contained and generally use networks to spread.
- Self replicating program

6. Denial of Service

– Blocking access from legitimate users

– Overload the targeted computer preventing it from doing any useful work

7. Trap door

– Created by code inserted into system by a system programmer to bypass some normal checks

– Specific user identifier or password that circumvents normal security procedures

Security Solutions

There are a number of basic ways that a computer can be made more secure.

1. Backups (redundancy)

Just about everyone who has used a computer system has experienced losing important data in some kind of accident. There are many reasons why data get lost: it might be due to carelessness or natural disaster. The purpose of a backup is to make a copy of data, which is unlikely to be lost or destroyed by the same act as the original.

In older times, backups of disks were always made to tape. Tape was chosen because it is a relatively cheap medium, which is easily transported. If we want a backup to be protected from the same accident that would destroy the original, we have to store it in a *different physical location*. Today, the economics of backup have changed and data can often be *mirrored* to a disk at a different physical location, by using network copying. Tapes are relatively unreliable, so they have low security compared to disks. Operating

systems have different preferred ways of making backups, using different software and media. Some things are common to all systems however.

The key principle of backups is *redundancy*. Redundancy means making multiple copies of data, so that we always have something to fall back on. We can have backups of data, but we can also have backup of services, in case we lose an important piece of hardware. Redundancy is like an insurance policy.

Clearly, making backups of every file is a time-consuming process, and it requires a lot of storage. There are two kinds of backup

- **Full dump**: copies every file on a source medium to a backup medium.
- **Incremental or differential dump**: copies files according to the level of the dump. A level 0 dump copies everything. A level 1 dump copies everything, which has changed since the last level 0 dump. A level 2 dump copies everything which has changed since the last level 1 dump or level 0 dump and so on. (i.e. all levels which are lower)

2. Encryption

The term encryption refers to the practice of obscuring the meaning of a piece of information by encoding it in such a way that it can only be decoded, read and understood by people for whom the information is intended. It is the process of encoding data to prevent unauthorized parties from viewing or modifying it.

Encryption is said to occur when data is passed through a series of mathematical operations that generate an alternate form of that data; the sequence of these operations is called an algorithm. To help distinguish between the two forms of data, the unencrypted data is referred to as the plaintext and the encrypted data as ciphertext. The security of encryption lies in the ability of an algorithm to generate ciphertext that is not easily reverted to the original plaintext.

Common Uses of Encryption

Authentication

Authentication is the process of logging in, signing on or otherwise presenting information or oneself in a manner that proves his or her identity. The most common example of authentication is the use of a username and password to gain access to a system, network or web site. The username and password combination is often referred to

as a person's credentials and it is frequently sent over networks. Encryption is used to protect these credentials. If no encryption is used to protect the information as it is sent over the network, an attacker could capture those credentials and assume the identity of the originator.

Validation

Validation describes the ability to provide assurance that a sender's identity is true and that a message, document or file has not been modified. Encryption can be used to provide validation by making a digital fingerprint of the information contained within a message. A digital fingerprint is a code that uniquely identifies a file or a message by reflecting the content of the file with tremendous specificity.

Data Protection

Probably the most widely used application of encryption is in the area of data protection. Encryption of files protects the data that is written to the hard disk on the computer. This information protection is vital in the event of theft of the computer itself or if an attacker successfully breaks into the system. However, file encryption becomes more difficult to use and manage if the office has multiple employees. Because each employee needs the encryption key, protection of the key becomes a more difficult task. The more people who have access to encryption keys, the less effective encryption becomes. The risk of loss, theft or compromise of information rises as the number of users increases. Files that have been encrypted are also vulnerable to employees who leave the organization or who are disgruntled and may want to cause the organization harm.

3. Remedy for Viruses

Organizations and single-users should establish some kind of internal routines for data handling, for running a virus free computing environment. To prevent viruses from entering a system there are two options.

- **Isolate the machine**: to avoid the virus entering into the computer
  - Disconnect it from the Internet or any other network
  - Not using floppy disks, CD-ROMs or any other removable disks.
- **Install an Antivirus program**.
  - Antivirus is software utility, which (upon installing on a computer) searches the hard disk for viruses and removes which are found.
  - Popular antivirus software programs available are Norton and McAfee Antivirus programs

Functions of anti-viruses

- Identification of known viruses
- Detection of suspected viruses
- Blocking of possible viruses
- Disinfection of infected objects
- Deletion and overwriting of infected objects

Computer security controls/Making the system Secure

- **Authentication**
  - Using passwords, smart card, fingerprint
- **Anti-virus**
  - Scan the system using anti-virus software
- **Firewall**
  - Limits network access b/n trusted and untrusted hosts
- **Encryption**
  - Encrypt clear text to cipher text