Computer Network Security

TE - IT

Lecture -5
21/07/2022

Session: 12:00 - 1:00 PM

Prof. Stella J
Department of Information Technology
Xavier Institute of Engineering

Module-1

✓ Contents

1. OSI Security Architecture
2. Security Attacks
3. Security Mechanism

OSI Security Architecture

- ITU-T X.800 Security Architecture for OSI

defines a systematic way of defining and providing security requirements

It deals with 3 Things

- Security Attack
- Security Mechanism
- Security Services

Attacks, Services and Mechanisms

Security Attack: Any action that compromises the security of information.
Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.
Security Service: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Attacks

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- have a wide range of attacks
- can focus of generic types of attacks
- note: often *threat* & *attack* mean same

Classify Security Attacks as

passive attacks - eavesdropping on, or monitoring of, transmissions to:

2 Methods,

- ✓ Release of message contents
- ✓ Traffic Analysis

active attacks – modification of data stream to:

4 Methods,

- ✓ masquerade of one entity as some other
- ✓ replay previous messages
- ✓ modify messages in transit
- ✓ denial of service

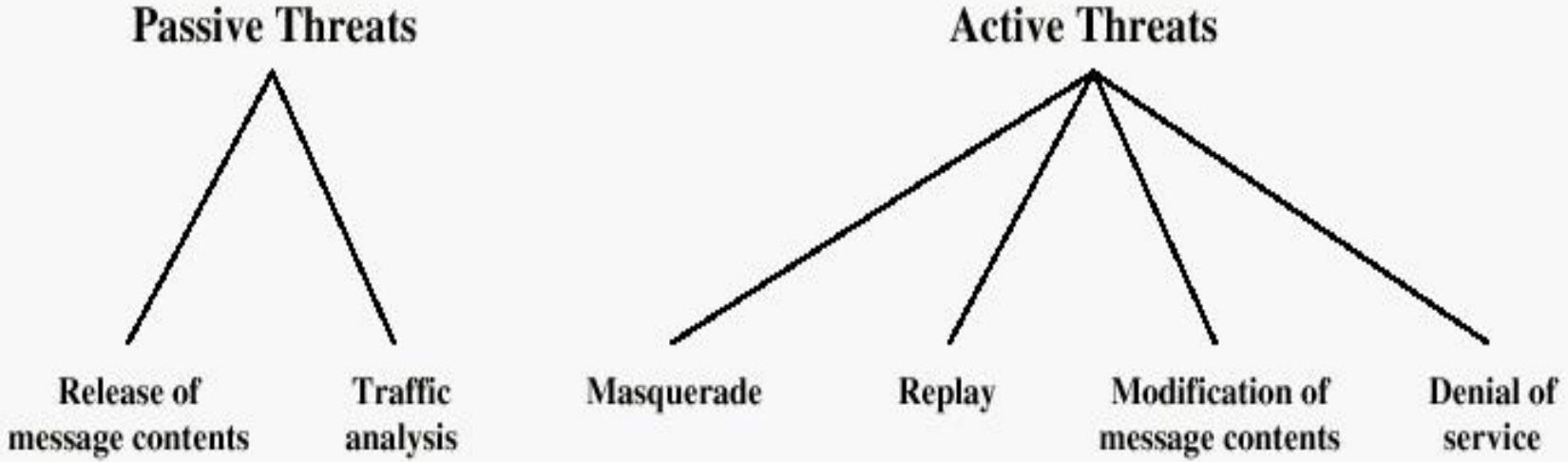
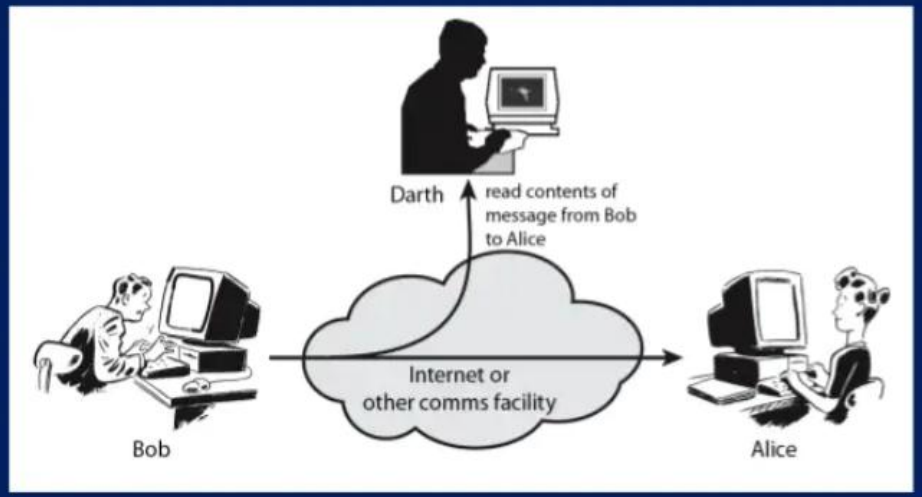


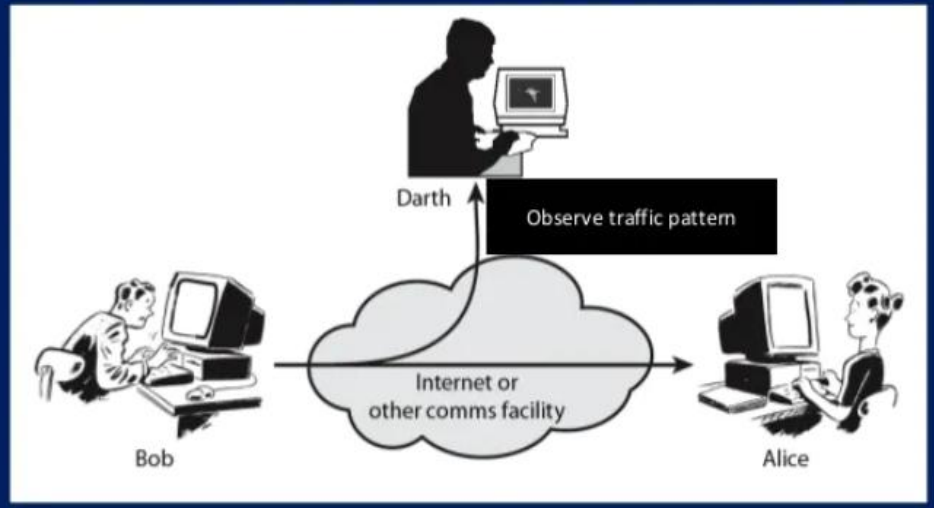
Figure 1.2 Active and Passive Security Threats

Passive Attack

Passive Attack - Interception



Passive Attack: Traffic Analysis



if Bob Send message without Encryption and if any attacker(Darth) get unauthorized access to Bob PC while transferring message then the attacker can read the content of message. So encryption is necessary while transferring messages

Bob sends message to Alice, Darth get unauthorized access in network.
Assume Message is encrypted.
Even it is encrypted Darth is anlaysing/ guessing the message depends upon the Traffic pattern such as identity of source, location of source, length of the packet being transferred.

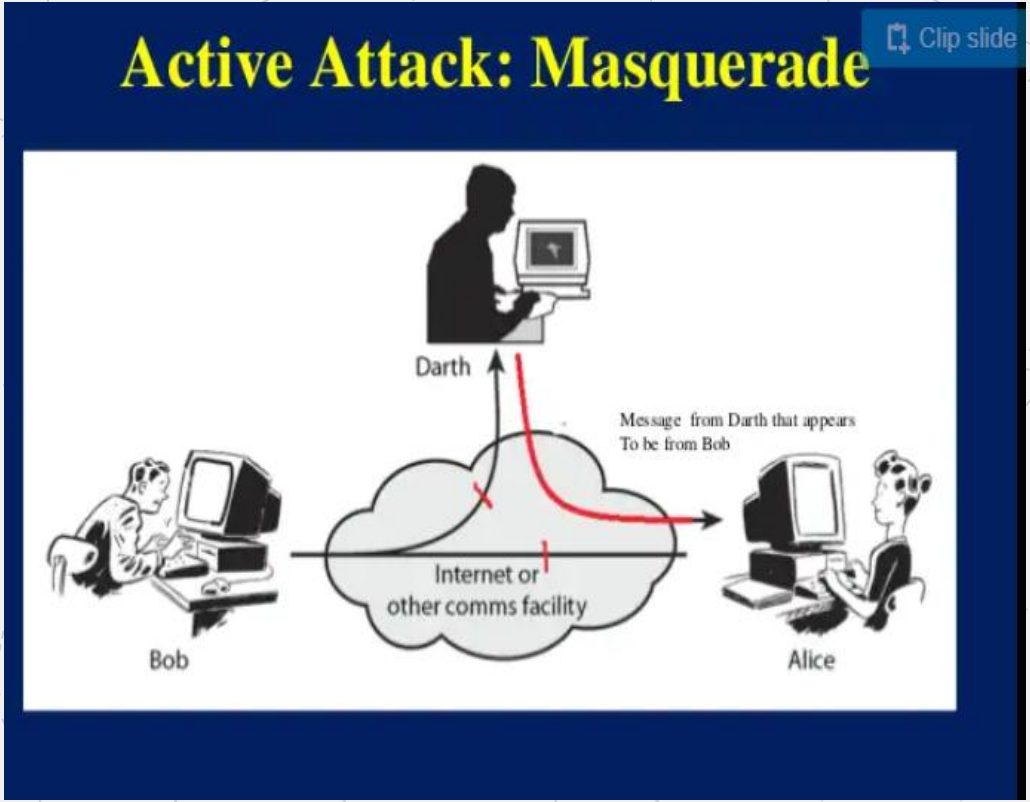
Active Attack

Masquerade:

One entity is replaced by another entity to access the resources.

Example:

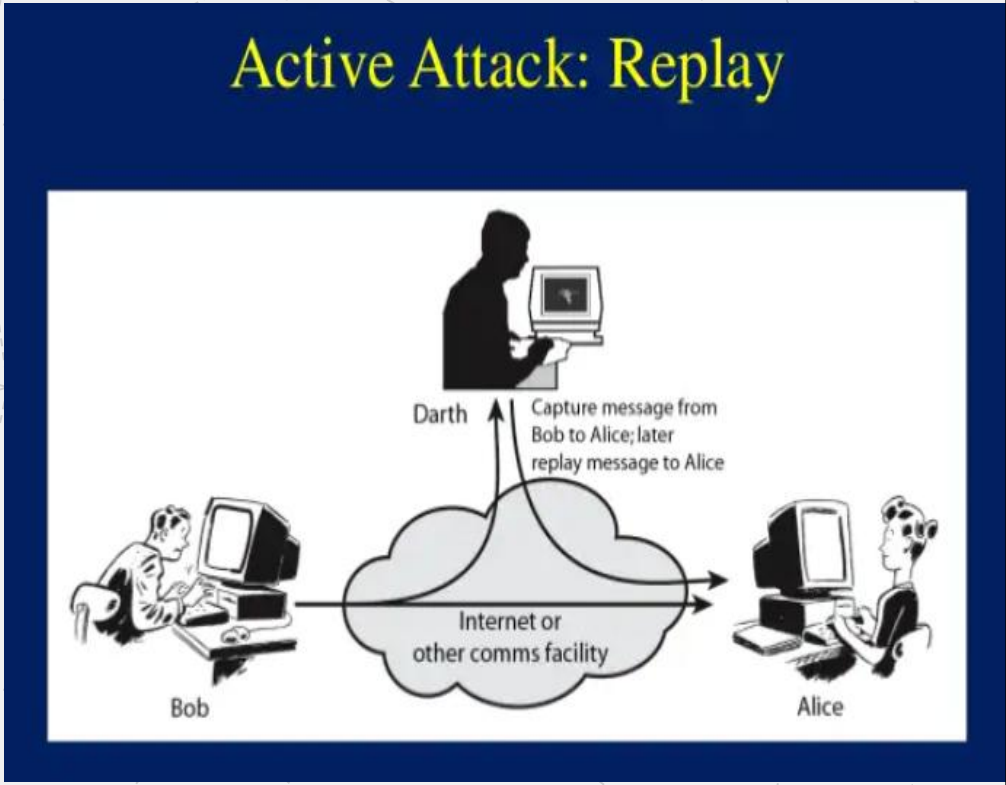
- ✓ Bob and Alice is an authorized entity, Let us assume Bob has few previliges. Darth the unauthorized entity pretends like Bob and giving request to Alice to provide some more previliges.
- ✓ The problem is, the end user doesnot know that the request is coming from attacker



Active Attack

Replay:

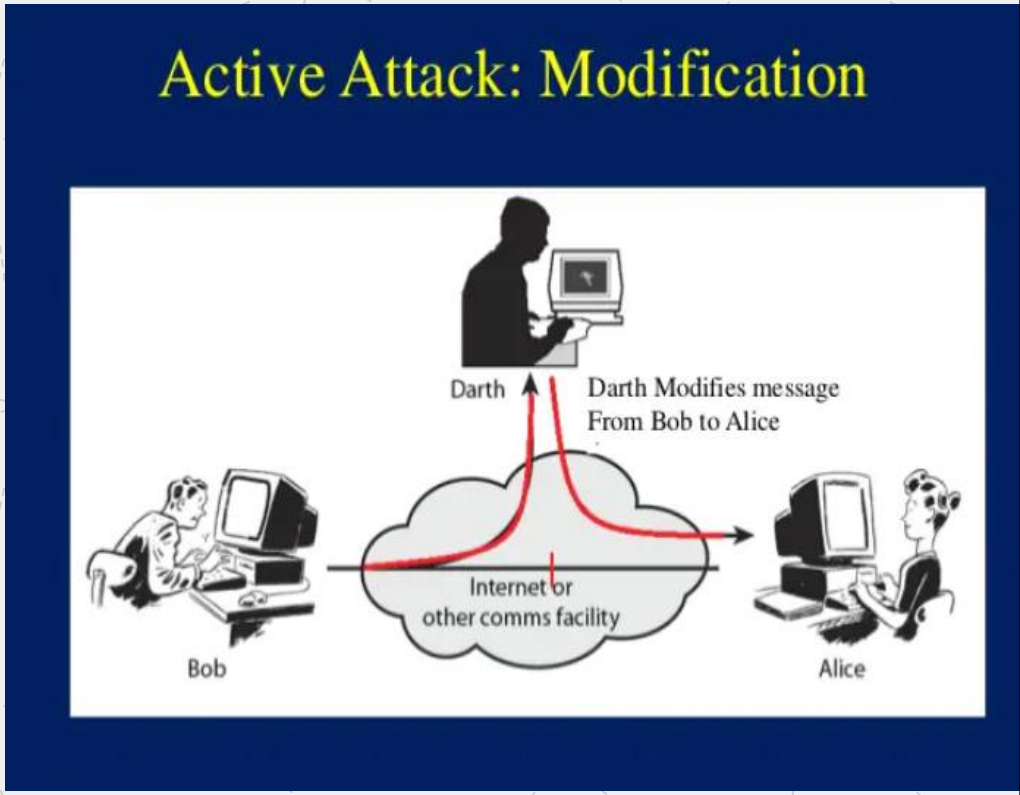
- ✓ Bob and Alice is an authorized entity, Let us assume Bob is sending message to Alice as “Hello”. Here Darth who gained unauthorized access through network and evesdrop the message sending the same messages subsequently again and again .
- ✓ The problem is, the end user (Alice) might be confused or Provoked.



Active Attack

Modification of Message:

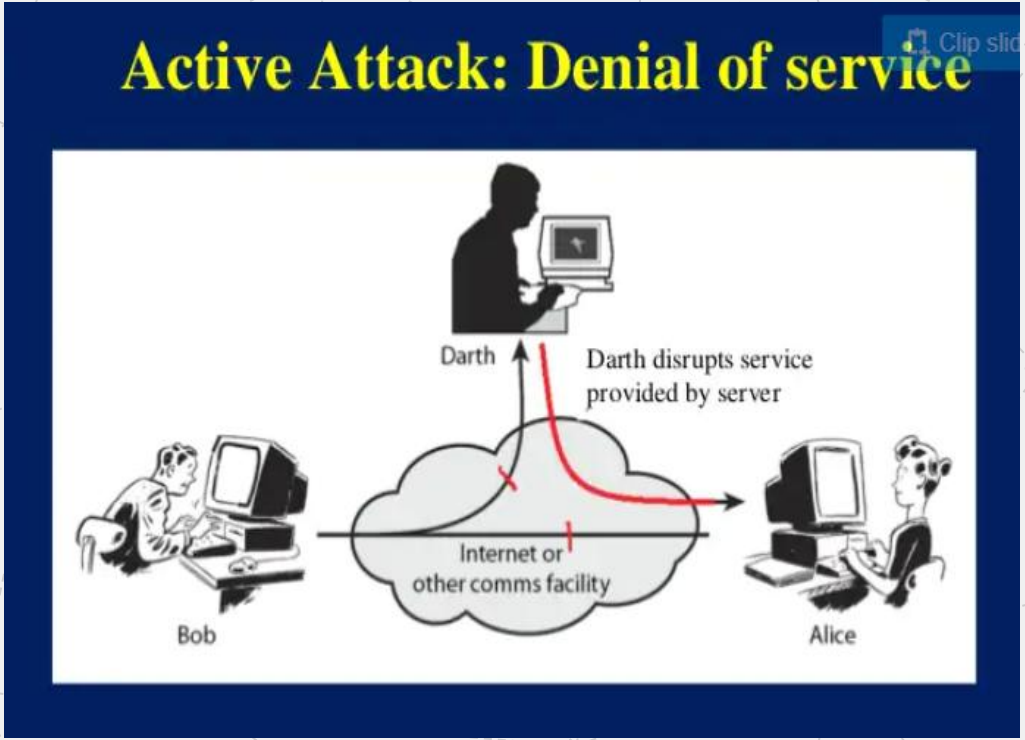
- ✓ Bob and Alice is an authorized entity, Let us assume Bob is sending message to Alice as “Hello Alice Edit the Document”. Here Darth who gained unauthorized access through network and evesdrop the message modifies the content like “Hello Alice Delete the Document”.
- ✓ The problem is, the end user (Alice) can be in loss of data while some attacker modifies the message
- ✓ Causes serious problem in the organization/individual.



Active Attack

Denial of Service:

- ✓ Consider, Bob is an authorized entity, Let us assume Bob is requesting some services from Server.
- ✓ the attacker Darth tries to overload the server by adding a small piece of code and tries to make multiple request to server.
- ✓ Server thinks that the request is from different system but it is actually from the attacker, so the authorized entity did not get acceess to the server.
- ✓ The services that denied for the user due to some attack is called Denial of service



Difference Between Active and Passive Attack:

Sr. No	Passive Attack	Active Attack
1	Hard to Detect	Hard to Prevent
2	Neither sender nor Receiver aware of the attack	Difficult to prevent physical, Software and Hardware vulnerabilities
3	Encryption prevents the success of the passive attacks	Detect and recover from any disruptions or delays
4	More emphasis is on prevention than detection	If the detection has a different effect, it may also contribute to prevention

Security Mechanisms (X.800)

- ✓ **Specific security mechanisms:**
  These specific security mechanisms are incorporated into appropriate protocol layers inorder to provide some security services.
  Types:
  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.

Security Mechanisms (X.800)

- ✓ **Specific security mechanisms:**

  2. **Digital signatures** : 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.

  3. **Access controls :** 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.

Security Mechanisms (X.800)

- ✓ **Specific security mechanisms:**

  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

Security Mechanisms (X.800)

- ✓ **Specific security mechanisms:**

  6. **Traffic padding:** 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.

  7. **Routing control:** selecting and continuously changing different available routes between sender and receiver to prevent the opponent from eavesdropping on a particular route.

  8. **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.

Security Mechanisms (X.800)

- ✓ **Pervasive security mechanisms:**
- ✓ **Types:**
  1. **Trusted functionality:** It can be used to either extend the scope or to establish the effectiveness of other security mechanisms. Any functionality that directly provides, or provides access to, security mechanisms should be trustworthy.
  2. **Security labels:** System resources may have security labels associated with them, for example, to indicate sensitivity levels. It is often necessary to convey the appropriate security label with data in transit. A security label may be additional data associated with the data transferred or may be implicit (e.g., implied by the use of a specific key to encipher data or implied by the context of the data such as the source address or route).

Security Mechanisms (X.800)

- ✓ **Pervasive security mechanisms:**
  3. **Event detection:** Security-relevant event detection can be used to detect apparent violations of security.
  4. **Security audit trails:** A security audit refers to an independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy, and procedures. Consequently, a security audit trail refers to data collected and potentially used to facilitate a security audit.
  5. **Security recovery:** Security recovery deals with requests from mechanisms such as event handling and management functions, and takes recovery actions as the result of applying a set of rules.

THANK YOU