UNIT-1

Syllabus:

Security Attacks, Security Services, Security Mechanisms, A model for Network security. Non-cryptographic protocol vulnerabilities –DoS, DDoS, Session hijacking and Spoofing.

1.1 SECURITY ATTACKS

- Any action that compromises the security of information owned by an organization.
- Security Attacks are classified into two categories as in X.800 and RFC 2828.
- The Two categories of security attacks are :
  - Passive Attacks
  - Active Attacks

1.1.1 Passive Attacks

A passive attack attempts to learn or make use of information from the system but does not alter system resources.

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.

Two types of passive attacks are the

- Release of Message Contents
- Traffic Analysis

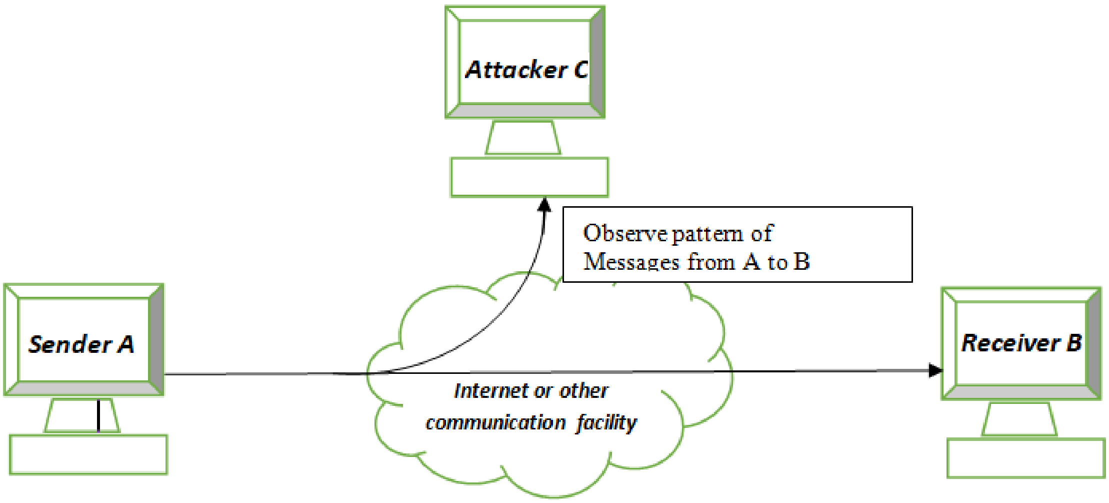
a. Release of Message Contents:

- A telephonic conversation, an E-mail message or a transferred file may contain confidential data.

A passive attack may monitor the contents of this ransmission

b. Traffic Analysis:

- In this attack the eavesdropper analyzes the traffic, determines the location, identify communicating hosts, and observes the frequency and length of message being exchanged.
- Using all these information they predict the nature of communication.
- All incoming and outgoing traffic of network is analyzed but not altered.



- Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
- Neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
- However, it is feasible to prevent the success of these attacks, usually by means of encryption.

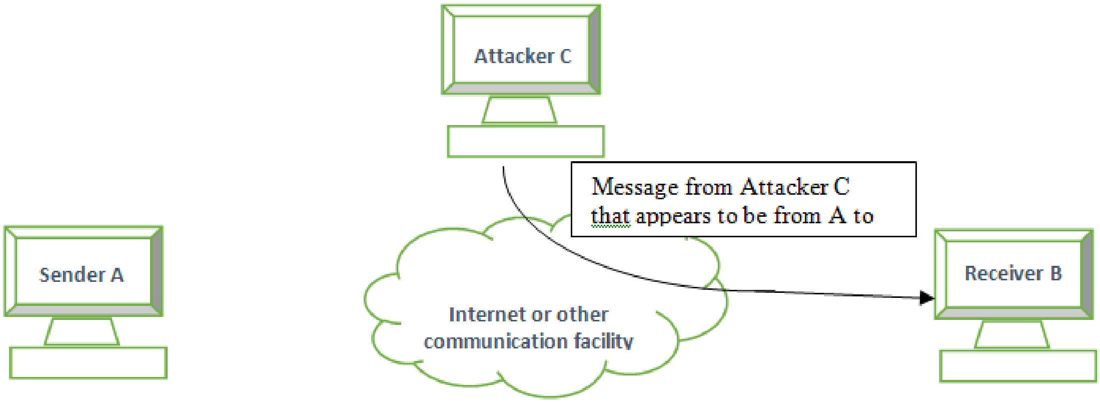
1.1.2 Active Attacks

Active attacks involve some alteration to resources of system or of the data stream or the creation of a false stream and caw be subdivided into four categories:

- Masquerade
- Replay
- Modification of Messages
- Denial of Service

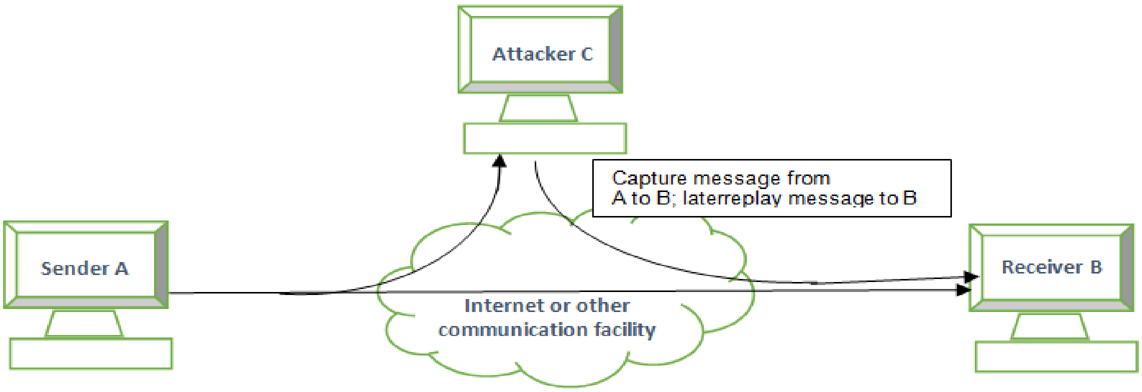
a. Masquerade

- It takes place when one entity pretends to be a different entity
- A masquerade attack usually includes one of the other forms of active attack.


Attacker C
Message from Attacker C that appears to be from A to
Sender A
Internet or other communication facility
Receiver B

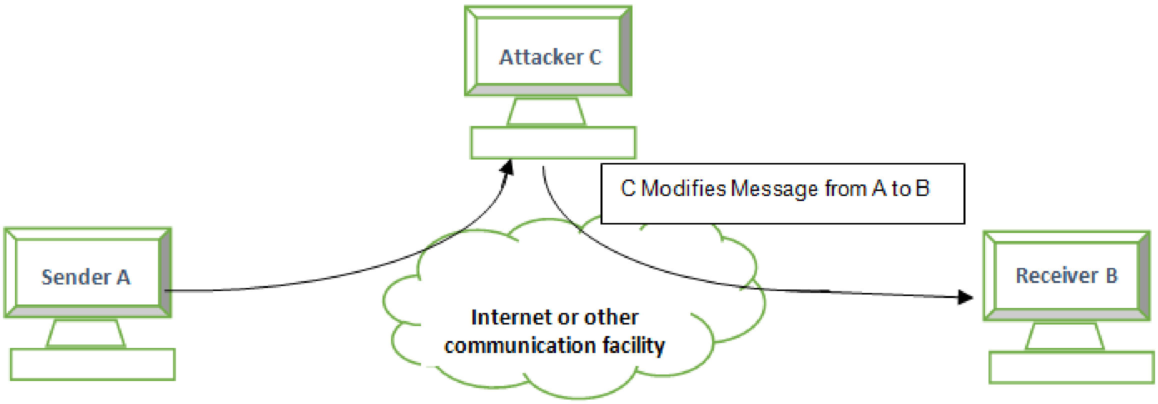
b. Replay

- It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.


Attacker C
Capture message from A to B; laterreplay message to B
Sender A
Internet or other communication facility
Receiver B

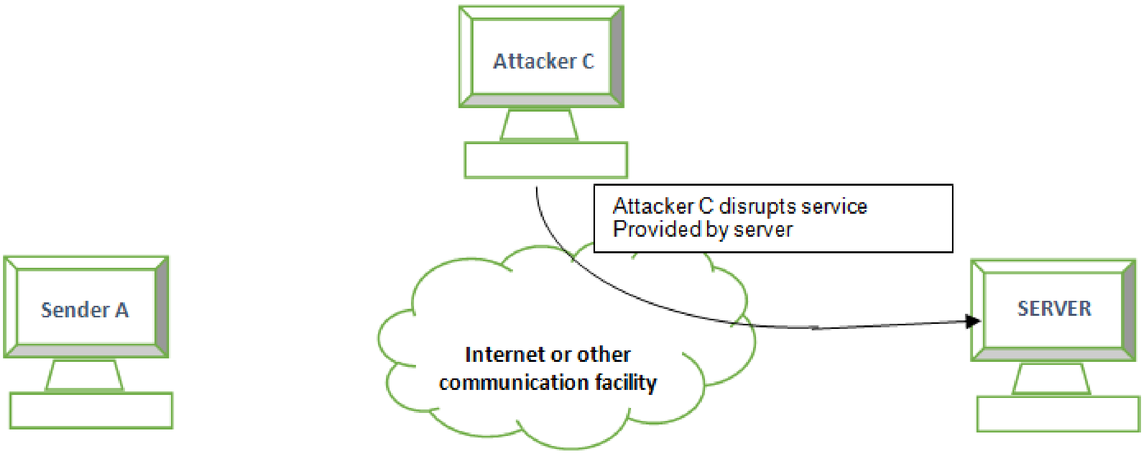
c. Modification of Messages

- simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.


Attacker C
C Modifies Message from A to B
Sender A
Internet or other communication facility
Receiver B

d. Denial of Service

○ prevents or inhibits the normal use or management of communications facilities.


Attacker C
Attacker C disrupts service Provided by server
Sender A
Internet or other communication facility
SERVER

1.2 SECURITY SERVICES

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers

OR

RFC 2828 defines it as: a processing or communication service that is provided bya system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

X.800 divides these services into five categories and fourteen specific services

Five categories in X.800 Services are

- Authentication
- Access Control
- Data Confidentiality
- Data Integrity
- Nonrepudiation

1. **Authentication:** The assurance that the communicating entity is the one that it claims to be

- **Peer Entity Authentication:** Used in association with a logical connection to provide confidence in the identity of the entities connected.
- **Data-Origin Authentication:** In a connectionless transfer, provides assurance that the source of received data is as claimed.

2. **Access Control:** The prevention of unauthorized use of a resource

3. **Data Confidentiality:** The protection of data from unauthorized disclosure.

- **Connection Confidentiality:** The protection of all user data on a connection.
- **Connectionless Confidentiality:** The protection of all user data in a single data block
- **Selective-Field Confidentiality:** The confidentiality of selected fields within the user data on a connection or in a single data block.
- **Traffic-Flow Confidentiality:** The protection of the information that might be derived from observation of traffic flows

4. **Data Integrity:** The assurance that data received are exactly as sent by an authorized entity

- **Connection Integrity with Recovery:** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
- **Connection Integrity without Recovery:** As above, but provides only detection without recovery.
- **Selective-Field Connection Integrity:** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- **Connectionless Integrity:** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification.
- **Selective-Field Connectionless Integrity:** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

5. **Nonrepudiation:** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication

- **Nonrepudiation-Origin:** Proof that the message was sent by the specified party.
- **Nonrepudiation-Destination:** Proof that the message was received by the specifiedparty.

1.3 SECURITY MECHANISM

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

Security mechanisms defined in X.800

Specific Security Mechanisms

1. Pervasive Security Mechanisms

1.3.1.Specific Security Mechanisms:

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services

1. **Encipherment**
   - The use of mathematical algorithms to transform data into a form that is not readily intelligible.
   - The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys

2. **Digital Signature**
   - Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

3. **Access Control**
   - A variety of mechanisms that enforce access rights to resources.

4. **Data Integrity**
   - A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

5. **Authentication Exchange**
   - A mechanism intended to ensure the identity of an entity by means of information exchange

6. **Traffic Padding**
   - The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

7. **Routing Control**
   - Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected

8. **Notarization**
   - The use of a trusted third party to assure certain properties of a data exchange.

1.3.2 Pervasive Security Mechanisms:

Mechanisms that are not specific to any particular OSI security service or protocol layer

1. **Trusted Functionality**
   - That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
2. **Security Label**
   - The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
3. **Event Detection**
   - Detection of security-relevant events
4. **Security Audit Trail**
   - Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities

5. Security Recovery

- Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

- **Relationship between Security Attacks and Security Services**

Security Services	Security Attacks					
	Release of Message Contents	Traffic Analysis	Masquerade	Replay	Modification of Messages	Denial of Services
Peer Entity Authentication			√			
Data Origin Authentication			√			
Access Control			√			
Traffic flow confidentiality		√				
Confidentiality	√					
Data Integrity				√	√	
Non- repudiation			√			
Availability						√

- **Relationship between Security Attacks andSecurity Mechanisms**

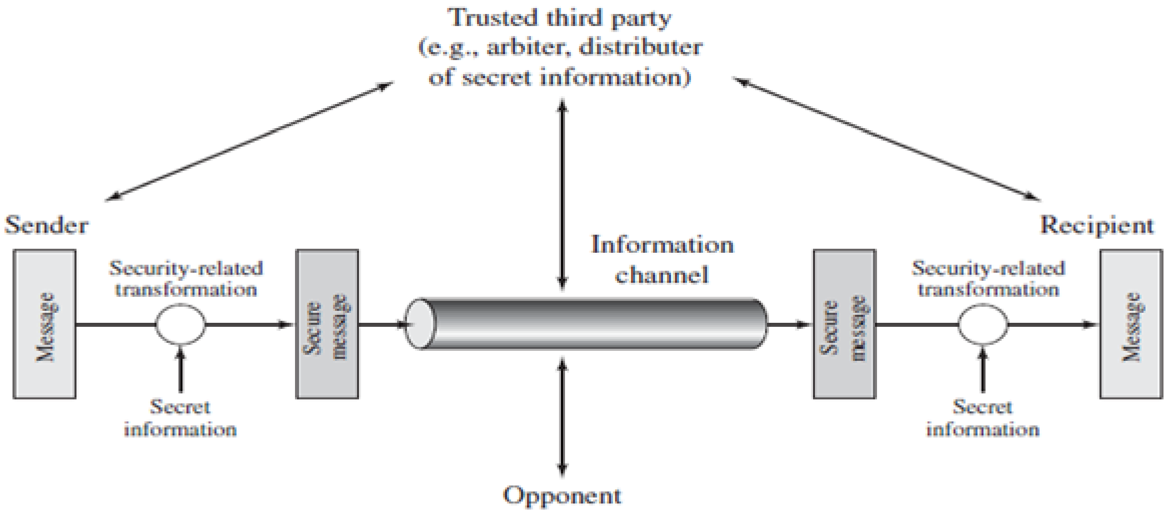
Security Services	Security Attacks					
	Release of Message Contents	Traffic Analysis	Masquerade	Replay	Modification of Messages	Denial of Services
Peer Entity Authentication			√			
Data Origin Authentication			√			
Access Control			√			
Traffic flow confidentiality		√				
Confidentiality	√					
Data Integrity				√	√	
Non- repudiation			√			
Availability						

Relationship between Security Services and Security Mechanisms

Security Services	Security Mechanisms
Data Confidentiality	Encipherment and Routing Control
Data Integrity	Encipherment, digital signature and data integrity
Authentication	Encipherment, digital signature and authentication exchange
Non-repudiation	digital signature, data integrity and authentication exchange
Access Control	Access control mechanisms

1.4 A MODEL FOR INTERNETWORK SECURITY

- A message is to be transferred from one party to another across some sort of Internet service.
- The two parties, who are the principals in this transaction, must cooperate for the exchange to take place.
- A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols by the two principals



- All the techniques for providing security have two components:
  - i. A security-related transformation on the information to be sent
  - ii. Some secret information shared by the two principals

1.5 NON CRYPTOGRAPHIC PROTOCOL VULNERABILITIES

1.5.1 DOS

- ➢ The main purpose of Dos attack is to consume the resources of its victim to the point where it crawls to halt. An attacker may, for example, waste the computational power of its victim by inducting it to perform time-consuming cryptographic operations. Such operations are performed in setting up a security association using the IPSec protocol discussed in chapter 13. The attacker may also attempt to exhaust the memory of its victim or saturate its victim’s access links to the internet. Dos attacks shot into prominence after several such attacks were launched on the websites of Amazon,Yahoo,eBay,etc...,in feburary 2000.

- We further highlight a number of Dos attack scenarios. Typically, a victim is flooded with packets that elicit some kind of response. Examples include the following:

- (1)An attacker sends thousands of TCP packets to its victim with the SYN flag set. The victim thinks that these are legitimate requests for TCP connection establishment (the first message of the three-way handshake).In response to each request, the victim reserves buffer space. Eventually, the victim’s communication link and/or memory are exhausted. This is one of the most common Dos attacks and is referred to as a SYN flood.

- (2)An attacker sends a large number of UDP packets to non-listening ports on the victim. This causes the victim to respond with an ICMP “Host unreachable” message for each packets that its receives.

- (3)An attacker sends a very large number of ICMP”Echo Request” messages to the victims network. The destination IP address of these packets is the special broadcast address of the network, while the source IP address is the address of the victim. This causes the victim be inundated with: Echo Reply” messages form each host on its network. This is referred to as a *Smurf Attack.*

- ***Impact of SYN flooding***

- The TCP SYN flooding attack exploits a stateful nature of the three way hand shake of the TCP protocol, where in buffer space is reserved for each incoming connection request. The victim responds by sending a packet with a SYN and ACK flag set. However, the attacker typically uses a spoofed IP source address. So, the SYN + ACK message from the victim, is sent to a non existing or unsuspecting machine. In either case, the victim does not receive the third message – an ACK. The victim times out and resends the SYN +ACK. The timeout period and total number of retries are dependent on the operating system running on the victim’s machine.

1.5.2 DDOS

- To magnify the impact of the above attacks, the perpetrator may distribute the sources of the attack. A distributed DoS is also harder to detect compared to a DoS attack emanating from a single source. In a DDos attack, the brain behind the attack scans the internet to find the multiple vulnerable hosts called handlers and compromises them each handler .Each handler, in turn recruits many agents or zombies to launch the attack.

- Having multiple levels of attackers mean that more zombies can be co-opted thus amplifying the attack. For example, the controller may recruit 1000 handlers. If each handler controls 500 zombies, then we have a total of 500,000 zombies. The zombies are injected with the code that sends attack packets to the victim in a coordinated fashion to overwhelm it. In addition, the source IP addresses are spoofed to obscure the source of the attacks.

- A SYN flood is easy to launch and can have devastating consequences. We next quantity the impact of such an attack on the victims network bandwidth and on memory exhaustion.

- The following parameters are specific to the OS and communication link at the victim:

  l=communication bandwidth of the victims link.

  B=maximum number of buffers reserved for TCP connections

  T=maximum amount of time that a buffer can be reserved for a half-open TCP connection

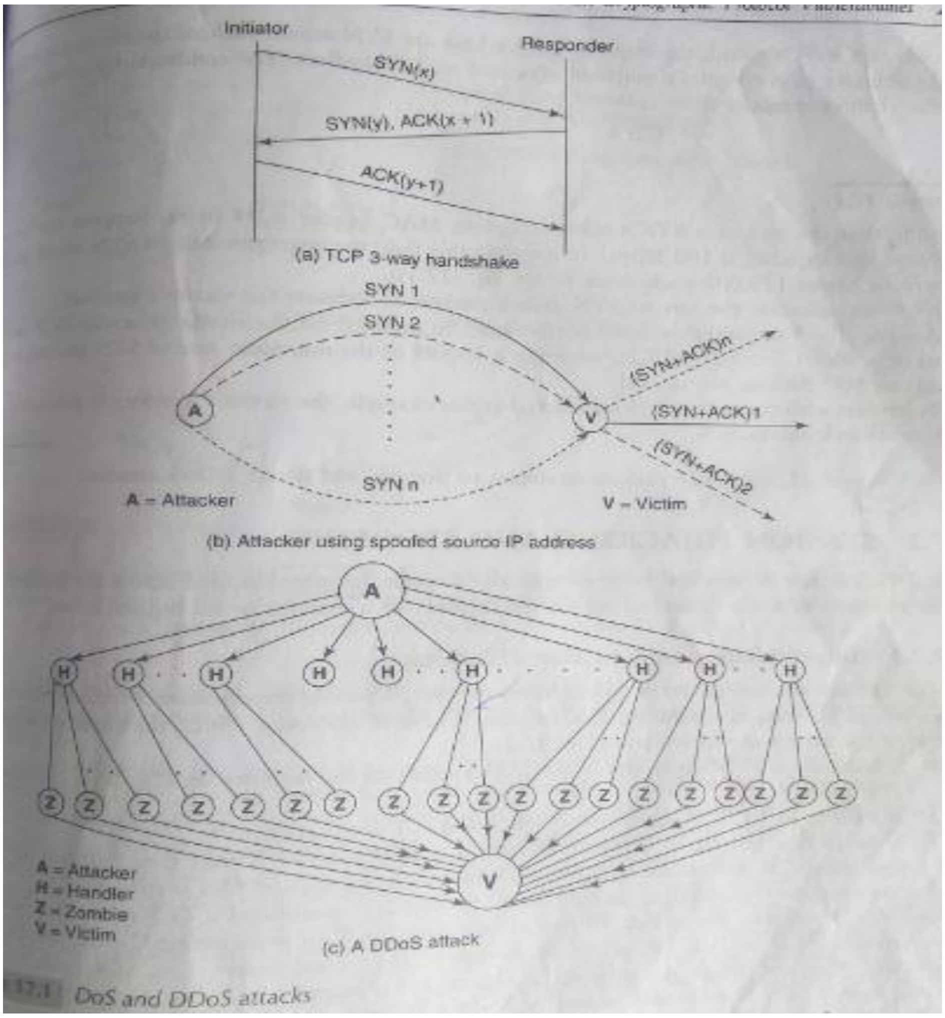
- The following variables characterize the attack:

  r=aggregate rate at which the victim receives SYN attack packets from the attack sources.

  P=SYN attack packet size.

- The flood of TCP SYN attack packets will saturate the victim's link if the following inequality is satisfied

$$r * p \geq l$$



(a) TCP 3-way handshake

(b) Attacker using spoofed source IP address

(c) A DDoS attack

17.1 DoS and DDoS attacks

1.5.3 Session hijacking and spoofing:

The DoS Attack is launched by geographically dispersed zombies located across the internet. Our next attack is typically launched within the confines of a computer or an organization.

I) Impersonation and Session Hijacking:

Kevin Mitnick devised an attack with in an attacker, X, Could impersonate a trusted client, C, to a server, S. The attack assumes that C, S, and X have IP addresses within the same network.

Step 1. X launches a SYN flood attack on C. This exhausts the memory on C’s station allocated for TCP buffer.

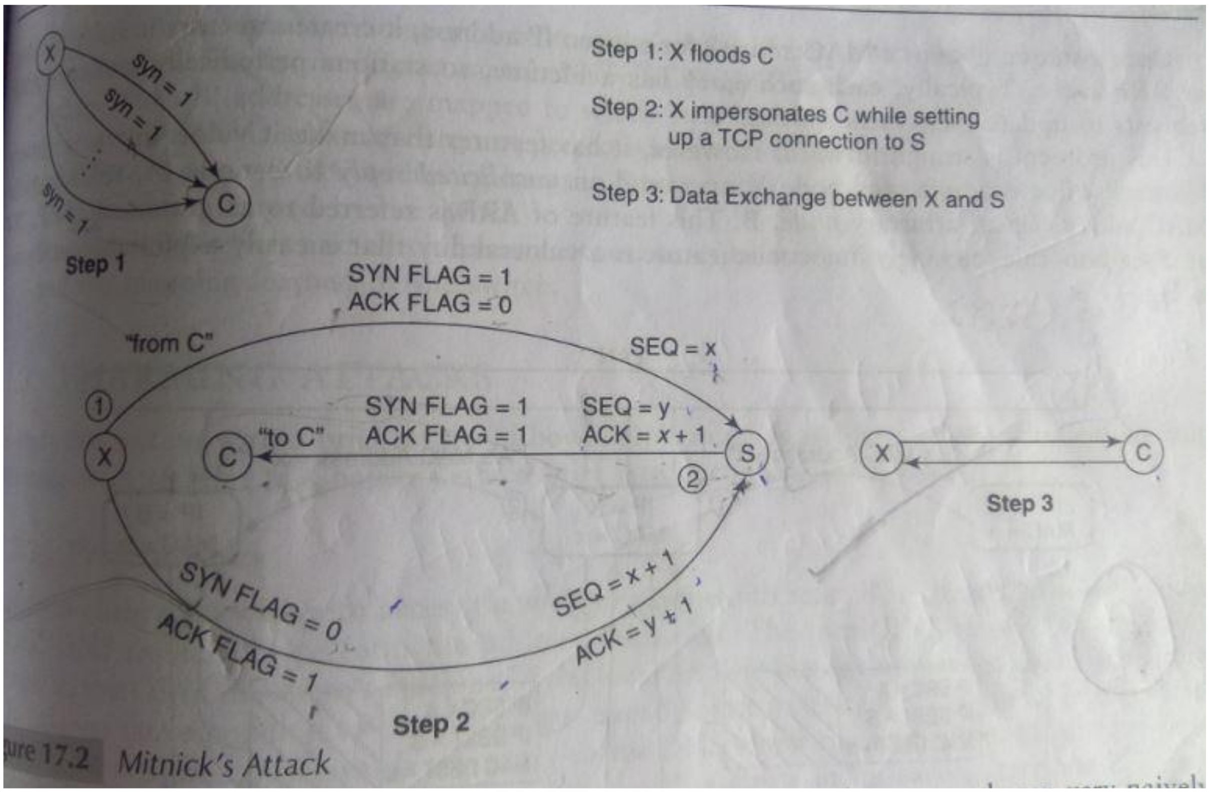
Step 2. X then spoofs C’s IP address and sets up a TCP connection to S.

Step 3. S thinks it is talking to C when, in fact, it is talking to X. X may then perform operations that only C is authorized.

- In Step2 X establishes a TCP connection with S. X spoofs C’s IP address.
- In TCP Connection establishment, the second packet is an ACK packet from the responder, S, to the presumed initiator, C. This packet is received by C but is ignored

because C is reeling from a SYN flood attack caused by X (step1) during which it ignores all incoming packets.

- To succeed, X will have to complete the three-way handshake that it initiated in step2. For this purpose it need to reed and increment the initial sequence number chosen by S. This number is denoted by y in the figure and include in the SYN+ACK response packet send by S to C. X can sniff this packet if it is on the same LAN as S.
- If X and S are in different LANs. In many early implementations of TCP, the initial sequence numbers were chosen very naively. For example, a station would increment y by a fixed amount for each new connection established by/to it. So, the initial sequence number chosen by S in the immediate past would be y-a, y-2a, y-3a... etc. In reverse chronological order.
- Once possibility is for X to repeatedly attempt to connect to C just to determine the algorithm used in choosing the initial sequence number. This could be done just before step2.
- The above attack succeeds because the server authenticates a client based on (1) the client's IP address and (2) the "ACK #" in the third message of the three-way handshake.
- The probability of success of this attack will be greatly reduced if initial sequence numbers are chosen randomly.
- If X is unable to sniff the second packet in the three-way handshake AND if the initial sequence number is truly random , it is hard for X to complete the three-way handshake so that X would not impersonate C.
- An attack similar to the above can be mounted to hijack a TCP connection. The difference between Mitnick's attack and TCP connection hijack is that, in the later two parties (say C and S) are already communicating. By flooding one of the parties (say C) and spoofing its address, an attacker may be able to continue the conversation with the other party, S. As before, the attacker makes S believe that it is talking to C.



ure 17.2 Mitnick's Attack

II) ARP Spoofing:

Address Resolution Protocol is used to resolve an IP address to a MAC address.

Consider two stations A and B on the same LAN. If A needs to send a packet to B, it not sufficient that A knows the IP address of B, A should also know B's MAC address.

For this purpose, A broadcasts an ARP query containing B's IP address. A station that has or knows B's MAC address responds directly to A.

Once a station obtains a MAC address for a given IP address, it creates an entry in its ARP table or ARP cache. Typically, each such cache has a lifetime, so stations periodically send out ARP requests to update their cache entries.

However, it has features that make it vulnerable to a verity of attacks. For example, any node X may send an unsolicited reply to node, A, regarding the MAC address of an arbitrary node, B. This feature of ARP is referred to as gratuitous ARP.

Consider an attacker, X, with IP address X, and MAC address, x.

It sends an unsolicited ARP response message to A containing the following: B's MAC address is x.

X also sends an unsolicited ARP response message to B containing the following: A's MAC address is x

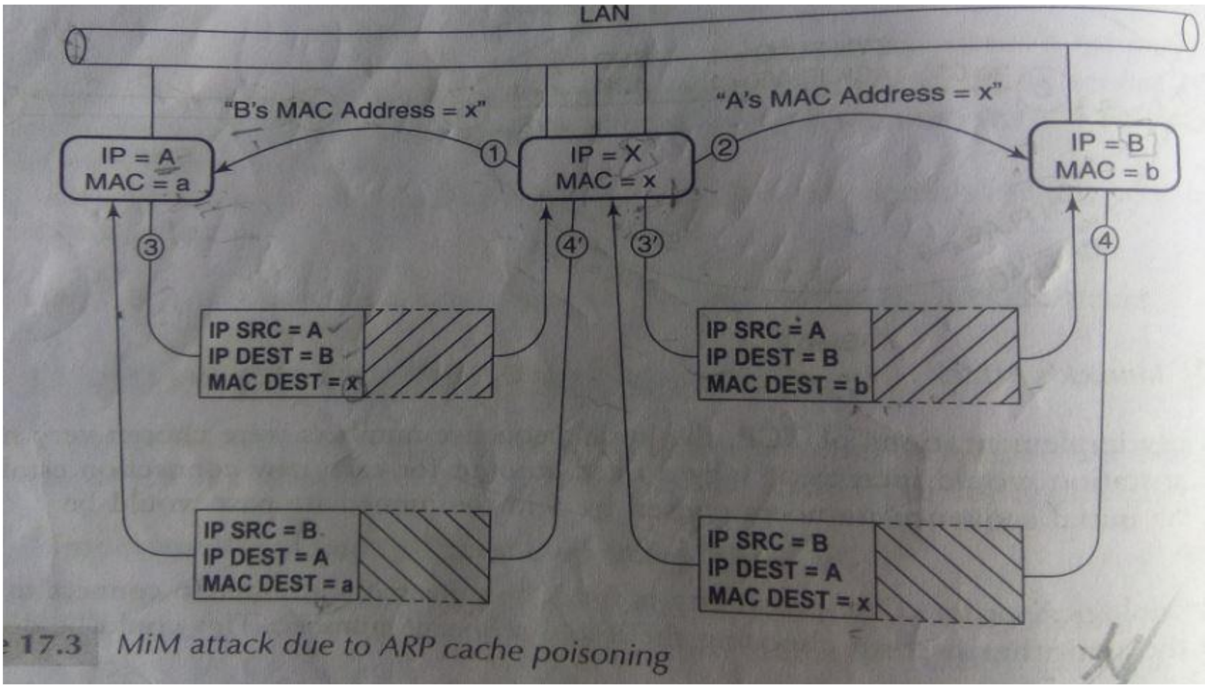
The unsolicited responses of X have created fake entries in the ARP cache of A and B. We say that their ARP caches have been poisoned.

Now, if A wishes to communicate with B, it will create a frame with destination MAC address =x. The LAN switch will forward this message to X. X may simply drop such frames thus choking off the connection from A to B. Alternatively, X may read and modify all such frames and then send them to B. Because B's cache has also poisoned, X will be able to launch a man-in-the-middle attack.

Fortunately, there are solutions to the problem of ARP spoofing. One possibility is to have only authenticated ARP responses. This might require Kerberos style infrastructure or PKI.

A more radical solution is to use static ARP caches, which ignores send by random machines. Finally, intelligent switches may be designed that

- Learn which IP addresses are mapped to which switch port.
- Learn which MAC addresses are mapped to which switch port.
- Monitor IP address/MAC address pairing in Ethernet frames and check for inconsistency with what has been learned by the switch.
- Examine ARP replies and check for any inconsistency between the address in the ARP reply and the mapping learned by the switch.



17.3 MiM attack due to ARP cache poisoning

ASSIGNMENT CUM TUTORIAL QUESTIONS

A. Objective Questions

1. Any action that compromises the security of information [ ]
   a. Security Attack b. Security Mechanism c. Security Service
2. A process that is designed to detect, prevent, or recover from a security attack. [ ]
   a.Security Mechanism b. Security Service

3. __________ attempts to learn or make use of information from the system but does not affect system resource [ ]

a. Passive Attack b. Active Attack

4. _______ attack attempts to alter system resources or affect their operation. [ ]

a. Passive Attack b. Active Attack

5. _______ takes place when one entity pretends to be a different entity [ ]

a. Masquerade b. Replay c. Modification of Message d. Denial of Service

6. _______ involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect [ ]

a. Masquerade b. Replay c. Modification of Message d. Denial of Service

7. _____ simply means that some portion of a legitimate message is altered [ ]

a. Masquerade b. Replay c. Modification of Message d. Denial of Service

8. _______ prevents or inhibits the normal use or management of communications facilities

a. Masquerade b. Replay c. Modification of Message d. Denial of Service

9. Message contents is released in ______ attack [ ]

a. release of message contents b. Denial of Service c. Traffic Analysis

10. ______ attack only traffic information is known [ ]

a. release of message contents b. Masquerade c. Traffic Analysis d. Replay

11. The protection of data from unauthorized disclosure is ______ [ ]

a. Data Confidentiality b. Access Control c. Authentication

12. A denial of service attack: [ ]

a) can erase an entire Web site

b) does not have to occur over a network

c) is an intentional attempt to overload a web server or website

d) all of the above

13. Authentication is done for [ ]

a) Conventional encryption

b) Scrambling data

c) Both a and b

d) None of the above

14. Authentication is: [ ]

a) Verification of user’s identification

b) Verification of data

c) Both a and b

d) None of the above

15. The process to discover plain text or key is known as: [ ]

a) Cryptanalysis

b) Crypto design

c) Crypto processing

d) Crypto graphic

16. Security mechanism is ensured in: [ ]

a) Detect attack

b) Prevent attack

c)Recover from attack

d) **All of the above**

17. In cryptography, what is cipher? [ ]

a) algorithm for performing encryption and decryption

b) encrypted message

c) both (a) and (b)
d) none of the mentioned

18. __________ enhances the security of the data processing systems and the information transfers of an organization [ ]
a)Security Attack b) Security Mechanism c) Security Service

19. Cryptanalysis is used [ ]
a) to find some insecurity in a cryptographic scheme
b) to increase the speed
c) to encrypt the data
d) none of the mentioned

20. When the firm's purpose for their information infrastructure is to make its data and information available to those who are authorized to use it, the firm is seeking the objective of: [ ]
a) confidentiality.
b) availability.
c) authorization.
d)integrity.

B. Descriptive Questions

1. What is meant by security attack? Explain different types of attacks with pictorial representation
2. Determine the security services required to counter various types of active and passive attacks.
3. Determine the security mechanisms required to provide various types of security services.
4. Draw the model of internetwork security and explain in detail.
5. Explain session hijacking and spoofing.
6. Differentiate passive and active attacks.
7. Define threat and attack. What is the difference between both? List some examples of attacks which have arisen in real world cases.
8. Write a short note on DDoS.