U20CS005

PAGE NO.
DATE / /

Tutorial-1

1 Write a short note on ~~(a)~~
(a) Security Attacks
(b) Security Mechanism.

→ A) Security Attacks:

~~Attack~~ Any action that compromises the security of information owned by an organization is known as security attacks. Attacks in cyber security are broadly classified in two categories.

a) Active attacks
b) Passive attacks

→ Active attacks:

- An active attack attempts to alter system resources or affect their operations. It involves some modification of the data stream or the creation of false statements.
- Types of active attacks are as follows:

(i) Masquerade
(ii) Modification of message
(iii) Repudiation
(iv) Replay.
(v) Denial of Service

(i) Masquerade: This attack takes place when one entity pretends to be a different entity. It may be performed using the stolen passwords & logins.

(ii) Modification of message: It means that some portion of a message is altered or the message is recorded or delayed. It is an attack on integrity and authentication and also through this they can gain access to data and can also spook the data by DOS attack.

(iii) Repudiation: It occurs when network is not completely secured or login control has been tempered. In this attack, author's information can be changed by actions of a

malicious users in order to serve false data in files.
(iv) Replay: It involves passive capture of a message and its subsequent transmission to produce an authorized effect. It is used to corrupt it or leak it to another person making it unsafe
(v) Denial of Service: It prevents the normal use of communication. It has a specific target. Disruption of entire networks by disabling or overloading is also DOS attack.

→ Passive attack:
- It uses information from the system but does not affect the system resources. They are eavesdropping or monitoring transmission in nature.
- Goal of opponent is to obtain information that is being transmitted. Types of passive attack are:
(i) The release of message content
(ii) Traffic analysis
(i) The release of message content: The main goal is to prevent files which have sensitive or confidential information.
(ii) Traffic analysis: Opponent could determine the location and identity of communicating host and could observe the frequency & length of message being exchanged.

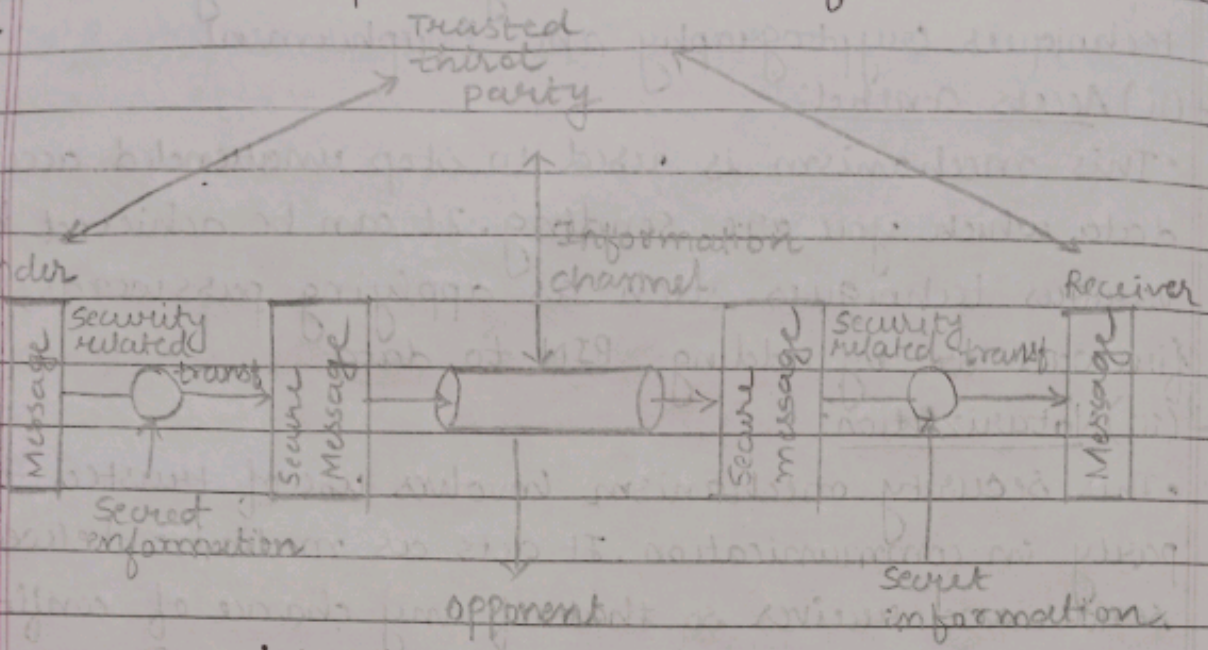
B) Security Mechanism:
- Variable mechanisms are designed to recover from the above specified attacks at various protocol layers.
- (i) Encipherment:
- It helps data to hide or cover to maintain its confidentiality. It uses mathematical calculations or algorithms which reconstruct information into not

not readable form. It can by achieved by these two techniques - Cryptography and Encipherment.

- (ii) 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 by adding PIN to data.
- (iii) 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 received for later denied.
- (iv) Data integrity:
  - 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.
- (v) 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.
- (vi) Bit Stuffing:
  - It adds 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.
- (vii) Digital Signature:
  - This security mechanism is achieved by an invisible digital data. It is used to preserve data which is not more confidential but sender's identity is to be notified.

2. Draw and explain the model for Network Security

→



Network Security Model.

- A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
- Some secret information shared by the two principles and it is hoped, unknown to the opponent. An example is an encryption key used in conjuction with the transformation to scramble the message before transmission & unscramble it on reception.
- A trusted third party may be needed to achieve secure transmission. Eg A third party may be responsible for distributing the secret information to the two principles while keeping it from any opponent or a third party may be needed to arbitrate disputes between the two principles concerning the authenticity of a message transmission.

PAGE NO.
DATE / /

- This general model shows that there are 4 basic tasks in designing a particular security service. These are:
  - Design an algorithm for performing the security related transformation
  - Generate the secret information to be used with algorithm
  - Develop methods for the distribution and sharing of the secret information
  - Specify a protocol to be used by the two principles that make use of the security algorithm and the secret information to achieve a particular security service

3. Explain the CIA triads.

→ Confidentiality, Integrity & Availability is also known as CIA triad. This model is designed to guide policies for information security within an organization. The following is a breakdown of the three key concepts that form the CIA triad.

- Confidentiality: It is roughly equivalent to privacy. Confidentiality measures are ~~defined~~ designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into wrong hand.
- Integrity: It involves maintaining the consistency accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transmit and steps must be taken to ensure data can't be altered by unauthorized people
- Availability: It means information should be consistently and readily accessible for authorized parties. This involves properly maintenance of hardware and technical infrastructure & system that hold & display the information