MODULE 2 :

THE NEED FOR IT SECURITY

• Business Needs-Protecting The Functionality

Information security performs **four important functions** for an organization

i. Protecting the organization' s ability to function
ii. Enabling the safe operation of application running on the organization
iii. Protecting the data the organization collects and uses
iv. Safeguarding the organization's technology assets

a. Protecting the Functionality of an Organization

- Both general management and IT management are responsible for implementing information security that protects the organization's ability to function.
- Each of an organization's communities of interest must address information security in terms of business impact and the cost of business interruption, rather than isolating security as a technical problem.

b. Enabling the Safe Operation of Applications

- A modern organization needs to create an environment that safeguards these applications
- the important elements of the organization's infrastructure—operating system platforms, electronic mail (e-mail), and instant messaging (IM) applications.
- Organizations acquire these elements from a service provider or they build their own. Once an organization's infrastructure is in place, management must continue to oversee it, and not relegate its management to the IT department.

c. Protecting Data that Organizations Collect and Use

- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers.
- Any business, educational institution, or government agency operating within the modern context of connected and responsive services relies on information systems
- protecting data in motion and data at rest are both critical aspects of information security.
- The value of data motivates attackers to steal, sabotage, or corrupt it.
- An effective information security program implemented by management protects the integrity and value of the organization's data.

d. Safeguarding Technology Assets in Organizations

- Organizations must have secure infrastructure services based on the size and scope of enterprise.
- Additional security services may be needed as organization expands.
- Organisation growth could lead to the need for:
  - ✓ Public key infrastructure (PKI)
  - ✓ An integrated system of software
  - ✓ Encryption methodologies
  - ✓ Legal aggrements that can be used to support the entire information infrastructure.

- **Threats :**

A threat is an object, person, or other entity that presents an ongoing danger to an asset

To protect your organization's information, you must

(1) know yourself, that is, be familiar with the information to be protected and the systems that store, transport, and process it &

(2) know the threats you face.

The threat from external sources increases when an organization connects to the Internet.

	Category of Threat	Examples
1.	Compromises to intellectual property	Piracy, copyright infringement
2.	Software attacks	Viruses, worms, macros, denial of service
3.	Deviations in quality of service	ISP, power, or WAN service issues from service providers
4.	Espionage or trespass	Unauthorized access and/or data collection
5.	Forces of nature	Fire, flood, earthquake, lightning
6.	Human error or failure	Accidents, employee mistakes
7.	Information extortion	Blackmail, information disclosure
8.	Missing, inadequate, or incomplete	Loss of access to information systems due to disk drive failure without proper backup and recovery plan organizational policy or planning in place
9.	Missing, inadequate, or incomplete controls	Network compromised because no firewall security controls
10.	Sabotage or vandalism	Destruction of systems or information
11.	Theft	Illegal confiscation of equipment or information
12.	Technical hardware failures or errors	Equipment failure
13.	Technical software failures or errors	Bugs, code problems, unknown loopholes
14.	Technological obsolescence	Antiquated or outdated technologies

Table 2-1 Threats to Information Security[4]

2a. Compromises to Intellectual Property

- Intellectual property is "the ownership of ideas and control over the tangible or virtual representation of those ideas" (or) property created by individuals or corporations which is protected under trade secret, patent etc…
- Intellectual property can be
  a. **Trade secrets :** intellectual work, such as business plan that is a company secret and is not based on public information.
  b. **Copyrights** : refers to the legal right of the owner of intellectual property / **copyright** is the right to copy.
     This means that the original creator of a product and anyone he gives authorization to are the only ones with the exclusive right to reproduce the work
  c. **Patents** : document that grants the holder exclusive rights on an invention or process for 20years.
  d. Trademarks : A **trademark** is a recognizable phrase or symbol that denotes a specific product or service and legally differentiates it from all other products. It identify a product or service with a specific company, and is a recognition of that company's ownership of the brand.

2b. Deliberate Software Attacks

- Malicious software designed to damage, destroy, or deny service to target system.
- Includes Virus. Worms, Trojan horse, logic bombs andback doors.

a. Virus

- Computer virus is a harmful software program written intentionally to enter a computer without the user's permission or knowledge.
- A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive.
- Characteristics of Computer Viruses:
  - Propagates when the host program is executed.
  - Has an incubation period, during which no damage is done.
  - After incubation period, begins to manifest its behavior.

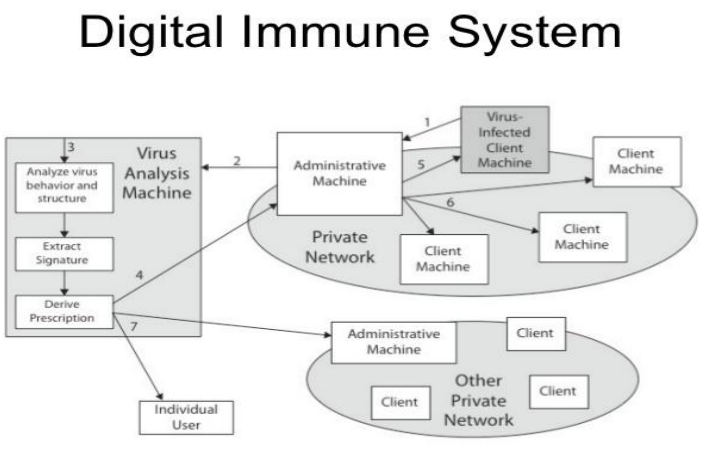
- **Types Of Virus** :

  ✓ Boot Sector Virus : This type of virus affects the boot sector of a hard disk. This is a crucial part of the disk, in which information of the disk itself is stored along with a program that makes it possible to boot (start) the computer from the disk.
  Examples: Polyboot.B, AntiEXE

  ✓ Macro Virus : Macro viruses infect files that are created using certain applications or programs that contain macros, like .doc, .xls, .pps, etc.
  Hideout: These hide in documents that are shared via e-mail or networks.
  Examples: Relax, Melissa.A, Bablas, O97M/Y2K

  ✓ Overwrite Viruses : A virus of this kind is characterized by the fact that it deletes the information contained in the files that it infects, rendering them partially or totally useless once they have been infected.
  Hideout: The virus replaces the file content. However, it does not change the file size.
  Examples: Way, Trj.Reboot, Trivial.88.D

  ✓ Memory Resident Virus : These viruses fix themselves in the computer memory and get activated whenever the OS runs and infects all the files that are then opened.
  Target: It can corrupt files and programs that are opened, closed, copied, renamed, etc.
  Examples: Randex, CMJ, Meve, and MrKlunky



b. Worms:

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- It uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.
- Symptoms of worm
  -----Slow bandwidth
  -----Slow processing speed
- **Types of worms :**

✓ *E-mail Worms:* Email Worms spread through infected email messages as an attachment or a link of an infected website.

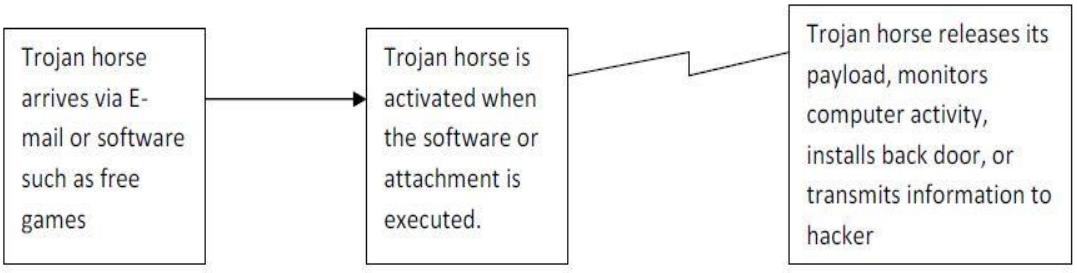
✓ *Instant Messaging* Worms: Instant Messaging Worms spread by sending links to the contact list of instant messaging applications.

✓ *Internet Worms*: Internet worm will scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. If a computer is found vulnerable it will attempt to connect and gain access to them.

✓ *File-sharing Networks Worms*: File-sharing Networks Worms place a copy of them in a shared folder and spread via P2P network.

c. Trojan horses :

- A Trojan horse, or Trojan, in computing is generally a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm.
- A Trojan often acts as a backdoor
- A Trojan may give a hacker remote access to a targeted computer system



How Trojan can impact you ?

Trojans are classified according to the type of actions that they can perform on your computer:

i. Backdoor :

- ✓ A backdoor Trojan gives malicious users remote control over the infected computer.
- ✓ They enable the author to do anything they wish on the infected computer – including sending, receiving, launching and deleting files, displaying data and rebooting the computer.

ii. Root kit :

- ✓ Rootkits are designed to conceal certain objects or activities in your system.
- ✓ Often their main purpose is to prevent malicious programs being detected – in order to extend the period in which programs can run on an infected computer.

iii. *Trojan-Banker:*

- ✓ Trojan-Banker programs are designed to steal your account data for online banking systems, e-payment systems and credit or debit cards.

iv. ***Trojan-DDoS*** :

- ✓ These programs conduct DoS (Denial of Service) attacks against a targeted web address. By sending multiple requests – from your computer and several other infected computers – the attack can overwhelm the target address… leading to a denial of service.

v. ***Trojan-Downloader*** :

- ✓ Trojan-Downloaders can download and install new versions of malicious programs onto your computer – including Trojans and *adware.*

vi. Trojan-GameThief :

- ✓ This type of program steals user account information from online gamers.

vii. Trojan-Ransom :

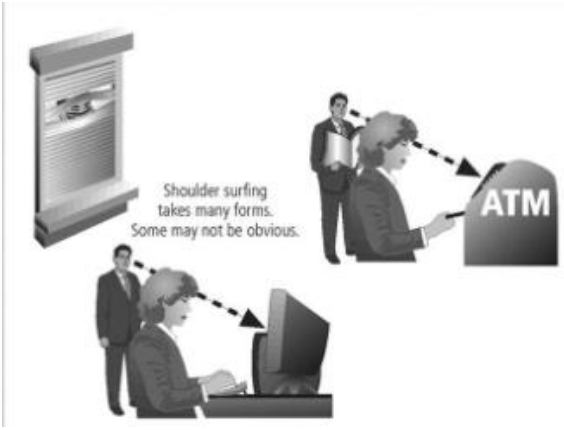
- ✓ This type of Trojan can modify data on your computer – so that your computer doesn't run correctly or you can no longer use specific data. The criminal will only restore your computer's performance or unblock your data, after you have paid them the ransom money that they demand.

d. Back Doors / Trap Doors :

- ✓ A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.
- ✓ The backdoor may take the form of a hidden part of a programme separate program (e.g., Back Orifice) may subvert the system through a root kit
- ✓ Default passwords can function as backdoors if they are not changed by the user. Some debugging features can also act as backdoors if they are not removed in the release version.

2c. Espionage or Trespass

- Unauthorised individuals gain access to the information an organisation is trying to protect.
- Attackers uses many methods to access information stored in information system.
- Some information gathering tchniques are quite legal.
- Ex : web browser to perform market research. These legal techniques are called as ***competitive intelligence.***
- When information gatherers employ techniques that cross threshold, then it is called as ***industrial espionage.***
- Some forms of espionage is ***Shoulder surfing.***
- ***Shoulder surfing:*** when individual gathers information they are not authorised to have by looking over another individual's shoulder or viewing the information from the distance. Ex : ATM machine.



Trespass : unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.

- Controls sometimes mark the boundaries of an organization's virtual territory.

- These boundaries give notice to trespassers that they are encroaching on the organization's cyberspace.

- Sound principles of authentication and authorization can help organizations protect valuable information and systems.
- These control methods and technologies employ multiple layers or factors to protect against unauthorized access.
- The classic perpetrator of espionage or trespass is the **Hacker.**
- Hackers are "people who use and create computer software [to] gain access to information illegally."
- hacker frequently spends long hours examining the types and structures of the targeted systems and uses skill, guile, or fraud to attempt to bypass the controls placed around information that is the property of someone else.
- There are generally two skill levels among hackers.
- The first is the **expert hacker, or elite hacker**, who develops software scripts and program exploits used by those in the second category**, the novice or unskilled hacker.**
- The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system.
- Novice hackers to act as script kiddies—hackers of limited skill who use expertly written software to attack a system—or packet monkeys—script kiddies who use automated exploits to engage in distributed denial-of-service attacks

2d. Sabotage or Vandalism

- Sabotage : weakening an enemy through subversion, obstruction, disruption, and/or destruction.
- Vandalism : Willful damage or destruction of any property with no other purpose than damage or destruction of said property
- acts of vandalism to either destroy an asset or damage the image of an organization.
- One who engages in **sabotage** is a saboteur.
- Saboteurs typically try to conceal their identities because of the consequences of their actions.

3. Attacks:

- An ***attack*** is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.
- It is accomplished by a threat agent that damages or steals an organization's information or physical asset.

- A vulnerability is an identified weakness in a controlled system, where controls are not present or are no longer effective.

a. Malicious Code

- The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
- Other forms of malware include covert software applications—bots, spyware, and adware— that are designed to work out of sight of users.
- A bot (an abbreviation of robot) is "an automated software program that executes certain commands when it receives a specific input.
- Bots are often the technology used to implement Trojan horses, logic bombs, back doors, and spyware.
- Spyware is "any technology that aids in gathering information about a person or organization without their knowledge.
- Spyware is placed on a computer to secretly gather information about the user and report it.
- The various types of spyware include

  (1) a Web bug, a tiny graphic on a Web site that is referenced within the Hypertext Markup Language (HTML) content of a Web page or e-mail to collect information about the user viewing the HTML content;

  (2) a tracking cookie, which is placed on the user's computer to track the user's activity on different Web sites and create a detailed profile of the user's behavior.
- Adware is "any software program intended for marketing purposes such as that used to deliver and display advertising banners or popups to the user's screen or tracking the user's online usage or purchasing activity."
- Each of these hidden code components can be used to collect information from or about the user which could then be used in a social engineering or identity theft attack.

b. Back Doors

- Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door.
- Sometimes these entries are left behind by system designers or maintenance staff, and thus are called trap doors.
- A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

c. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)

- In a denial-of-service (DoS) attack, the attacker sends a large number of connection or information requests to a target (below fig).
- So many requests are made that the target system becomes overloaded and cannot respond to legitimate requests for service.
- The system may crash or simply become unable to perform ordinary functions.
- A distributed denialof-service (DDoS) is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.
- Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised.
- The compromised machines are turned into **zombies**, machines that are directed remotely by the attacker to participate in the attack.
- Any system connected to the Internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is vulnerable to DoS attacks.
- DoS attacks can also be launched against routers or other network server systems if these hosts enable (or turn on) other TCP services (e.g., echo).

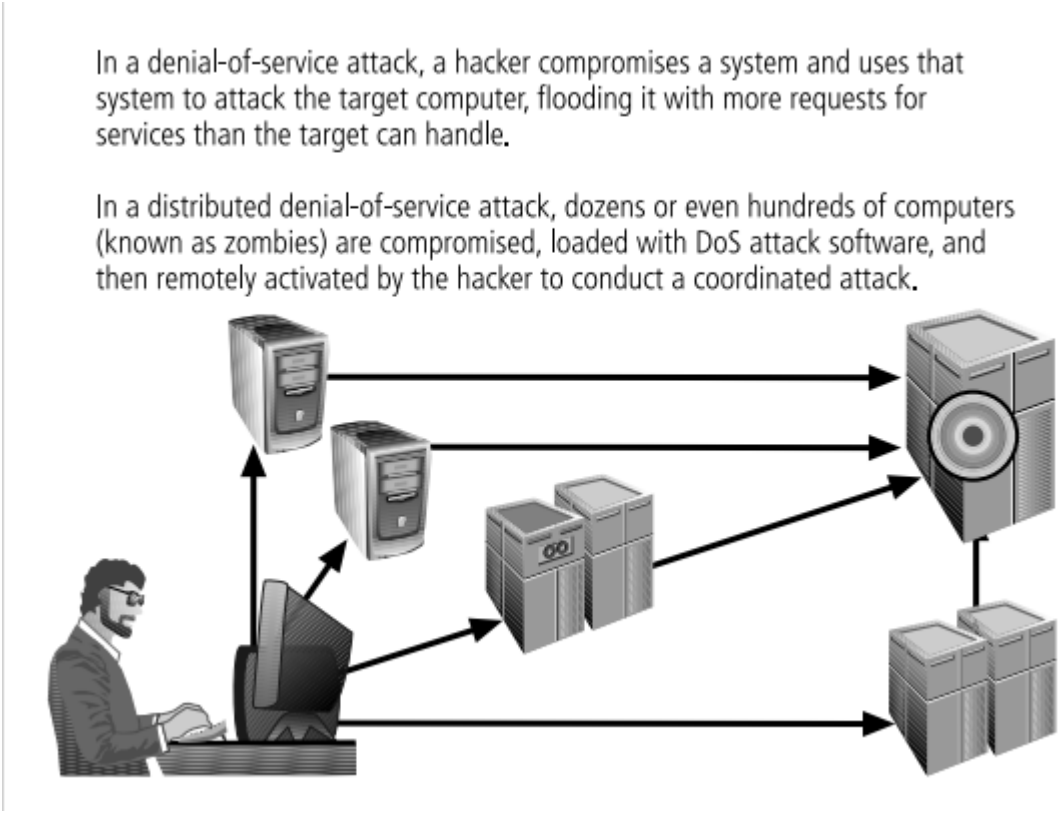


Fig : Denial of service Attack

d. Spoofing

- Spoofing is a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host.
- To engage in IP spoofing, hackers use a variety of techniques to obtain trusted IP addresses, and then modify the packet headers (fig) to insert these forged addresses.
- Newer routers and firewall arrangements can offer protection against IP spoofing.

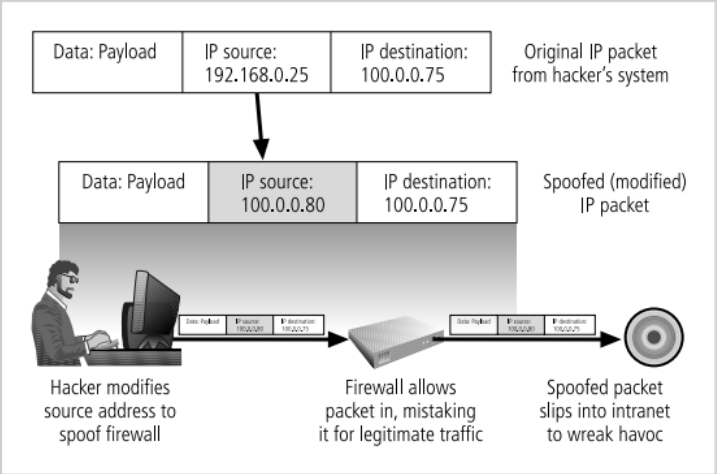


Figure 2-12 IP Spoofing

e. Spam

- Spam is unsolicited commercial e-mail.
- While many consider spam a trivial nuisance rather than an attack, it has been used as a means of enhancing malicious code attacks
- The most significant consequence of spam, however, is the waste of computer and human resources.
- Many organizations attempt to cope with the flood of spam by using e-mail filtering technologies.
- Other organizations simply tell the users of the mail system to delete unwanted messages.

f. Sniffing

- A sniffer is a program or device that can monitor data traveling over a network.
- Sniffers can be used both for legitimate network management functions and for stealing information.
- Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.

- Sniffers often work on TCP/IP networks, where they're sometimes called packet sniffers.
- Sniffers add risk to the network, because many systems and users send information on local networks in clear text.
- A sniffer program shows all the data going by, including passwords, the data inside files—such as word-processing documents—and screens full of sensitive data from applications.

g. Social Engineering

- social engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.
- Social engineering attacks may involve individuals posing as new employees or as current employees requesting assistance to prevent getting fired
- Ex: Phishing
- Phishing is an attempt to gain personal or financial information from an individual, usually by posing as a legitimate entity.
- A variant is **spear phishing**, a label that applies to any highly targeted phishing attack.
- While normal phishing attacks target as many recipients as possible
- a spear phisher sends a message that appears to be from an employer, a colleague, or other legitimate correspondent, to a small group or even one specific person.
- This attack is sometimes used to target those who use a certain product or Web site.
- Phishing attacks use three primary techniques, often in combination with one another:
  - ✓ URL manipulation,
  - ✓ Web site forgery, and
  - ✓ phone phishing

- In **URL manipulation**, attackers send an HTML embedded e-mail message, or a hyperlink whose HTML code opens a forged Web site.
- **Web site Forgery** : **Website Forgery** is a type of **web** based attack where the phisher builds a **website** that is completely independent or a replica of a legitimate **website**, with the goal of deceiving a user by extracting information that could be used to defraud or launch other attacks upon the victim. The attackers can use the recorded credentials to perform transactions, including funds transfers, bill payments, or loan requests.
- **Phone phishing** is pure social engineering. The attacker calls a victim on the telephone and pretends to be someone they are not (a practice sometimes called pretexting) in order to gain access to private or confidential information such as health or employment records or financial information.

4. Other Types of Attack

i. PassWord Crack
ii. Brute Force
iii. Dictionary Attack
iv. Man in the Middle Attack
v. Timing Attack