COMPUTER SECURITY

Definition: *(* What is Computer Security? OR Define Computer Security.)*

- Computer Security is the process of detecting and preventing any unauthorized use of your laptop/computer.
- It involves the process of safeguarding against trespassers from using your personal or office based computer resources with malicious intent or for their own gains, or even for
  gaining any access to them accidentally.

Concepts of Computer Security:

1. Confidentiality
2. Integrity
3. Availability
4. Accountability

Computer Security Challenges:

Expanded Attack Opportunities for Hackers
• Lack Of IT Talent
• Critical Infrastructure
• Developing a Cyber Security Strategy
• Deter the threats on the inside
• Plan for breaches ahead of time

 # OSI Architecture:

Need of OSI Architecture:
To assess the security needs of an organization effectively and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security.
• The Open System Interconnect(OSI) security architecture was designated by the ITU-T (International Telecommunication Union - Telecommunication).

#Note: The International Telecommunication Union (ITU) is an agency of the United
Nations (UN) whose purpose is to coordinate telecommunication operations and services

throughout the world.

• The OSI security architecture focuses on:
- security attacks
- mechanisms
- services.

• **Security attack:**

Any action that compromises the security of information owned by an organization.

• **Security mechanism:**

A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

• **Security service:**

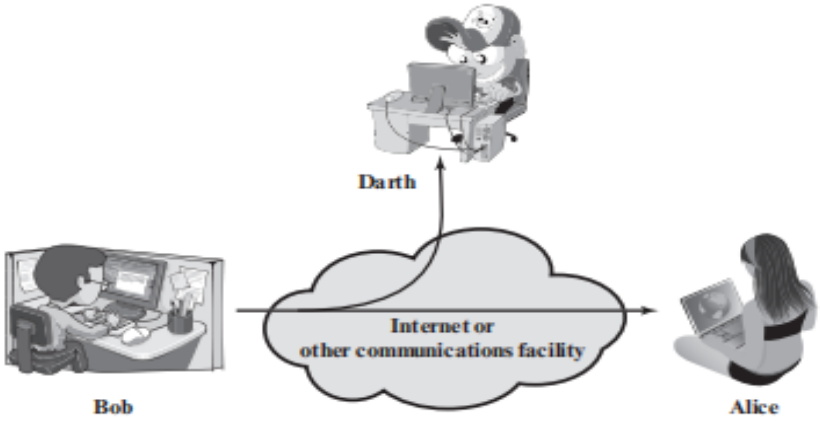
A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security Attacks: *(Q. Write a short note on Security Attacks.)*

- Attack is an assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.
- There are two types of attacks:
  1. Passive Attack
  2. Active Attack

1. **Passive Attack:** A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.



a. Release of Message Content:

An electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions. Solution for this problem was encrypting the message.

b. Traffic Analysis:

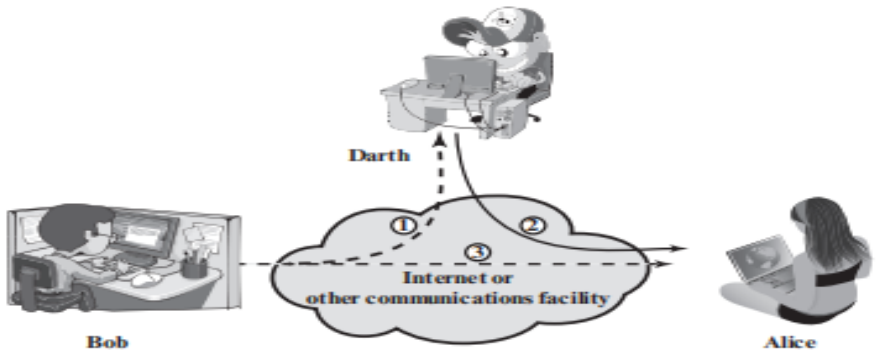
Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption.

If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

2. Active Attack:

Active attacks involve some modification of the data stream or the creation of a false stream.

These attacks are a big threat to the integrity and availability of data. Theseattack can not be prevented easily. This attack is subdivided into four categories:



a. Masquerade:
b. Replay
c. Modification of messages
d. Denial of Services.

Security Services:

1. Authentication:

2. Access Control:

3. Confidentiality:

4. Integrity:

5. Non- Repudiation:

It refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Nonrepudiation, Origin Proof that the message was sent by the specified party.

Nonrepudiation, Destination Proof that the message was received by the specified party.

Security Mechanisms: *(Q. Mention any 6 Security Mechanisms)*

1. Encipherment:

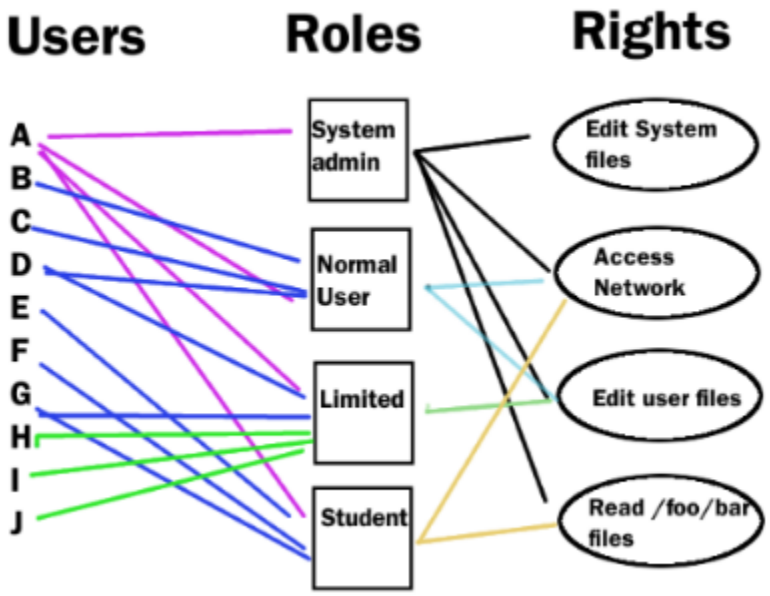
Converting your data into a secret code language using intelligent techniques in such a way that only the recipient of the data knows how to decipher it.

2. Digital Signature:

Digital Signature is a process that guarantees that the contents of a message have not been altered in transit. When you, the server, digitally sign a document, you add a one-way hash (encryption) of the message content using your public and private key pair.

3. Access control:

Access control is a security technique that regulates who or what can view, use or access a place or other resources.



4. Data Integrity techniques:

5. Security Label:

A security label is a simple, one- to eight-byte, installation-defined character string. This character string represents the union of a securitylevel with zero or more security categories.

Security Label

(*NOTE- Just for knowledge:

https://www.ibm.com/docs/en/zvm/7.2?topic=lsm-what-is-security-label)

6. Event Detection:

When a particular event occurs, the alert is sent to the concerned officials.

Ex- Triggers in DB

7. Security Audit Trail:

A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit Trails are useful both for maintaining security and for recovering lost transactions.

8. Security Recovery:

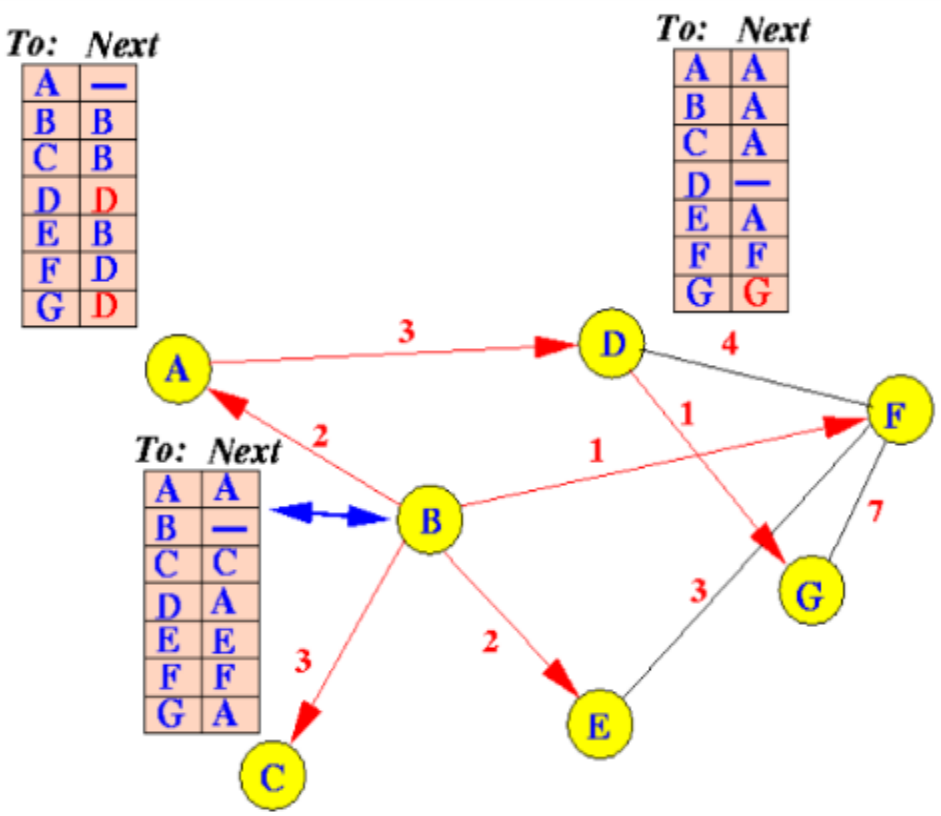
Recovery has two forms.

The first is to stop an attack and to assess and repair any damage caused by that attack. As an example, if the attacker deletes a file, one recovery mechanism would be to restore the file from backup tapes. In practice, recovery is far more complex,because the nature of each attack is unique.

In a second form of recovery, the system continues to function correctly while an attack is underway. This type of recovery is quite difficult to implement because of the complexity of computer systems.

9. Routing Control:

A routing control mechanism is composed of hardware and software, which monitors all the outgoing traffic through its connection with the Internet Service providers (ISPs), and helps in selecting the best path for efficient delivery of the data.



10. Notarization:

Notarization means selecting a third trusted party to control the communication between two entities. The receiver can involve a trusted third party to store the sender request in order to prevent the sender from later denying that she has made a request.