Loyola Institute of Technology & Science

Dept: CSE & IT
Sem: 07

Subject code: CS B792
Subject Name: CNS

WEEKLY TEST: 01

PART A (2x2 = 4 marks)

WT1.1 Compare passive and active attack. (April/May 2019)

WT1.2 Why is asymmetric cryptography bad for huge data? Specify the reason. (April/May 2018)

PART B (1x16 = 16 marks)

WT1.3 Write a note on different types of security attacks and services in detail.

(Nov/Dec 2019)

# CNS - Weekly Test-01

## Answer Key:

## PART A

WT 1.1

| | Passive attack | Active attack |
|---|---|---|
| 1. | * Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. | * Active attacks involve some modification of the data stream or the creation of a false stream. |
| 2. | Very difficult to detect | * Easy to detect. |
| 3. | The emphasis in dealing with passive attacks is on prevention rather than detection. | * It is quite difficult to prevent active attacks absolutely. |
| 4. | It does not affect the system | * It affects the system. |

NT 1.2

## Why is asymmetric cryptography bad for huge data

1. Size of cryptogram: symmetric encryption does not increase the size of the cryptogram (asymptotically), but asymmetric encryption does.

2. performance: on a modern cpu with hardware AES support, encryption or decryption speed is over 2000 megabyte / second (per core).

## 1.5 Types of Security Attacks

AU : Dec.-13,19

- An attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems.
- Security attacks are of two types : Passive attack and active attack

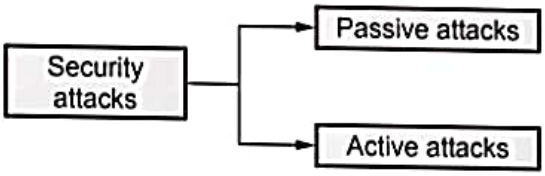


Fig. 1.5.1

### 1.5.1 Passive Attack

- Passive attacks are those, wherein the attacker indulges in eavesdropping on, or monitoring of data transmission. A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- The attacker aims to obtain information that is in transit. The term passive indicates that the attacker does not attempt to perform any modifications to the data.
- **Passive attacks** are of two types :
  1. Release of message contents 2. Traffic analysis
- **Release of message content** is shown in Fig. 1.5.2. A telephone conversation, an electronic mail message and a transferred file may contain sensitive or confidential information we would like to prevent an opponent from learning the content of these transmissions.

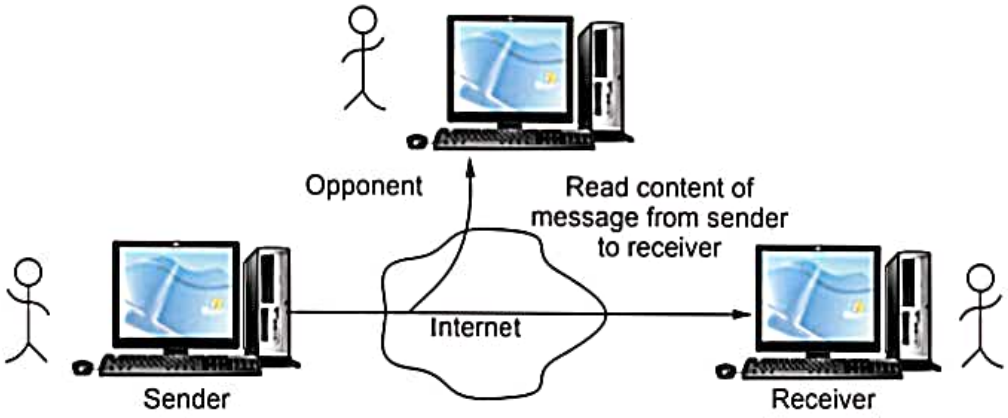


Fig. 1.5.2 Release of message contents

- **Traffic analysis :** Mask the contents of message so that opponents could not extract the information from the message. Encryption is used for masking Fig. 1.5.3 shows the traffic analysis.
- Passive attacks are very difficult to detect because they do not involve any alternation of data. It is feasible to prevent the success of attack, usually by means of encryption.

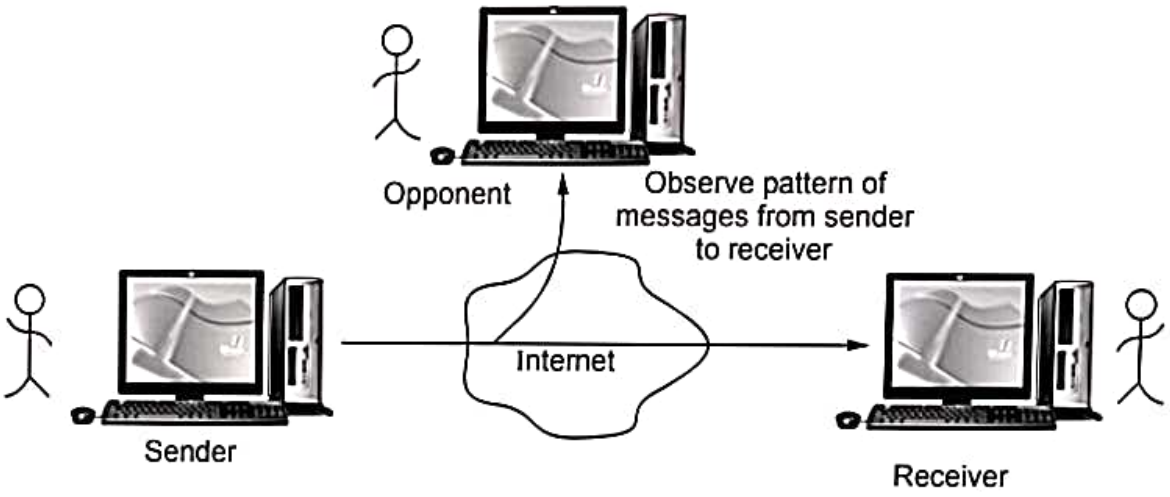


**Fig. 1.5.3 Traffic analysis**

## 1.5.2 Active Attack

- Active attacks involve some modification of the data stream or the creation of a false stream. These attacks can not be prevented easily.
- Active attacks can be subdivided into four types :
  1. Masquerade
  2. Replay
  3. Modification of message
  4. Denial of service

### 1. Masquerade

- It takes place when one entity pretends to be a different entity. Fig. 1.5.4 shows masquerade.

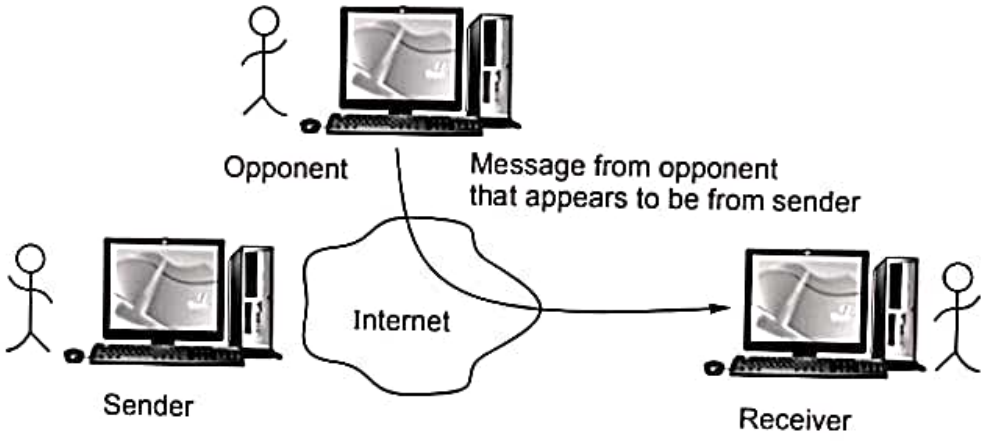


**Fig. 1.5.4 Masquerade**

- **For example :** Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

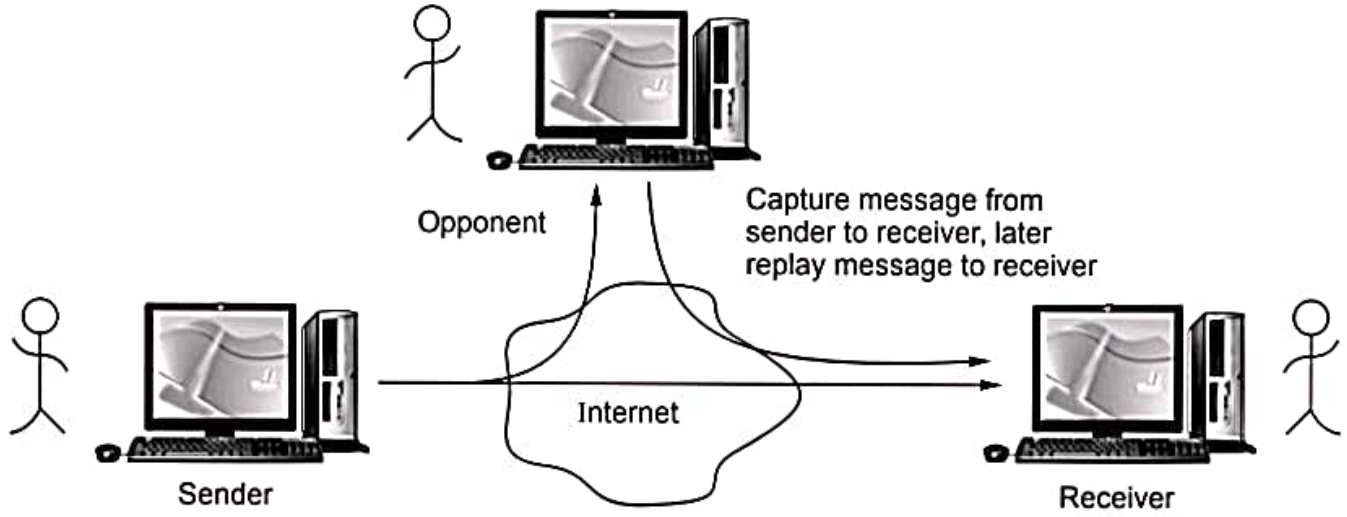


**Fig. 1.5.5 Replay**

### 3. Modification of message

- It involves some change to the original message. It produces an unauthorized effect. Fig. 1.5.6 shows the modification of message.

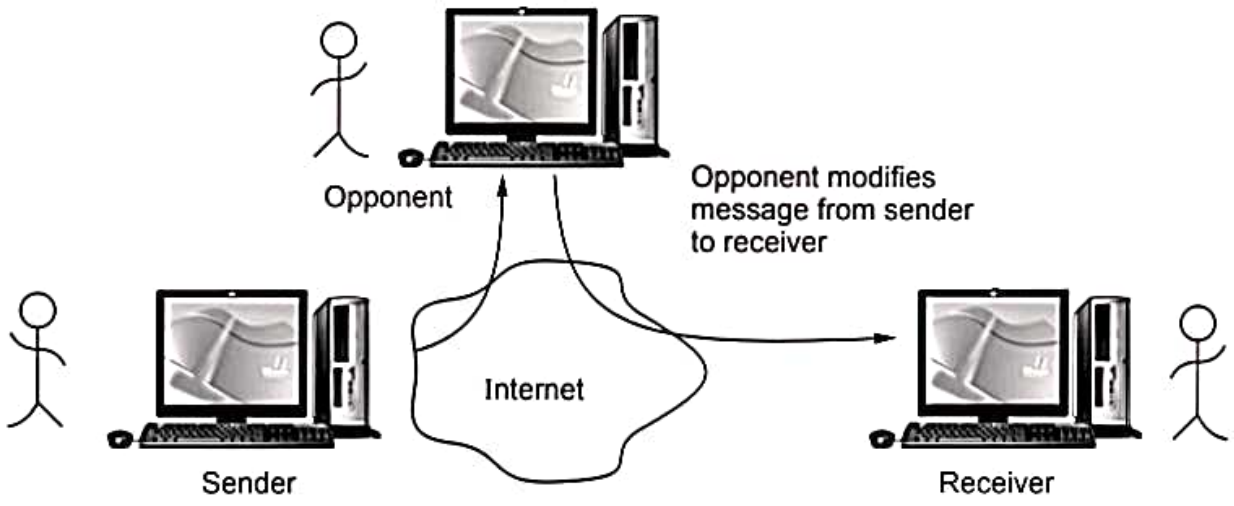


**Fig. 1.5.6 Modification of message**

- For example, a message meaning "Allow Rupali Dhotre to read confidential file accounts " is modified to mean "Allow Mahesh Awati to read confidential file accounts".

### 4. Denial of service

- Fabrication causes Denial Of Service (DOS) attacks.
- DOS prevents the normal use or management of communications facilities.

- Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.
- Fig. 1.5.7 shows denial of service attack.

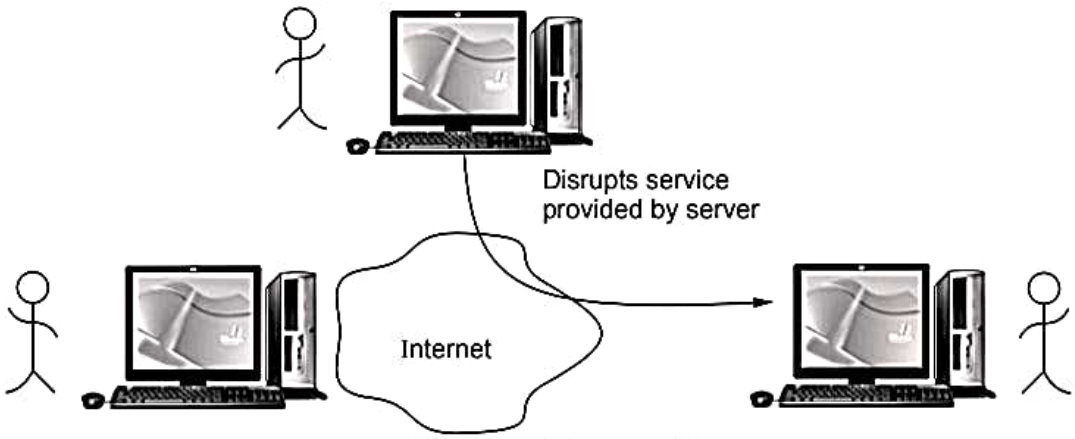


**Fig. 1.5.7 Denial of service**

- It is difficult to prevent active attack because of the wide variety of potential physical, software and network vulnerabilities.
- The first type of DOS attacks were single source attacks, meaning that a single system was used to attack another system and cause something on that system to fail. SYN flood is the most widely used DOS attack.
- Fig. 1.5.8 shows the SYN flood DOS attack.

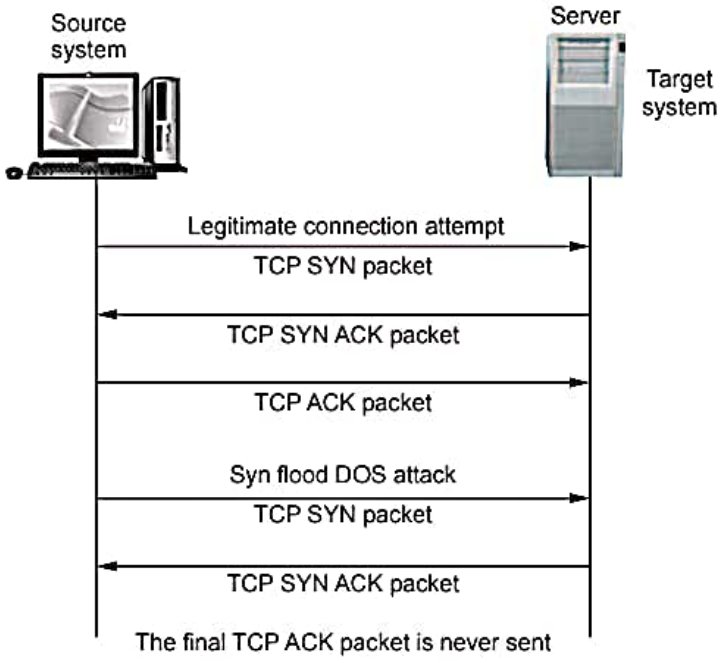


**Fig. 1.5.8 SYN flood DOS attack**

- Source system sends a large number of TCP SYN packets to the target system. The SYN packets are used to begin a new TCP connection.

public key is distributed through a secure channel.

**University Questions**

1. *What are the different types of attacks ? Explain.* **AU : Dec.-13, Marks 8**
2. *Write a note on different types of security attacks and services in detail.* **AU : Dec.-19, Marks 13**

## 1.6 Security Services

- X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.
- X.800 divides security services into five different categories.
  1. Authentication
  2. Access control
  3. Data confidentiality
  4. Data integrity
  5. Nonrepudiation

### 1. Authentication

- Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In public and private computer network, authentication is commonly done through the use of login passwords.
- Two specific authentication services are defined in X.800 :
  a. Peer entity authentication
  b. Data origin authentication
- **Peer entity authentication** used in association with a logical connection to provide confidence in the identity of the entities connected.
- Data origin outhentication enables the recepient to verify that the message have not been tempered in transit (data integrity) and they originally from expected sender (authenticity).
- **Data origin authentication** does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.

### 2. Access control

- It is the ability to limit and control the access to host systems and applications via communications links.
- This service controls who can have access to a resource.

### 3. Data confidentiality

- Confidentiality is the concealment of information or resources. It is the protection of transmitted data from passive attacks.
- Confidentiality is classified into
  1. **Connection confidentiality :** The protection of all user data on a connection.
  2. **Connectionless confidentiality :** The protection of all user data in a single data block.
  3. **Selective field confidentiality :** The confidentiality of selected fields within the user data on a connection or in a single data block.
  4. **Traffic flow confidentiality :** The protection of the information that might be derived from observation of traffic flows.

### 4. Data integrity

- Integrity can apply to a stream of messages a single message or selected fields within a message.
- Modification causes loss of message integrity.
- Data integrity can be classified as
  1. Connection integrity with recovery
  2. Connection integrity without recovery
  3. Selective field connection integrity
  4. Connectionless integrity
  5. Selective field connectionless integrity
- 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 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.
- Connectionless integrity provides for the integrity of a single connectionless data block and may take the form of detection of data modification.

### 5. Nonrepudiation

- Nonrepudiation prevents either sender or receiver from denying a transmitted message.
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message.
- When a message is received, the sender can prove that the alleged receiver in fact received the message.