Introduction to Network Security & cryptography

☼Computer security

"Computer security refers to protecting and securing computers and their related data, networks, software, hardware from unauthorized access, misuse, theft, information loss, and other security issues."
Types of computer security

Computer security can be classified into four types:

1. Cyber Security: Cyber security means securing our computers, electronic devices, networks, programs, systems from cyber-attacks. Cyber-attacks are those attacks that happen when our system is connected to the Internet.

2. Information Security: Information security means protecting our system's information from theft, illegal use and piracy from unauthorized use. Information security has mainly three objectives: confidentiality, integrity, and availability of information.

3. Application Security: Application security means securing our applications and data so that they don't get hacked and also the databases of the applications remain safe and private to the owner itself so that user's data remains confidential.

4. Network Security: Network security means securing a network and protecting the user's information about who is connected through that network. Over the network hackers steal, the packets of data through sniffing and spoofing attacks, man in the middle attack, war driving, etc, and misuse the data for their benefits.

☼Three main Key Objectives:

- Confidentiality-Data Confidentiality: Private or sensitive information is not available to the unauthorized ones.
- Privacy: What information is gathered & processed ,who has access to it & to whom it is revealed.
- Integrity
- Data Integrity: Data remains in its intended state & can only be edited by the authorized parties.
- System Integrity: System performs its indented purpose without any unauthorized manipulation.
- Availability: System are running properly and providing services to the authorized users.

☼Network Security

Network security means securing a network and protecting the user's information about who is connected through that network.

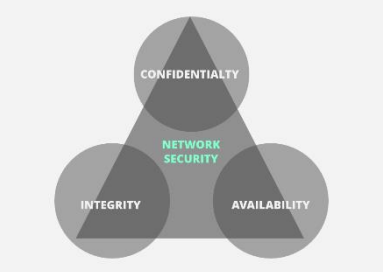
Taking Physical & software preventative measures to protect networking infrastructure from unauthorized access, misuse, modification, malfunction, destruction

Creating a secure platform users & programs to perform their critical functions within a secure environment.

☼CIA Triad

The CIA Triad is a benchmark model in information security designed to govern and evaluate how an organization

handles data when it is stored, transmitted, or processed.



CIA stands for :

- Confidentiality
- Integrity
- Availability

Confidentiality

Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals.

Integrity

The next thing to talk about is integrity. Well, the idea here is to make sure that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function.

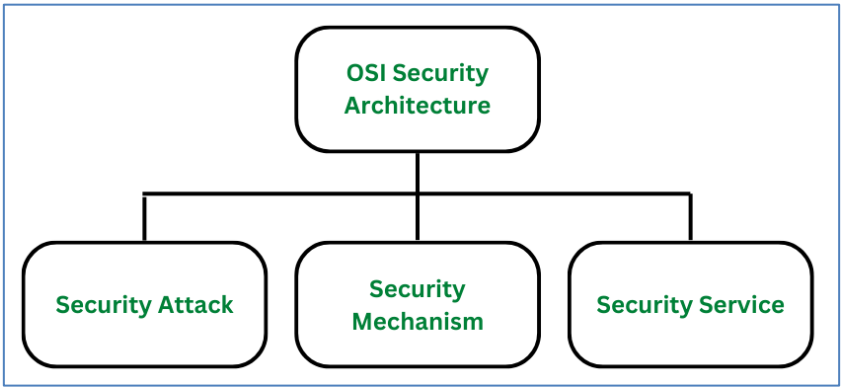
We have two common types: SHA (Secure Hash Algorithm) and MD5(Message Direct 5). Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1. There are also other SHA methods that we could use like SHA-0, SHA-2, and SHA-3.

Availability

This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades.

OSI Security Architecture:

- The OSI (Open Systems Interconnection) Security Architecture defines a systematic approach to providing security at each layer.
- It defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network.
- OSI architecture is internationally acceptable as it lays the flow of providing safety in an organization.



(1) Security attacks: An attack is when the security of a system is compromised by some action of a perpetrator. Attacks could either be active attacks or passive attacks.

(2) Security mechanisms: A mechanism that is designed to detect, prevent, or recover from a security attack.

(3) Security services: A service that enhances the security of the data processing systems and the information transfers of an organization. The services make use of one or more security mechanisms to provide the service.

Eavesdropping:

Eavesdropping attack also referred to as sniffing or snooping attack is a major concern when comes to cyber security. Through these attacks, your information like passwords, card details, and other sensitive data is easily stolen while it is getting transferred from one device to another.

These attacks are generally classified into four categories as:

(1) Interception: It is an attack on confidentiality. An adversary can compromise the network to get unauthorized access to node or data stored within it. The main purpose is to eavesdrop on the information carried in the messages.

(2) Fabrication: It is an attack on authentication. This gives threats to message authenticity.

(3) Modification: It means that a party without any authorization, not only accesses the data but tampers the data. This threatens message integrity. The main purpose is to create confusion or mislead the parties involved in the communication protocol. This is usually aimed at the network layer and the application layer.

(4) Interruption: It is an attack on the availability of the network, for example physical nodes capturing, corruption of message, malicious code insertion etc. The main purpose [4] is to launch denial-of-service (DoS) attacks.

1.4.1 Active Attacks

- Active attacks are attacks in which the hacker attempts to change or transform the content of messages or information.
- These attacks are a threat to the integrity and availability of the system.
- Due to these attacks, systems get damaged, and information can be altered.
- The prevention of these attacks is difficult due to their high range of physical and software vulnerabilities.
- The damage that is done with these attacks can be very harmful to the system and its resources.
- The good thing about this type of attack is that the victim is notified about the attack. So, instead of prevention, the paramount importance is laid on detecting the attack and restoration of the system from the attack.
- An active attack typically requires more effort and generally have more difficult implication.
- Some protective measures that can be taken against this kind of attack are:
  (a) Making use of one time passwords helps in authenticating the transactions between two parties.
  (b) A random session key can be generated, which will be valid for only one transaction. This will help in preventing the attacker from retransmitting the original information after the actual session ends.
- **Active attacks are further divided into five types**
  (i) **Masquerade attack :** A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.
  (ii) **Replay attack:** A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

(iii) **Message modification attack :** In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or modify that data on a target machine.

(iv) **Repudiation attack :** A repudiation attack occurs when the user denies the fact that he or she has performed a certain action or has initiated a transaction. A user can simply deny having knowledge of the transaction or communication and later claim that such transaction or communication never took place.

(v) **Denial-of-service attack :** A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.

1.4.2 Passive Attacks

- Passive attacks are the ones in which the attacker observes all the messages and copy the content of messages or information. They focus on monitoring all the transmission and gaining the data.
- The attacker does not try to change any data or information he gathered. Although there is no potential harm to the system due to these attacks, they can be a significant danger to your data's confidentiality.
- Unlike the Active attacks, these are difficult to detect as it does not involve alteration in data or information. Thus, the victim doesn't get any idea about the attack. Although it can be prevented using some encryption techniques.
- In this way, at any time of transmission, the message is in indecipherable form, so that hacker could not understand it. So this is the reason why more emphasis is given to prevention than detection.
- **There are some protective measures that you can take to prevent these attacks.**
  (a) Avoid posting sensitive and personal information online as attackers can use it to hack your network.
  (b) Use the encryption method for your messages and make them unreadable for any unintended intruder.
- Passive attacks are further divided into two types:
  (i) **Eavesdropping :** Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, video conference or fax transmission. The term eavesdrop derives from the practice of actually standing under the eaves of a house, listening to conversations inside. It is sometimes called as snooping.
  (ii) **Traffic analysis :** Traffic analysis is a special type of inference attack technique that looks at communication patterns between entities in a system. "Traffic analysis" is the process of intercepting and examining messages in order to deduce information from patterns in communication.

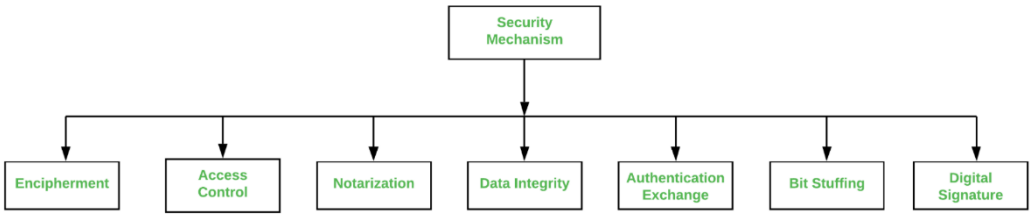
Security Services: (diagram)

Security services refer to the different services available for maintaining the security and safety of an organization. They help in preventing any potential risks to security. Security services are divided into 5 types:

- **Authentication** is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.
- **Access control** involves the use of policies and procedures to determine who is allowed to access specific resources within a system.
- **Data Confidentiality** is responsible for the protection of information from being accessed or disclosed to unauthorized parties.
- **Data integrity** is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.
- N**on- repudiation** involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message.

Security Mechanism:

Network Security is field in computer technology that deals with ensuring security of computer network infrastructure. As the network is very necessary for sharing of information whether it is at hardware level such as printer, scanner, or at software level. Therefore security mechanism can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.



1)**Encipherment**: This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.

2)**Access Control**: This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.

3)**Notarization**: This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

4)**Data Integrity**: This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.

5) **Authentication exchange**: This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not

6)**Bit stuffing**: This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

6)**Digital Signature**: This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

What Is Steganography?

- A steganography technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected.
- **Steganography** is a method of hiding information by hiding the secret message within a **fake** message.
- Steganography may be utilized on any medium, including text files, audio-video files, and images. On the other hand, Cryptography is exclusively utilized on text files.
- The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection.
- Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.
- Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection.
- It comes from the Greek words steganos, which means "covered" or "hidden," and graph, which means "to write." Hence, "hidden writing."

Different Types of Steganography

1. Text Steganography − There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

2. Image Steganography − The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

3. Audio Steganography − It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

4. Video Steganography − Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

5. Network or Protocol Steganography − It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

Active Attack	Passive Attack
In an active attack, Modification in information takes place.	While in a passive attack, Modification in the information does not take place.
Active Attack is a danger to **Integrity** as well as **availability**.	Passive Attack is a danger to **Confidentiality**.
In an active attack, attention is on prevention.	While in passive attack attention is on detection.
Due to active attacks, the execution system is always damaged.	While due to passive attack, there is no harm to the system.
In an active attack, Victim gets informed about the attack.	While in a passive attack, Victim does not get informed about the attack.
In an active attack, System resources can be changed.	While in passive attack, System resources are not changing.
Active attack influences the services of the system.	While in a passive attack, information and messages in the system or network are acquired.
In an active attack, information collected through passive attacks is used during execution.	While passive attacks are performed by collecting information such as passwords, and messages by themselves.
An active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibit in comparison to active attack.
Can be easily detected.	Very difficult to detect.
The purpose of an active attack is to harm the ecosystem.	The purpose of a passive attack is to learn about the ecosystem.
In an active attack, the original information is modified.	In passive attack original information is Unaffected.
The duration of an active attack is short.	The duration of a passive attack is long.
The prevention possibility of active attack is High	The prevention possibility of passive attack is low.
Complexity is High	Complexity is low