SUBJECT CODE : 317530

As per Revised Syllabus of

SAVITRIBAI PHULE PUNE UNIVERSITY

T.E. (AI and DS) Semester - VI

CYBER SECURITY

Vilas S. Bagad

M.E. (E&Tc), Microwaves

M.M.S. (Information systems)

Faculty, Institute of Telecommunication Management,

Ex-Faculty Sinhgad College of Engineering,

Pune.

Iresh A. Dhotre

M.E. (Information Technology)

Ex-Faculty, Sinhgad College of Engineering,

Pune.

TECHNICAL PUBLICATIONS

SINCE 1993

An Up-Thrust for Knowledge

TABLE OF CONTENTS

Unit I

Unit II

Unit III

Unit IV

Unit V

Unit VI

Unit I

1 Introduction

Syllabus

Introduction, Elements of Information Security, Security Policy, Techniques, Steps, Categories, Operational Model of Network Security, Basic Terminologies in Network Security. Threats and Vulnerability, Difference between Security and Privacy.

Contents

1.1 Introduction

- The history of information security begins with computer security.
- Network security, to protect networking components, connections, and contents.
- Information security to protect the confidentiality, integrity and availability of information assets, whether in storage, processing or transmission.
- Physical security consists of all mechanisms used to ensure that physical access to the computer systems and networks is restricted to only authorize users.
- Data security is the science and study of methods of protecting data from unauthorized disclosure and modification.
- Data and information security is about enabling collaboration while managing risk with an approach that balances availability versus the confidentiality of data.
- Security is required because the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means.
- Network security measures are needed to protect data during their transmission.
- Following are the examples of security violations.

1. User A transmits a sensitive information file to user B. The unauthorized user C is able to monitor the transmission and capture a copy of the file during its transmission.
2. A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.
3. While transmitting the message between two users, the unauthorised user intercepts the message, alters its contents to add or delete entries and then forwards the message to destination user.

1.2 Elements of Information Security

- Security goals are as follows :

1. Confidentially
2. Integrity
3. Availability

1. Confidentiality

- Confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones.
- Sensitive information should be kept secret from individuals who are not authorized to see the information.
- Underpinning the goal of confidentiality are authentication methods like user-IDs and passwords that uniquely identify a data system's users, and supporting control methods that limit each identified user's access to the data system's resources.

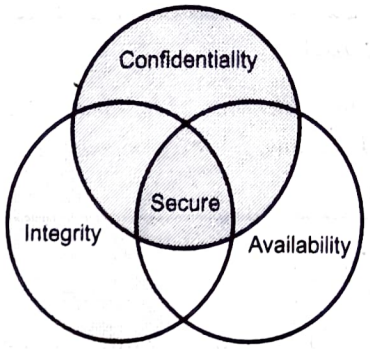

Fig. 1.2.1 Relationship between confidentiality integrity and availability

- Confidentiality is not only applied to storage of data but also applies to the transmission of information.
- Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.

2. Integrity

- Integrity refers to the trustworthiness of information resources.
- Integrity should not be altered without detection.
- It includes the concept of "data integrity" namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity.
- It also includes "origin" or "source integrity" that is, the data actually came from the person or entity you think it did, rather than an imposter.
- Integrity ensures that information is not changed or altered in transit. Under certain attack models, an adversary may not have to power to impersonate an authenticated party or understand a confidential communication, but may have the ability to change the information being transmitted.

- On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.

3. Availability

- Availability refers, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all.
- Availability means that people who are authorized to use information are not prevented from doing so. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure.
- Almost all modern organizations are highly dependent on functioning information systems. Many literally could not operate without them.
- Availability, like other aspects of security, may be affected by purely technical issues (e.g. a malfunctioning part of a computer or communications device), natural phenomena (e.g. wind or water), or human causes (accidental or deliberate).
- For example, an object or service is thought to be available if
  i. It is present in a usable form.
  ii. It has capacity enough to meet the services needs.
  iii. The service is completed an acceptable period of time.
- By combining these goals, we can construct the availability. The data item, service or system is available if
  i. There is a timely response to our request.
  ii. The service and system can be used easily.
  iii. Concurrency is controlled.
  iv. It follows the fault tolerance.
  v. Resources are allocated fairly.

Review Questions

1. *List and explain various elements of information security.*
2. *What are the elements of information security ? Explain in brief.*

1.3 Security Policy

- Security policy is a definition of what it means to be secure for a system, organization or other entity.
- For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.
- A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur.
- A security policy must identify all of a company's assets as well as all the potential threats to those assets. Company employees need to be kept updated on the company's security policies. The policies themselves should be updated regularly as well.
- 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.
- A security policy establishes what must be done to protect information stored on computers. A well written policy contains sufficient definition of "what" to do so that the "how" can be identified and measured or evaluated.
- Security to the information can be provided by using internal approach and external approach.
- Internal approach : Protect from internal attacks by using necessary measures.
- External approach : Protect from outside attacks.
- In general, a good security policy does the following :
  1. Communicates clear and concise information and is realistic;
  2. Includes defined scope and applicability;
  3. Consistent with higher-level policy and guidance;
  4. Open to change based on new risks and vulnerabilities;
  5. Identifies the areas of responsibility for users, administrators and management;
  6. Provides sufficient guidance for development of specific procedures;
  7. Balances protection with productivity;
  8. Identifies how incidents will be handled.

Review Question

1. *What are the security approaches used to implement security policy ?*

1.4 Techniques

- Commonly used security techniques are as follows :

1. Encryption : Used to protect information and data. It is cryptography techniques. Different types of encryption are used for providing security.
2. Access control : Access to data or computer is controlled by using some mechanism. Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.
3. Data backup : Data backup refers to saving additional copies of your data in separate physical or virtual locations from data files in storage. If you lose your data, recovery could be slow, costly or impossible. It is important that you secure, store and backup your data on a regular basis.
4. Firewall : Firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
5. Antivirus software : Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities as they happen, as well as system scans that monitor device and system files looking for possible risks.
6. Intrusion detection systems : IDS can offer protection from external users and internal attackers. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.
7. Series of confidence : It ensure that all software use has been authentic.

Review Questions

1. *List and explain different security techniques.*
2. *What are various security technique used in cyber security.*

1.5 Steps

- Steps in providing security to information or computer system includes following steps :

1. Assets : The information on the server was secured with appropriate security controls. Although the hacker was able to gain access only to the information with a lower level of protection, the breach had a huge impact on the organization. There are several good reasons to classify information. Not all data has the same value to an organization.
2. Risks : A successful information risk management programs starts at the top of the organization.
3. Protections : To find solutions for the protection of the information.
4. Tools and techniques : Select proper tools and techniques for the protection of information.
5. Priorities : Decide the order of the security tools and techniques for the protection of the information.

1.6 Categories

- Various categories of computer security are :
  1. Cryptography
  2. Data security
  3. Computer security
  4. Network security
- Cryptography is data encryption and decryption.
- Data security is ensuring safe data from modification and corruption.
- Computer security is formal description of security policies. It includes protection, preventation and detection of unauthorized use of computer.
- Network security is protection of data on the network during transmission or sharing.

Review Questions

1. *List and explain categories of information security.*
2. *What are the categories of computer security.*

1.7 Operational Model of Network Security

- A message is to be transferred from source to destination across some sort of internet. Both the sides must cooperate for the exchange of the data.
- A logical information channel is established by defining a route through the internet from source to destination.
- All the techniques for providing security have two components :
  1. A security related transformation on the information to be sent.
  2. Some secret information shared by the two principles, it is hoped, unknown to the opponent.
- Fig. 1.7.1 shows the network security model.
- A trusted third party is needed to achieve secure transmission.
- Basic tasks in designing a particular security service.
  1. Design an algorithm for performing the security related transformation.
  2. Generate the secret information to be used with the algorithm.
  3. Develop methods for the distribution and sharing of the secret information.
  4. Specify a protocol to be used by the two principles that makes use of the security algorithm and the secret information to achieve a particular security service.

Review Questions

1. *Draw and explain operational model of network security.*
2. *Draw and explain operational model of security.*
3. *Explain operational model of network security.*

1.8 Basic Terminologies in Network Security

- Basic terminology used for security purposes are as follows :
  - a. **Cryptography :** The art or science encompassing the principles and methods of transforming an plaintext message into one that is unintelligible and then retransforming that message back to its original form.
  - b. **Plaintext :** The original message.
  - c. **Ciphertext :** The transformed message produced as output, It depends on the plaintext and key.
  - d. **Cipher :** An algorithm for transforming plaintext message into one that is unintelligible by transposition and/or substitution methods.
  - e. **Key :** Some critical information used by the cipher, known only to the sender and receiver.
  - f. **Encipher (encode) :** The process of converting plaintext to ciphertext using a cipher and a key.
  - g. **Decipher (decode) :** The process of converting ciphertext back into plaintext using a cipher and a key.

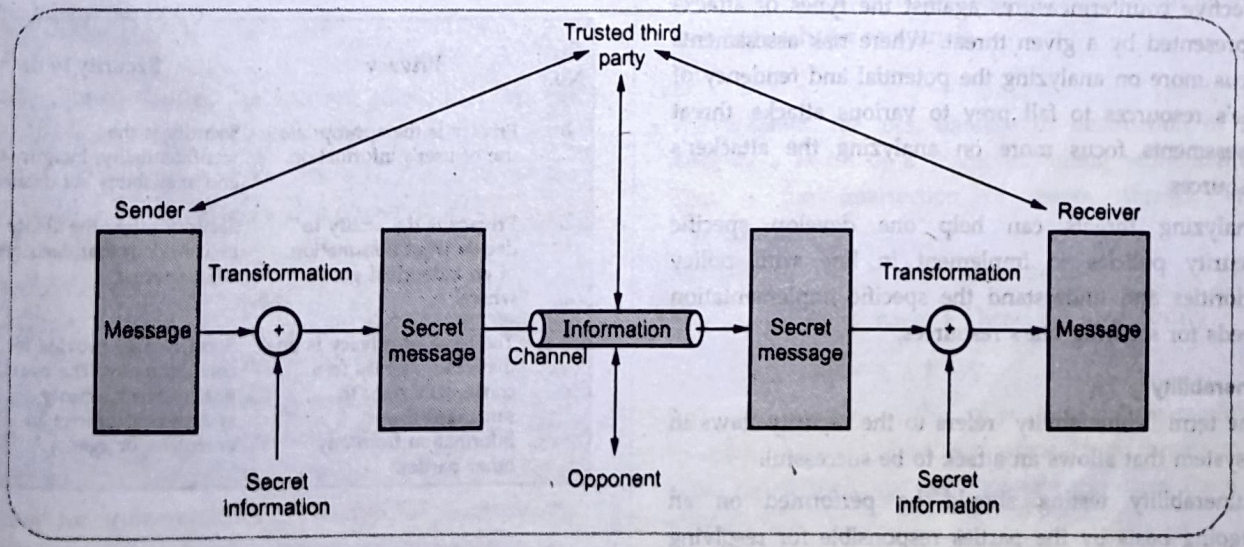

Fig. 1.7.1 Network security model

h. **Cryptanalysis** : The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key. Also called **code-breaking.** Cryptanalysis is to break an encryption. Cryptanalyst can do any or all of the three different things :

1. Attempt to break a single message.
2. Attempt to recognize patterns in encrypted messages, in order to be able to break subsequent ones by applying a strainghtforward decryption algorithm.
3. Attempt to find general weakness in an encryption algorithm, without necessarily having intercepted any messages.

i. **Cryptology** : Both cryptography and cryptanalysis.

j. **Code** : An algorithm for transforming an plaintext message into an unintelligible one using a code-book.

1.9 Threats and Vulnerability

Threat

- The term "threat" refers to the source and means of a particular type of attack.
- A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of threat.
- Penetration testing exercises are substantially focused on assessing threat profiles, to help one develop effective countermeasures against the types of attacks represented by a given threat. Where risk assessments focus more on analyzing the potential and tendency of one's resources to fall prey to various attacks, threat assessments focus more on analyzing the attacker's resources.
- Analyzing threats can help one develop specific security policies to implement in line with policy priorities and understand the specific implementation needs for securing one's resources.

Vulnerability

- The term "vulnerability" refers to the security flaws in a system that allows an attack to be successful.
- Vulnerability testing should be performed on an ongoing basis by the parties responsible for resolving such vulnerabilities, and helps to provide data used to identify unexpected dangers to security that need to addressed.
- Such vulnerabilities are not particular to technology they can also apply to social factors such as individu authentication and authorization policies.
- Testing for vulnerabilities is useful for maintainin ongoing security, allowing the people responsible f the security of one's resources to respond effectively new dangers as they arise. It is also invaluable f policy and technology development, and as part of technology selection process; selecting the rig technology early on can ensure significant savings i time, money, and other business costs further dow the line.
- Understanding the proper use of such terms i important not only to sound like you know wha you're talking about, nor even just to facilitate communication. It also helps develop and employ good policies.
- The specificity of technical jargon reflects the way experts have identified clear distinctions betwee practical realities of their fields of expertise, and ca help clarify even for oneself how one should addres the challenges that arise.
- Other examples of vulnerability include these :
  1. A weakness in a firewall that lets hackers get into a computer network
  2. Unlocked doors at businesses
  3. Lack of security cameras

1.10 Difference between Security and Privacy

Sr. No.	Privacy	Security
1.	Privacy is the appropriate use of user's information.	Security is the "confidentiality, integrity and availability" of data.
2.	Privacy is the ability to decide what information of an individual goes where.	Security offers the ability to be confident that decisions are respected.
3.	The issue of privacy is one that often applies to a consumer's right to safeguard their information from any other parties.	Security may provide for confidentiality. The overall goal of most security system is to protect an enterprise or agency.

4.	It is possible to have poor privacy and good security practices.	However, it is difficult to have good privacy practices without a good data security program.
5.	For example, if user make a purchase from XYZ Company and provide them payment and address information in order for them to ship the product, they cannot then sell user's information to a third party without prior consent to user.	The company XYZ uses various techniques (Encryption, Firewall) in order to prevent data compromise from technology or vulnerabilities in the network.

1.11 Security Attacks

- Computer based systems have three valuable components : **Hardware, software and data.**
- Securities of these components are evaluated in terms of vulnerability, threats, attacks and control.
- An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

Asset

- Asset means people, property and information.
- People may include employees and customers along with other invited persons such as contractors or guests.
- Property assets consist of both tangible and intangible items that can be assigned a value.
- Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records and many other intangible items.

Vulnerability

- Vulnerability refers to the security flaws in a system that allows an attack to be successful.
- Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. Vulnerability is a weakness or gap in our protection efforts.
- Vulnerability testing should be performed on an ongoing basis by the parties responsible for resolving such vulnerabilities, and helps to provide data used to identify unexpected dangers to security that need to be addressed.
- Testing for vulnerabilities is useful for maintaining ongoing security, allowing the people responsible for the security of one's resources to respond effectively to new dangers as they arise.
- **Example** : In design, implementation or procedure, that might be exploited to cause loss or harm.

Threat

- Anything that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. A threat is what we're trying to protect against.
- Threat refers to the source and means of a particular type of attack.
- A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of threat.
- A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.
- Penetration testing exercises are substantially focused on assessing threat profiles, to help one develop effective countermeasures against the types of attacks represented by a given threat.
- Where risk assessments focus more on analyzing the potential and tendency of one's resources to fall prey to various attacks, threat assessments focus more on analyzing the attacker's resources.
- Analyzing threats can help one develop specific security policies to implement in line with policy priorities and understand the specific implementation needs for securing one's resources.
- Threats come in many forms, depending on their mode of attack. From viruses to trojans, spyware and bots, threats have evolved into sophisticated programs intended to harm computers.

Risk

- The potential for loss, damage or destruction of an asset as a result of a threat exploiting vulnerability. Risk is the intersection of assets, threats, and vulnerabilities.
- The formula used to determine risk is

$$\text{Risk} = \text{Asset} + \text{Threat} + \text{Vulnerability}$$

$$R = A + T + V$$

- Risk is a function of threats exploiting vulnerabilities to obtain damage or destroy assets. Thus, threats may exist, but if there are no vulnerabilities then there is little/no risk.

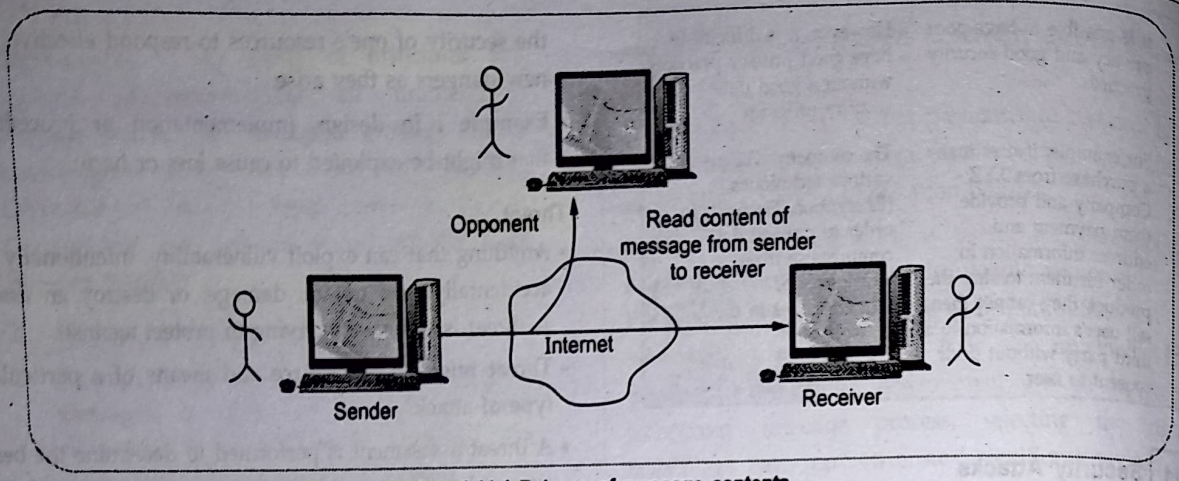

Fig. 1.11.1 Release of message contents

- Similarly, you can have vulnerability, but if you have no threat, then you have little/no risk.

Control

- Control is used as proactive measure. Control is a action, device, procedure, or technique that removes or reduces a vulnerability.
- A threat is blocked by control of vulnerability.
- Interception, interruption, modification and fabrication are the system security threats.

1.11.1 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 th data.
- **Passive attacks** are of two types :
  1. Release of message contents
  2. Traffic analysis
- **Release of message content** is shown in Fig. 1.11.1. telephone conversation, an electronic mail message an a transferred file may contain sensitive or confidenti information we would like to prevent an opponen from learning the content of these transmissions.
- **Traffic analysis :** Mask the contents of message so tha opponents could not extract the information from th message. Encryption is used for masking Fig. 1.11 shows the traffic analysis.
- Passive attacks are very difficult to detect because the do not involve any alternation of data. It is feasible t prevent the success of attack, usually by means o encryption.

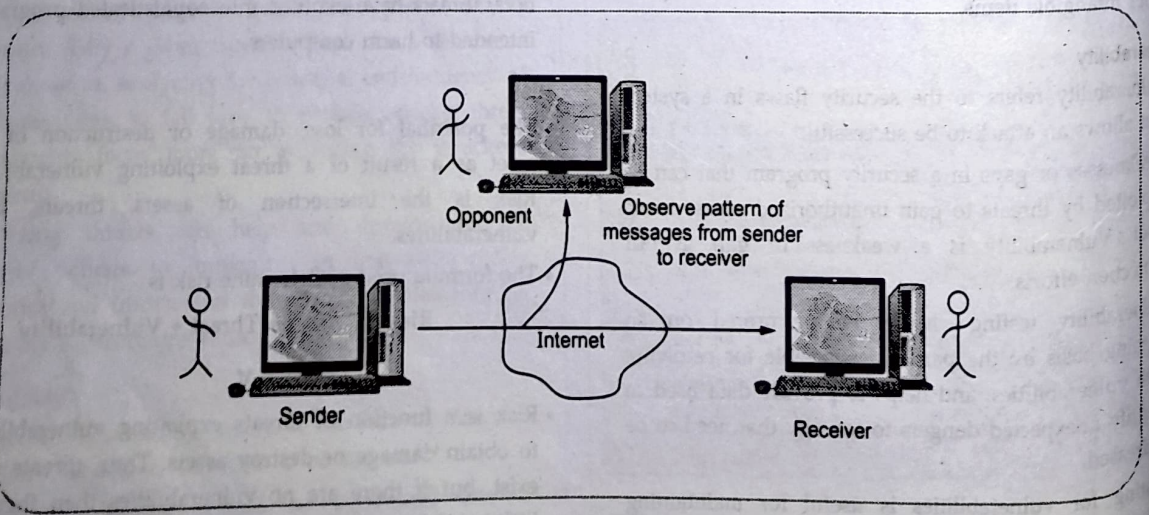

Fig. 1.11.2 Traffic analysis

1.11.2 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. 1.11.3 shows masquerade.

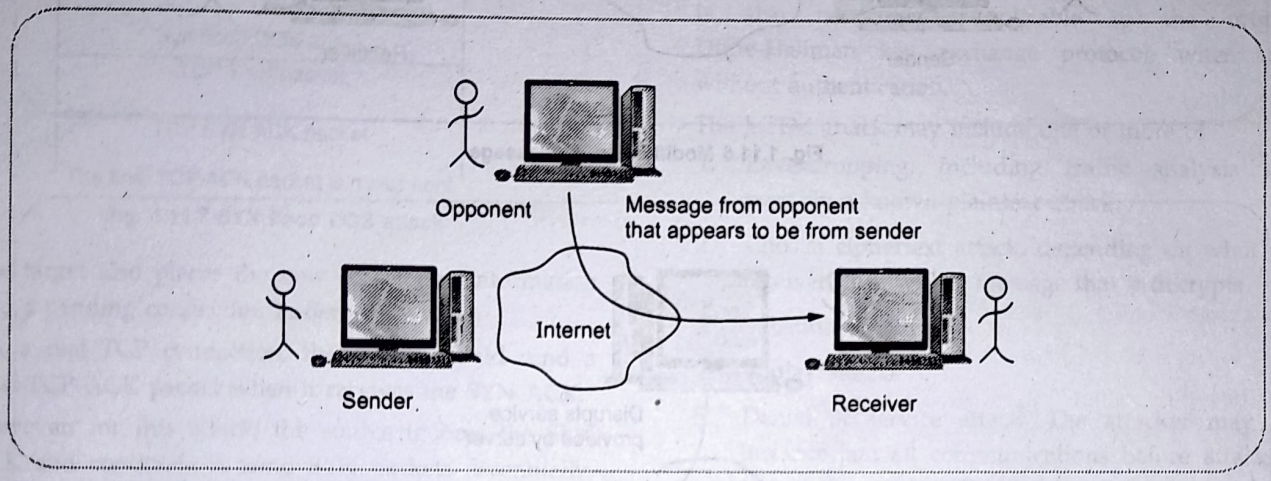

Fig. 1.11.3 Masquerade

- **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.
- **Interruption** attacks are called as masquerade attacks.

2. Replay

- It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- Fig. 1.11.4 shows replay attack.

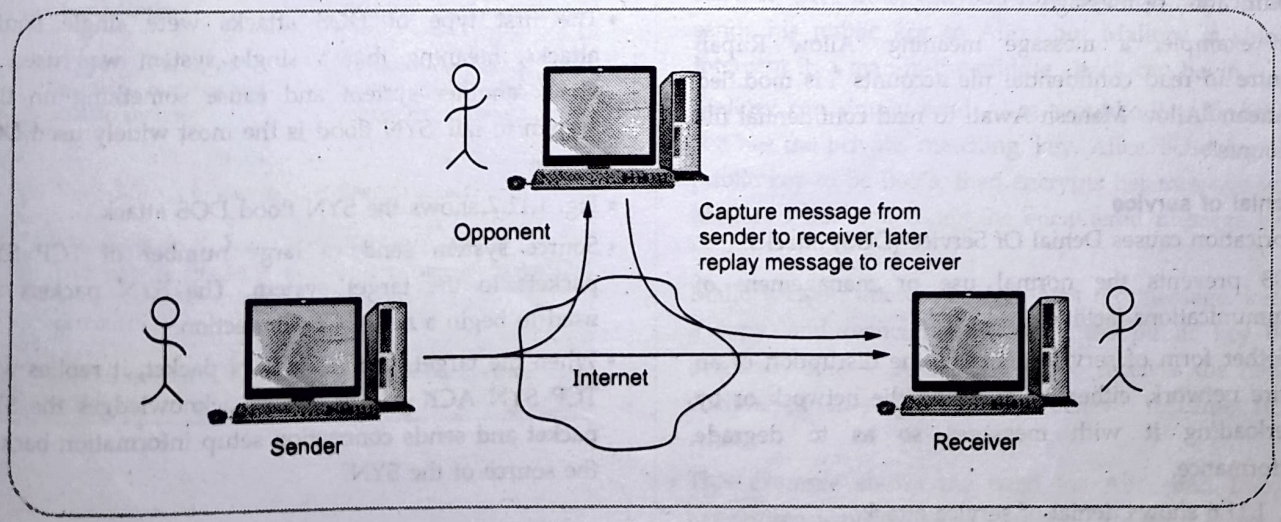

Fig. 1.11.4 Replay

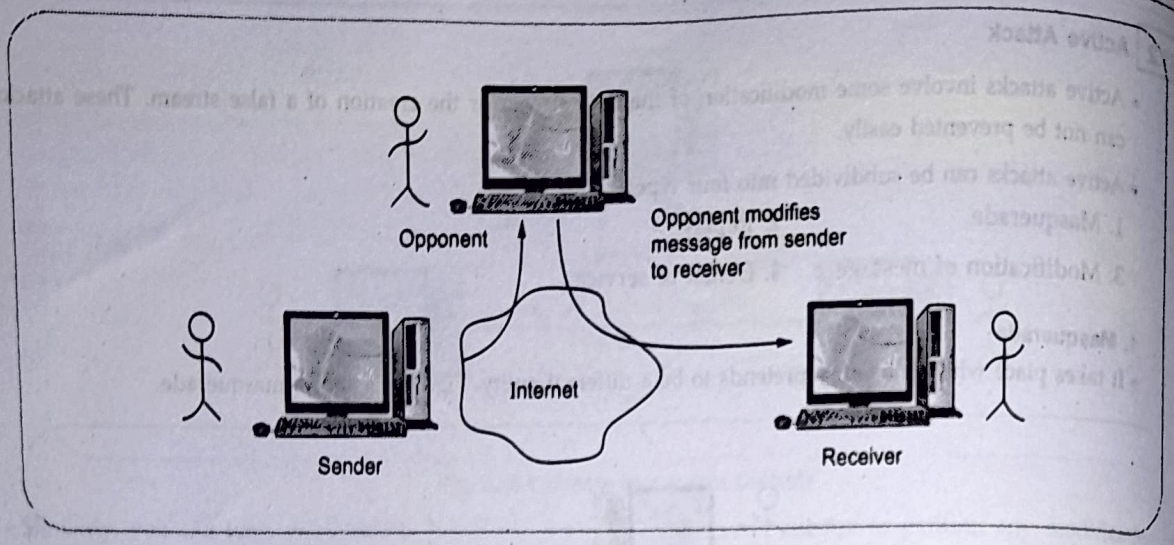

Fig. 1.11.5 Modification of message

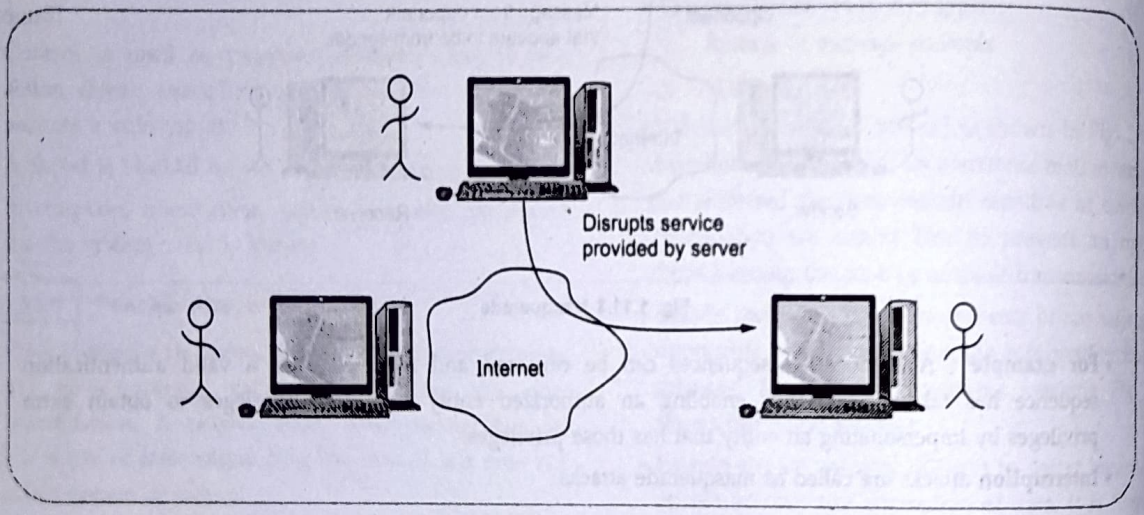

Fig. 1.11.6 Denial of service

3. Modification of message

- It involves some change to the original message. It produces an unauthorized effect. Fig. 1.11.5 shows the 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. 1.11.6 shows denial of service attack.
- 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. 1.11.7 shows the 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.
- When the target receives a SYN packet, it replies with TCP SYN ACK packet, which acknowledges the SYN packet and sends connection setup information back to the source of the SYN.

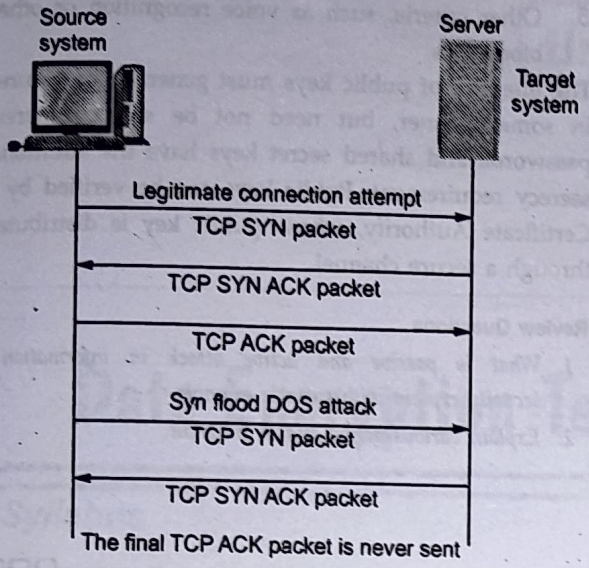

Fig. 1.11.7 SYN flood DOS attack

- The target also places the new connection information into a pending connection buffer.
- For a real TCP connection, the source would send a final TCP ACK packet when it receives the SYN ACK.
- However, for this attack, the source ignores the SYN ACK and continues to send SYN packets. Eventually, the target's pending connection buffer fills up and it can no longer respond to new connection requests.

1.11.3 Difference between Passive and Active Attack

Sr. No.	Passive attacks	Active attacks
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.	**Types :** Release of message contents and traffic analysis	**Types :** Masquerade, replay, modification of message and denial of service.
3.	Very difficult to detect.	Easy to detect.
4.	The emphasis in dealing with passive attacks is on prevention rather than detection.	It is quite difficult to prevent active attacks absolutely.
5.	It does not affect the system.	It affects the system.

1.11.4 Man-In-the-Middle Attack

- In cryptography, a **Man-In-The-Middle (MITM) attack** is an attack in which an attacker is able to read, insert and modify at will, meassages between two parties without either party knowing that the link between them has been compromised.
- The attacker must be able to observe and intercept messages going between the two victims. The MITM attack can work against public-key cryptography and is also particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication.
- The MITM attack may include one or more of
  1. Eavesdropping, including traffic analysis and possibly a known-plaintext attack.
  2. Chosen ciphertext attack, depending on what the receiver does with a message that it decrypts.
  3. Substitution attack
  4. Replay attacks
  5. Denial of service attack. The attacker may for instance jam all communications before attacking one of the parties. The defense is for both parties to periodically send authenticated status messages and to treat their disappearance with paranoia.
- MITM is typically used to refer to active manipulation of the meassages, rather than passively eavesdropping.

Example of a successful MITM attack against public-key encryption

- Suppose Alice wishes to communicate with Bob and that Mallory wishes to eavesdrop on the conversation, or possibly deliver a false message to Bob. To get started. Alice must ask Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a man-in-the-middle attack can begin.
- Mallory can simply send Alice a public key for which she has the private, matching, key. Alice, believing this public key to be Bob's, then encrypts her message with Mallory's key and sends the enciphered message back to Bob.
- Mallory again intercepts, deciphers the message, keeps a copy, and reenciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he will believe it came from Alice.
- This example shows the need for Alice and Bob to have some way to ensure that they are truly using the

correct public keys of each other. Otherwise, such attacks are generally possible in principle, against any message sent using public-key technology.

Defenses against the attack

- The possibility of a man-in-the-middle attack remains a serious security problem even for many public-key based cryptosystems. Various defenses against MITM attacks use authentication techniques that are based on :
  1. Public keys
  2. Stronger mutual authentication
  3. Secret keys (high information entropy secrets)
  4. Passwords (low information entropy secrets)
  5. Other criteria, such as voice recognition or other biometrics
- The integrity of public keys must generally be assured in some manner, but need not be secret, whereas passwords and shared secret keys have the additional secrecy requirement. Public keys can be verified by a Certificate Authority, whose public key is distributed through a secure channel.

Review Questions

1. *What is passive and active attack in information security explain with suitable example.*
2. *Explain various active attacks in detail.*