CSS2C08

COMPUTER NETWORKS

MODULE 5
Security in Networks

1. **Principles of cryptography**
2. Integrity
3. Authentication
4. Key distribution and certification
5. Firewalls
6. Attacks and counter measures

Security Attacks

- There are four general categories of attack :

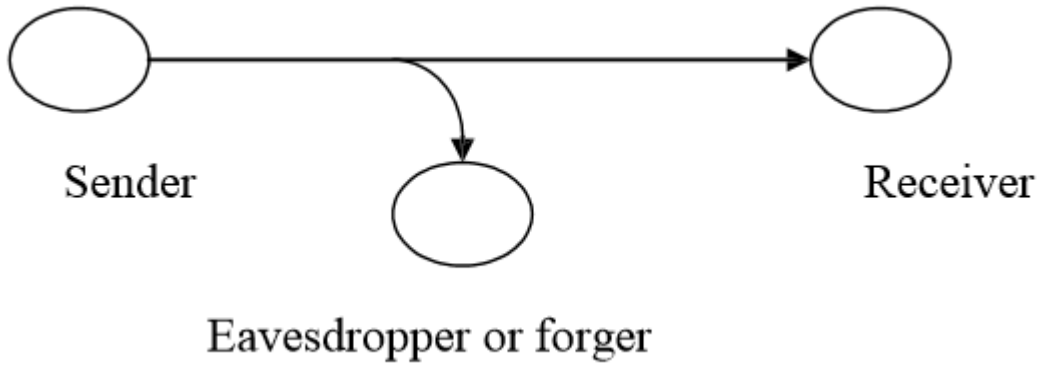
1. Interruption
2. Interception
3. Modification
4. Fabrication

1. **Interruption :**

   - An asset of the system is destroyed or becomes unavailable or unusable.
   - This is an attack on availability
   - e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

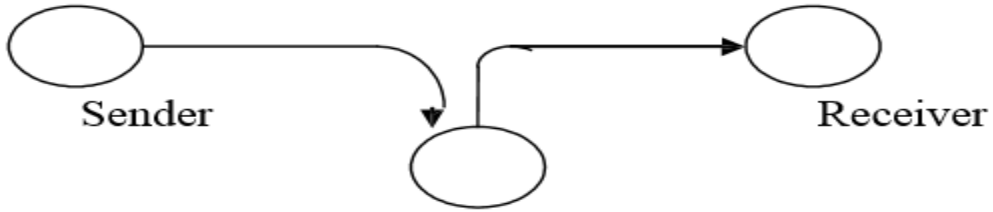
2. Interception:

- An unauthorized party gains access to an asset. This is an attack on confidentiality.
- Unauthorized party could be a person, a program or a computer.
- Eg: wire tapping to capture data in the network.



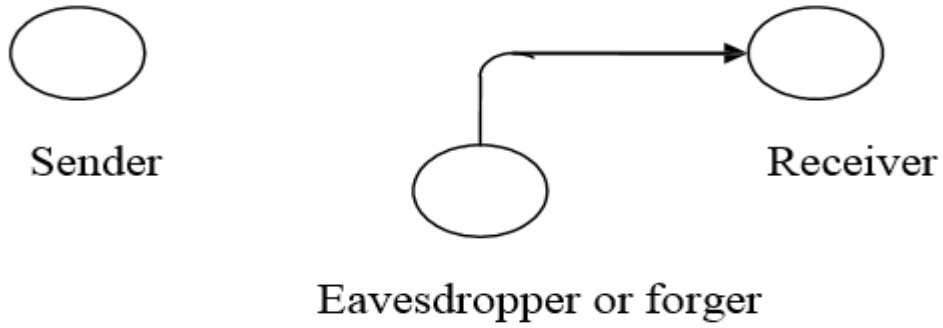
3. Modification:

- An unauthorized party not only gains access to but tampers with an asset.
- This is an attack on integrity.
- e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



4. Fabrication:

- An unauthorized party inserts counterfeit objects into the system.
- This is an attack on authenticity.
- e.g., addition of records to a file.



Cryptographic Attacks

- **Passive Attacks:**
  - Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
  - The goal of the opponent is to obtain information that is being transmitted.
  - Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.
  - Passive attacks are of two types:
    1. Release of message contents
    2. Traffic analysis

1. **Release of message contents:** A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.
2. **Traffic analysis:** If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

- **Active attacks**
  - These attacks involve some modification of the data stream or the creation of a false stream.
  - These attacks can be classified into four categories:
    1. Masquerade
    2. Replay
    3. Modification of messages
    4. Denial of service

1. **Masquerade :**One entity pretends to be a different entity.
2. **Replay**: involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.
3. **Modification of messages :**Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
4. **Denial of service:** Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.

Counter measures

- Security countermeasures are the controls used to protect the confidentiality, integrity, and availability of data and information systems.
- There is a wide array of security controls available at every layer of the stack.
- Overall security can be greatly enhanced by adding additional security measures, removing unneeded services, hardening systems, and limiting access.

- The various counter measures tools are:

1. Firewall
2. IPSec
3. SSL-Secure Socket Layer
4. TLS-Transport Layer Security

2. IPSecurity (IPSec):

- IPSecurity (IPSec) is a collection of protocols .
- To provide security for a packet at the network level.
- IPSec helps to create authenticated and confidential packets for the IP layer .
- IPSec operates in one of two different modes:
  - **the transport mode**: IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.
  - **the tunnel mode** :IPSec in tunnel mode protects the original IP header.

- IPSec defines two protocols:

1. **The Authentication Header (AH) Protocol :**

   - The AH Protocol provides source authentication and data integrity, but not privacy.

2. **The Encapsulating Security Payload (ESP) Protocol:**

   - ESP provides source authentication, data integrity, and privacy.

3. SSL:

- SSL is designed to provide security and compression services to data generated from the application layer.
- SSL can receive application data from any application layer protocol, but the protocol is normally HTTP.
- SSL provides services such as fragmentation, compression, message integrity, confidentiality, and framing on data received from the application layer.

4. TLS:

- Transport layer security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet.
- It enables privacy, integrity and protection for the data that's transmitted between different nodes on the Internet.
- TLS is a successor to the secure socket layer (SSL) protocol.

Network Layer	Attacks	Countermeasures
Physical layer	Jamming	Detect and sleep, route around jammed areas
	Node tampering	Temper-proof boxing
Link layer/medium access control	Collision, unfairness and	Authentication and anti-replay protection
	Denial of sleep	Authentication and anti-replay, detect and sleep, broadcast attack protection
Network and routing layer	Neglect and greed, misdirection, spoofing, replaying, routing-control traffic or clustering	Authentication and anti-replay protection, Secure cluster formation
	Homing	Header encryption and dummy packets
	Hello floods	Pair-wise authentication, geographic routing
Transport layer	Flooding	SYN cookies
	De-synchronization	Packet authentication
Application layer	Overwhelming sensors	Sensor tuning, data aggregation
	Reprogramming attack	Authentication and anti-replay protection Authentication streams
	Path-based DoS	Authentication and anti-replay protection