# Network and Cyber Security

Bachelor in Computer Engineering

Er. Anuj Sherchan

Assistant Professor

# Unit 1: Introduction to Network Security

- Outline:
- 1.1 Security, Attack, Types of Attack
- 1.1.1 Virus, Worm, Trojan Horse
- 1.1.2 Intruder, Hacker, Role of Firewall and DMZ
- 1.2 CIA Triad ,Security Service ,Security Mechanism
- 1.3 Network Security ,Network Security Access Model

# Introduction

- Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings.
- Once the data is out of hand, people with bad intention could modify or forge your data, either for enjoyment or for their own benefit.
- Cryptography can reformat and transform our data, making it safer on its trip between computers.
- The technology is based on the secret codes, modern mathematics that protects our data in powerful ways.
- **Computer Security** - generic name for the collection of tools designed to protect data and to prevent hackers.
- **Network Security** - measures to protect data during their transmission.
- **Internet Security -** measures to protect data during their transmission over a collection of interconnected networks.

# Need for Security

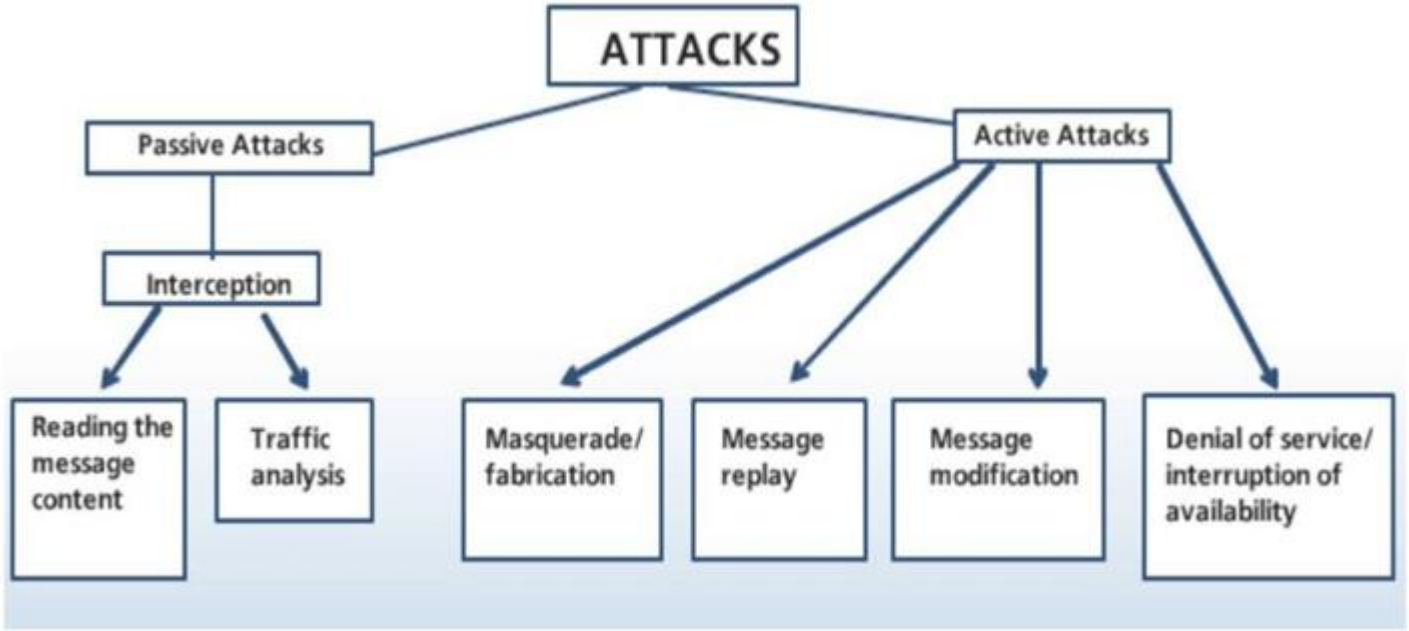
- Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use.
- It is the process of preventing and detecting unauthorized use of your computer system.
- Cyber security or Network Security is defined as protecting computer systems, which communicate over the computer networks.
- Computer security is important because it keeps your information protected.
- It's also important for your computer's overall health; proper computer security helps prevent viruses and malware, which allows programs to run quicker and smoother.

# Security Attacks, Types of Attack

- To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements.
- One approach is to consider three aspects of information security:
- **Security attack** – Any action that compromises the security of information owned by an organization.
- **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 the data processing systems and the information transfers of an organization.
- The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

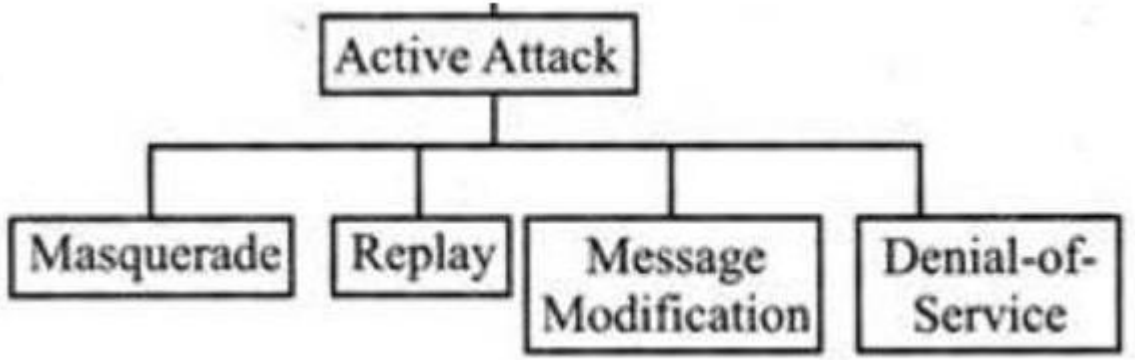
# Security Attacks, Types of Attack

- **Types of Attacks**
- There are two types of attacks.
- **Active attacks**
- **Passive attacks**



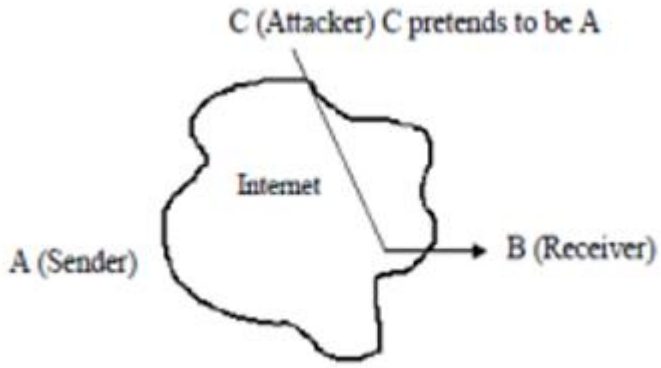
# Security Attacks, Types of Attack

- **Active attacks**
- An active attack is an attempt to alter system resources or affect their operation. i.e., these attacks involve in some modification to the original message in some manner or the creation of a false stream.
- These attacks can be classified in to four categories:



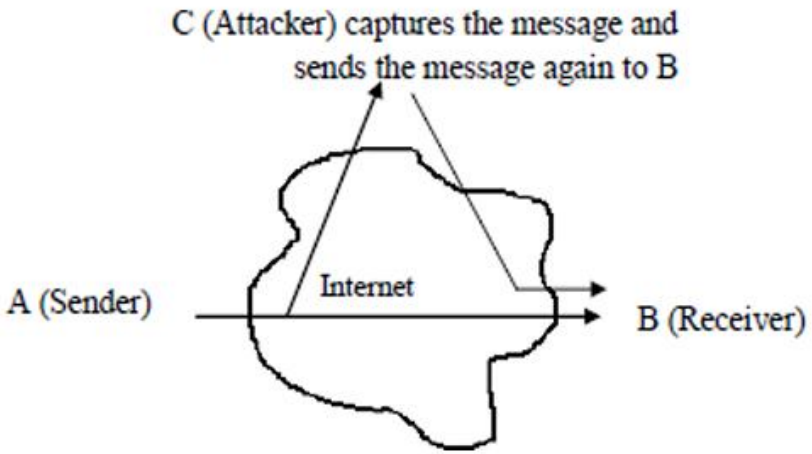
# Security Attacks, Types of Attack

- **Masquerade**
- One entity pretends to be a different entity.
- It is generally done by using stolen IDs and passwords or through bypassing authentication mechanism.



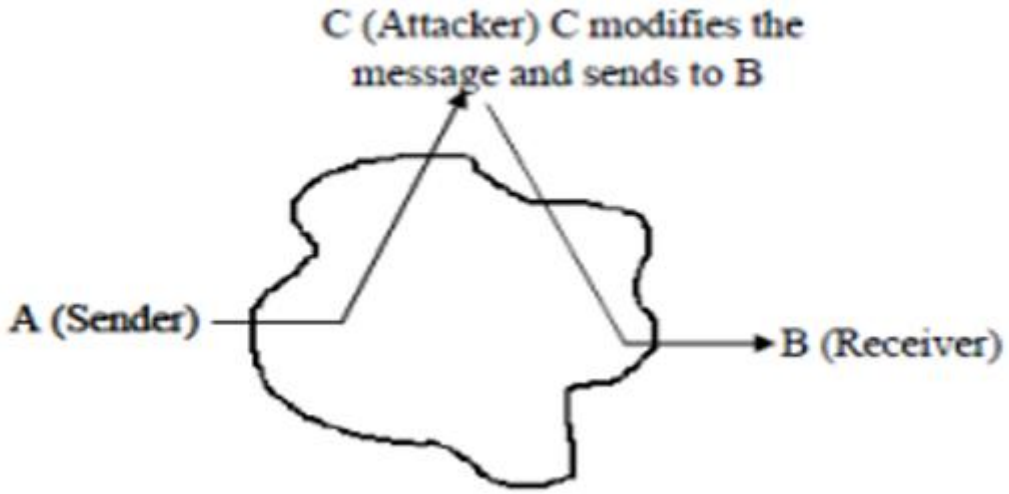
# Security Attacks, Types of Attack

- **Replay**
- This attack involves capturing a copy of the message sent by the original sender and retransmitting it later to bring an unauthorized result.



# Security Attacks, Types of Attack

- **Modification of messages**
- Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
- For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."



# Security Attacks, Types of Attack

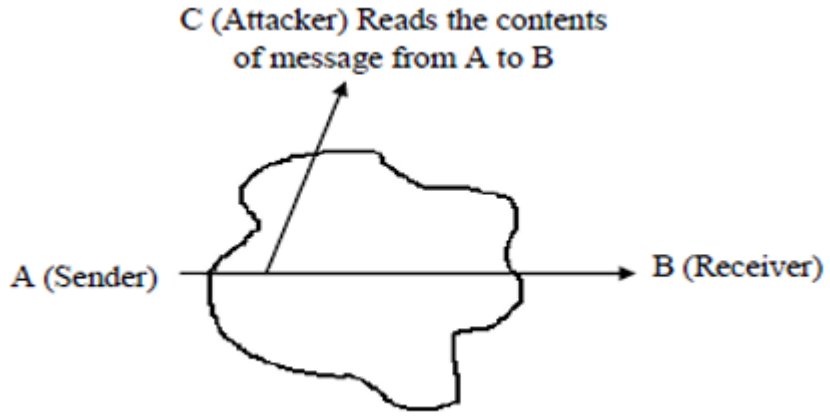
- **Denial of service**
- A denial-of-service (DoS) is a form of cyberattack that prevents legitimate users from accessing a computer or network.
- In a DoS attack, rapid and continuous online requests are sent to a target server in order to overload the server’s bandwidth.
- Prevents the normal use 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.

# Security Attacks, Types of Attack

- **Passive Attacks**
- Passive attacks are those where the attacker indulges in eavesdropping or monitoring of data transmission.
- Passive attacks do not involve any modifications to the contents of an original message.
- There are two types of passive attacks.
- **Release of message contents**
- **Traffic analysis.**

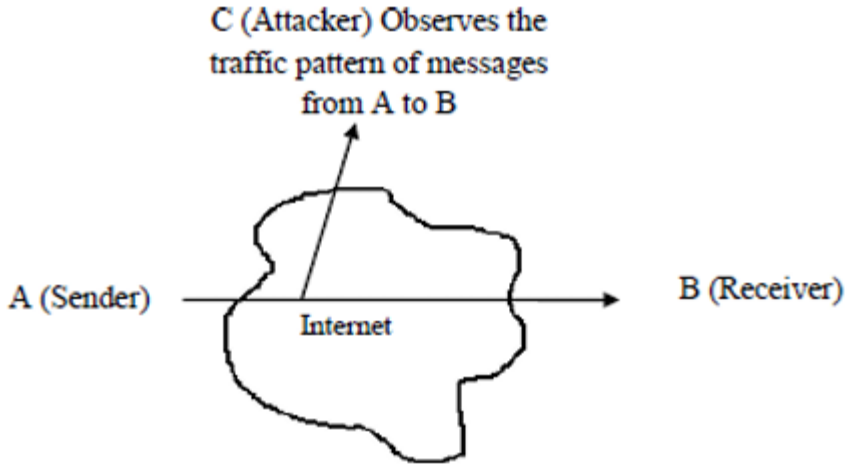
# Security Attacks, Types of Attack

- **Release of message contents**
- The release of message contents is a type of attack that analyzes and read the message delivered between senders to receiver.
- A telephone conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information.
- We would like to prevent an opponent from getting the contents of these transmissions.



# Security Attacks, Types of Attack

- **Traffic analysis**
- The attacker simply listens to the network communication to perform traffic analysis to determine the location of key nodes, the routing structure, and even application behavior patterns.
- In this type of attack, an intruder observes the frequency and length of msg. being exchanged between communicating nodes.
- Attacker can then use this information for guessing the nature of communication that was taking place.



# Security Attacks, Types of Attack

- **Virus**
- A virus is malicious code that attaches itself to a legitimate program or file and activates when the host is run.
- It requires user action (like opening an infected file) to spread.
- Viruses can corrupt files, delete data, or disrupt system performance by replicating into other programs.

# Security Attacks, Types of Attack

- **Worm**
- A worm is a standalone malware program that spreads automatically without needing a host file or user action.
- It exploits vulnerabilities in operating systems, applications, or networks to replicate across devices.
- Worms often consume large amounts of bandwidth and system resources, causing slowdowns or crashes.

# Security Attacks, Types of Attack

- **Trojan Horse**
- A Trojan horse (Trojan) is malicious software disguised as legitimate or useful software.
- Unlike viruses and worms, it does not self-replicate. Instead, it tricks users into installing it.
- Once inside the system, it can steal sensitive data (like login or credit card details), create backdoors, or allow attackers remote access.

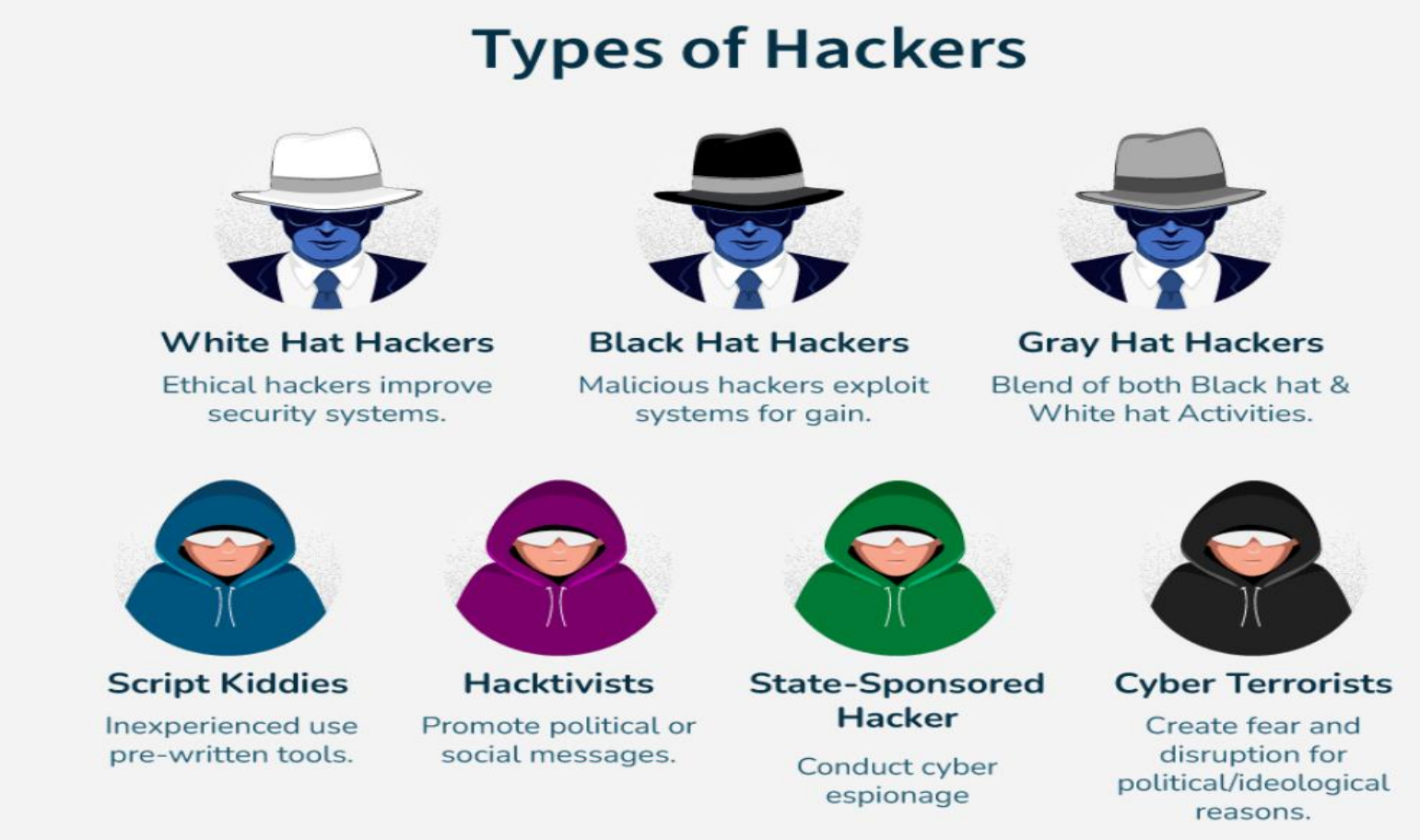
# Security Attacks, Types of Attack

- **Intruder**
- **Definition**: An intruder is any unauthorized individual who gains access to a system, network, or physical space.
- This can include a wide range of activities, from breaking into a building to accessing a computer system without permission.
- **Intent**: Intruders may have various motives, including theft, vandalism, or simply curiosity.
- Their activities can be malicious or non-malicious.
- **Examples**: Physical break-ins, unauthorized access to a network, or using stolen credentials to access a system.

# Security Attacks, Types of Attack

- **Hacker**
- **Definition**: A hacker is typically someone who uses technical skills to gain unauthorized access to systems or networks.
- The term can be both positive and negative, depending on the context.
- **Types**:
- **White hat hackers**: Ethical hackers who test systems for vulnerabilities to improve security.
- **Black hat hackers**: Malicious hackers who exploit vulnerabilities for illegal purposes, such as stealing data or causing damage.
- **Grey hat hackers**: Those who may violate ethical standards but do not have malicious intent, often revealing vulnerabilities without permission.
- **Intent**: Hackers may be motivated by a desire to exploit systems for personal gain, curiosity, or the challenge of overcoming security measures.

# Security Attacks, Types of Attack

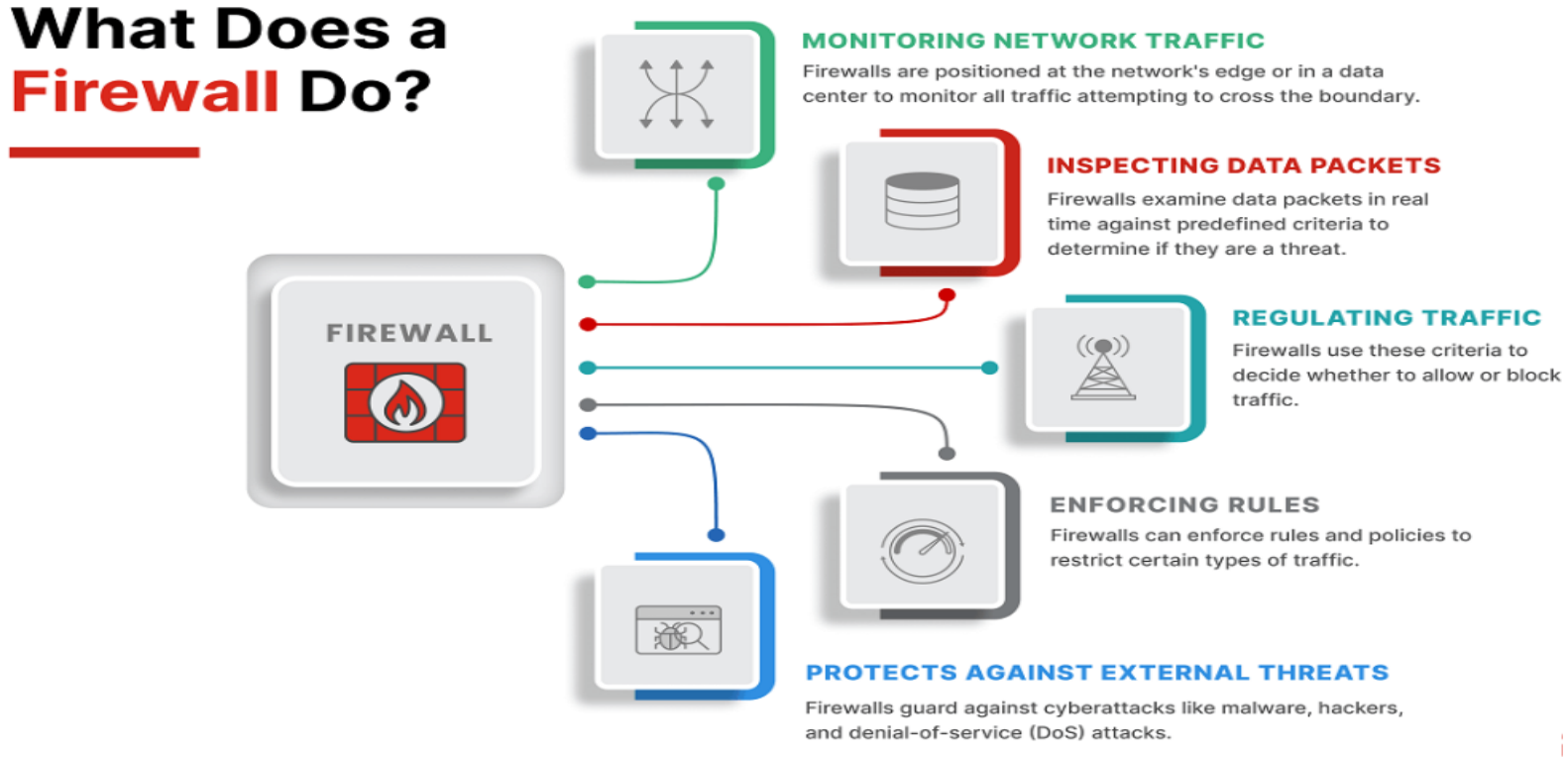


# Security Attacks, Types of Attack

- **Role of Firewall and DMZ**
- A firewall is a component that is used to monitor the incoming and outgoing traffic in a network.
- The term ‘firewall’ can be used to refer to hardware or software.
- Firewalls can be used to limit access to internal networks and protect them from internal and external dangers.

# Security Attacks, Types of Attack

## What does a firewall do?



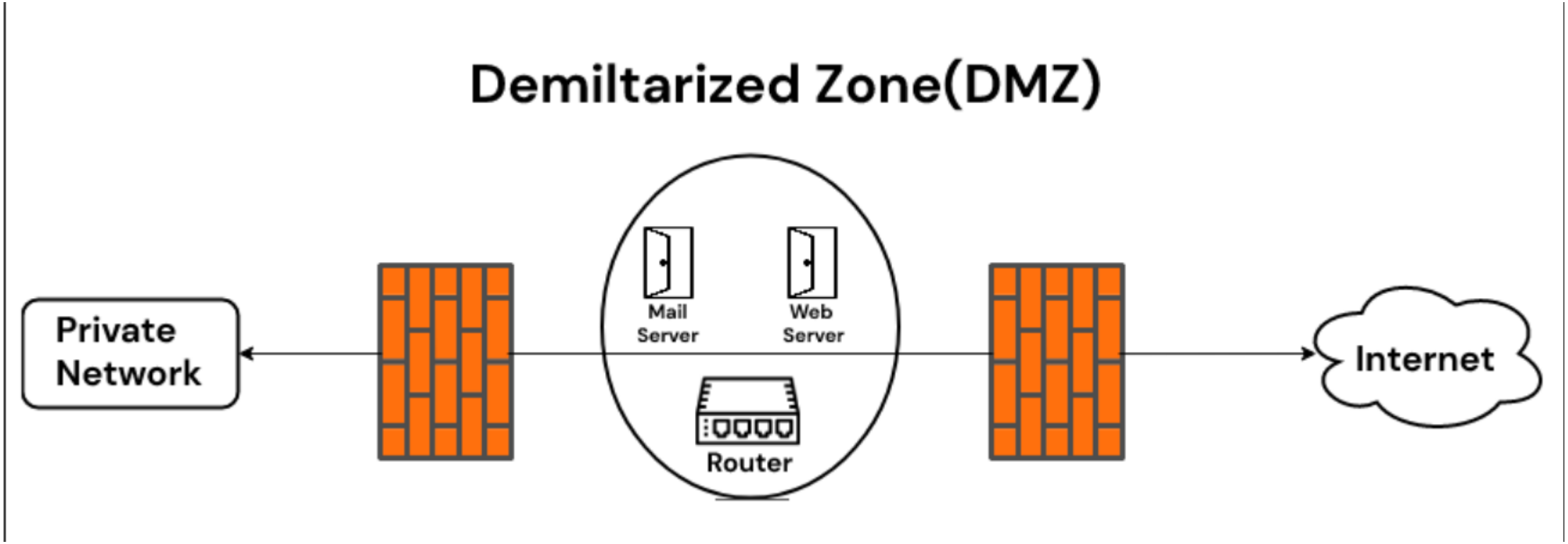
# Security Attacks, Types of Attack

- **Demilitarized Zones (DMZ)**
- are used in cybersecurity to separate internal networks from the internet and are often found on corporate networks.
- A DMZ is typically created on a company's internal network to isolate the company from external threats.
- While the name might sound negative, a DMZ can be a helpful tool for network security.
- The DMZ is a network barrier between the trusted and untrusted networks in a company's private and public networks.
- The DMZ acts as a protection layer through which outside users cannot access the company's data.

# Security Attacks, Types of Attack

- DMZ receives requests from outside users or public networks to access the information and website of a company.
- For such type of request, DMZ arranges sessions on the public network.
- It cannot initiate a session on the private network.
- If anyone tries to perform malicious activity on DMZ, the web pages are corrupted, but other information remains safe.
- The goal of DMZ is to provide access to the untrusted network by ensuring the security of the private network.
- DMZ is not mandatory, but a better approach is to use it with a firewall.

# Security Attacks, Types of Attack



# Security Services(CIA Triad)

- The classification of security services are as follows:
- **Confidentiality**
- The principle of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message.
- Confidentiality gets compromised if an unauthorized person is able to access a message.
- Unauthorized party could be a person, a program or a computer.
- Example: Suppose a confidential email message sent by user A to user B, which is accessed by user C without the permission or knowledge of A and B. This type of attack is called interception.
- Interception causes loss of message confidentiality.

# Security Services(CIA Triad)

- **Authentication**
- Authentication mechanism helps to establish proof of identities.
- The authentication process ensures that the origin of a electronic message or document is correctly identified.
- Fabrication is possible in absence of proper authentication mechanisms.
- **Integrity**
- When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. It is shown in figure.
- For example, consider that user A sends message to user B. User C tampers with a message originally sent by user A, which is actually meant for user B. User C change its contents and send the changed message to user B. User B has no way of knowing that the contents of the message changed after user A had sent it. User A also does not know about this change. This type of attack is called modification.
- Modification causes of loss of message integrity.

# Security Services(CIA Triad)

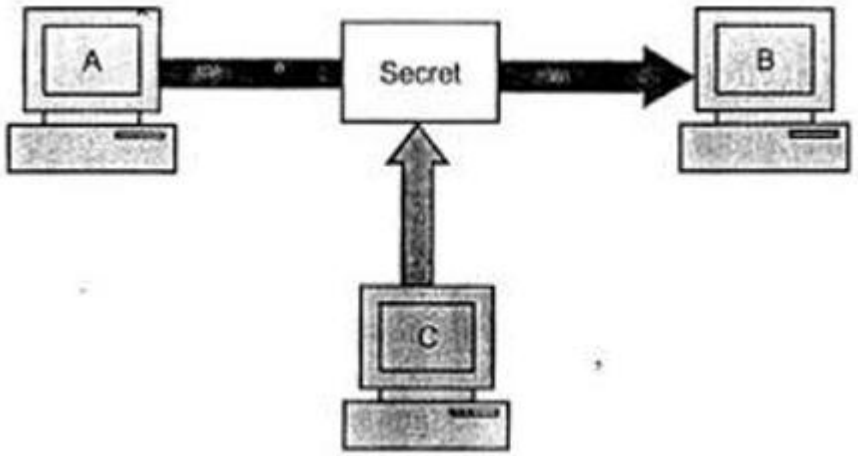



**Fig : Confidentiality**

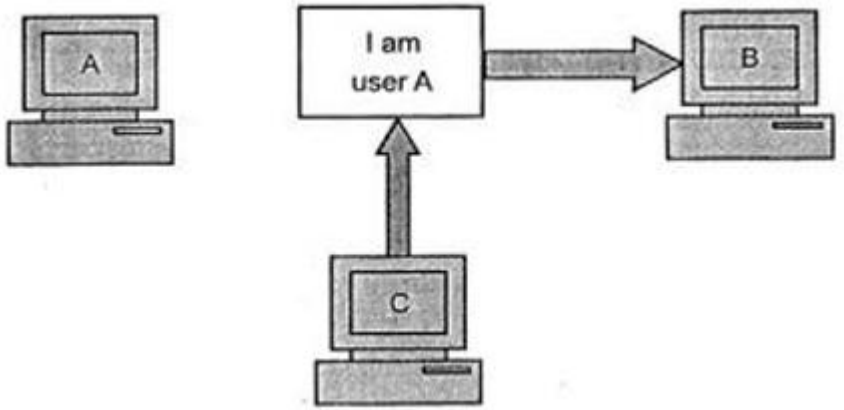



**Fig: Authenticity**

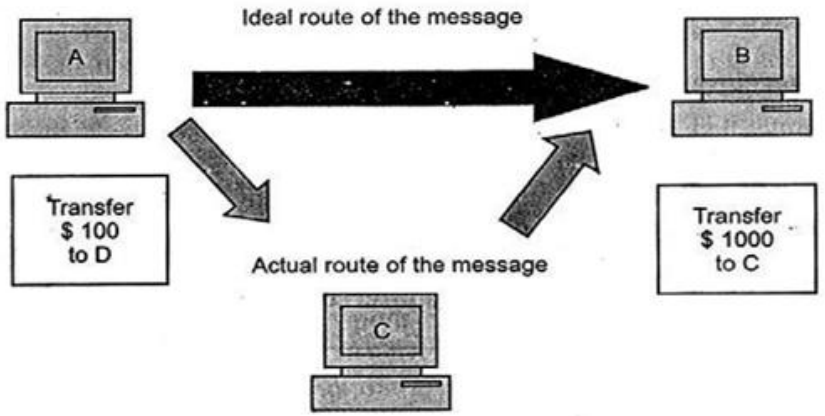
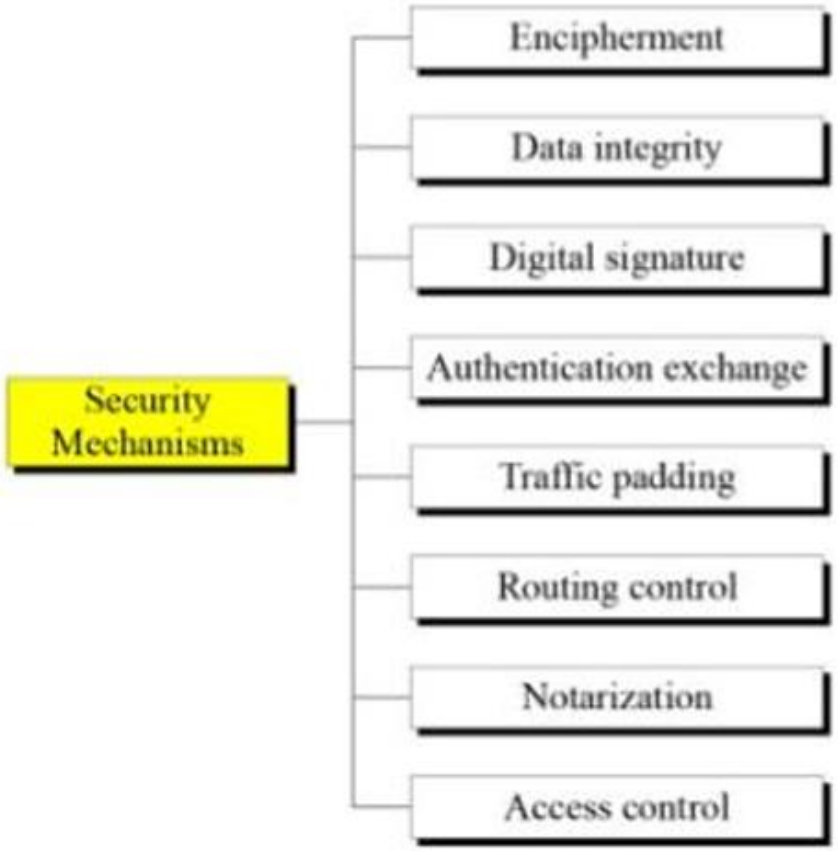



**Fig: Integrity**

# Security Mechanisms

- **Security Mechanisms**
- One of the most specific security mechanisms in use is cryptographic techniques.
- Encryption or encryption-like transformations of information are the most common means of providing security.
- Security mechanisms have been defined by ITU-T (X 800).
- Some of the security mechanisms defined by ITU-T (X 800) are shown in the figure.

# Security Mechanisms



# Security Mechanisms

- **Encipherment**
- This refers to the transformation of the message or data with the help of mathematical algorithms.
- The main aim of this mechanism is to provide confidentiality.
- The two techniques that are used for encipherment are cryptography and steganography.
- **Data integrity**
- This refers to the method of ensuring the integrity of data.
- For this, the sender computes a check value by applying some process over the data being sent, and then appends this value to the data.
- On receiving the data, the receiver again computes the check value by applying the same process over the received data.
- If the newly computed check value is same as the received one, then it means that the integrity of data is preserved.

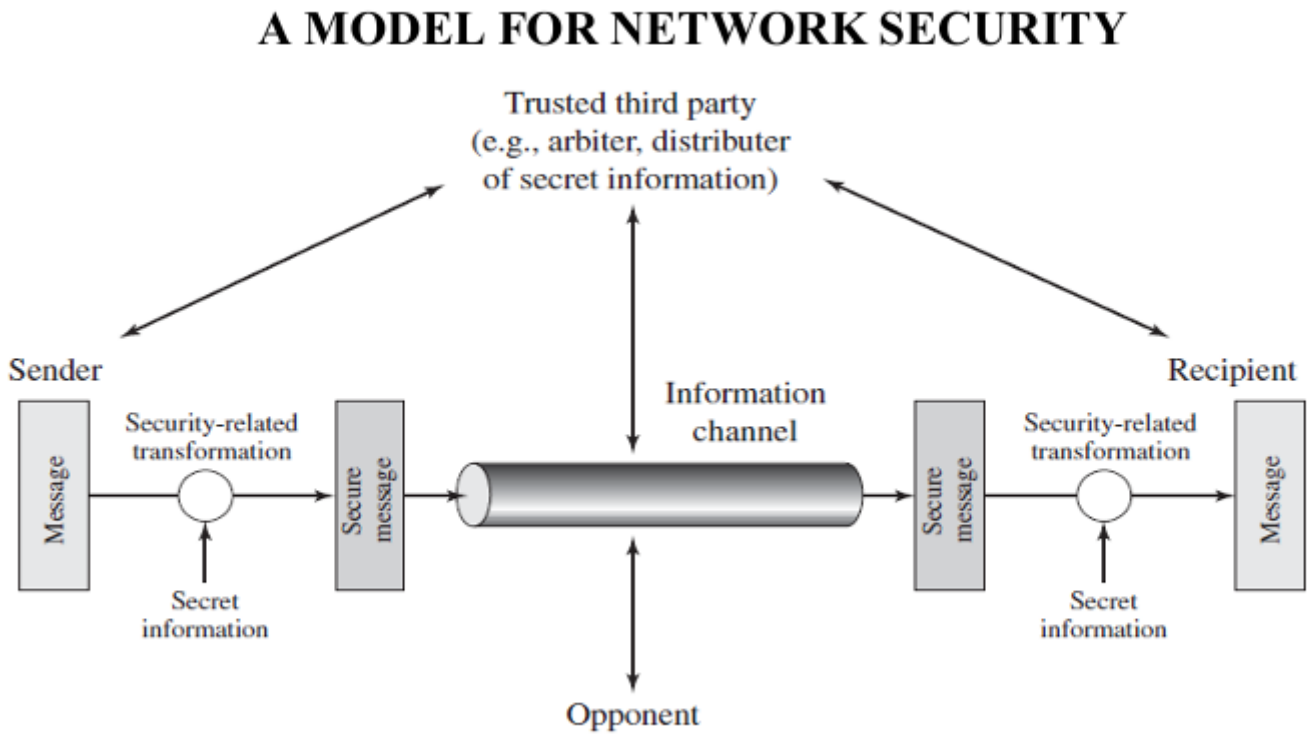
# Security Mechanisms

- **Digital signature**
- This refers to the method of electronic signing of data by the sender and electronic verification of the signature by the receiver.
- It provides information about the author, date and time of the signature, so that the receiver can prove the sender's identity.
- **Authentication exchange**
- This refers to the exchange of some information between two communicating parties to prove their identity to each other.
- **Traffic padding**
- This refers to the insertion of extra bits into the stream of data traffic to prevent traffic analysis attempts by attackers.

# Security Mechanisms

- **Routing control**
- This refers to the selection of a physically secured route for data transfer.
- It also allows changing of route if there is any possibility of eavesdropping on a certain route.
- **Notarization**
- This refers to the selection of a trusted third party for ensuring secure communication between two communicating parties.
- **Access control**
- It refers to the methods used to ensure that a user has the right to access the data or resource.

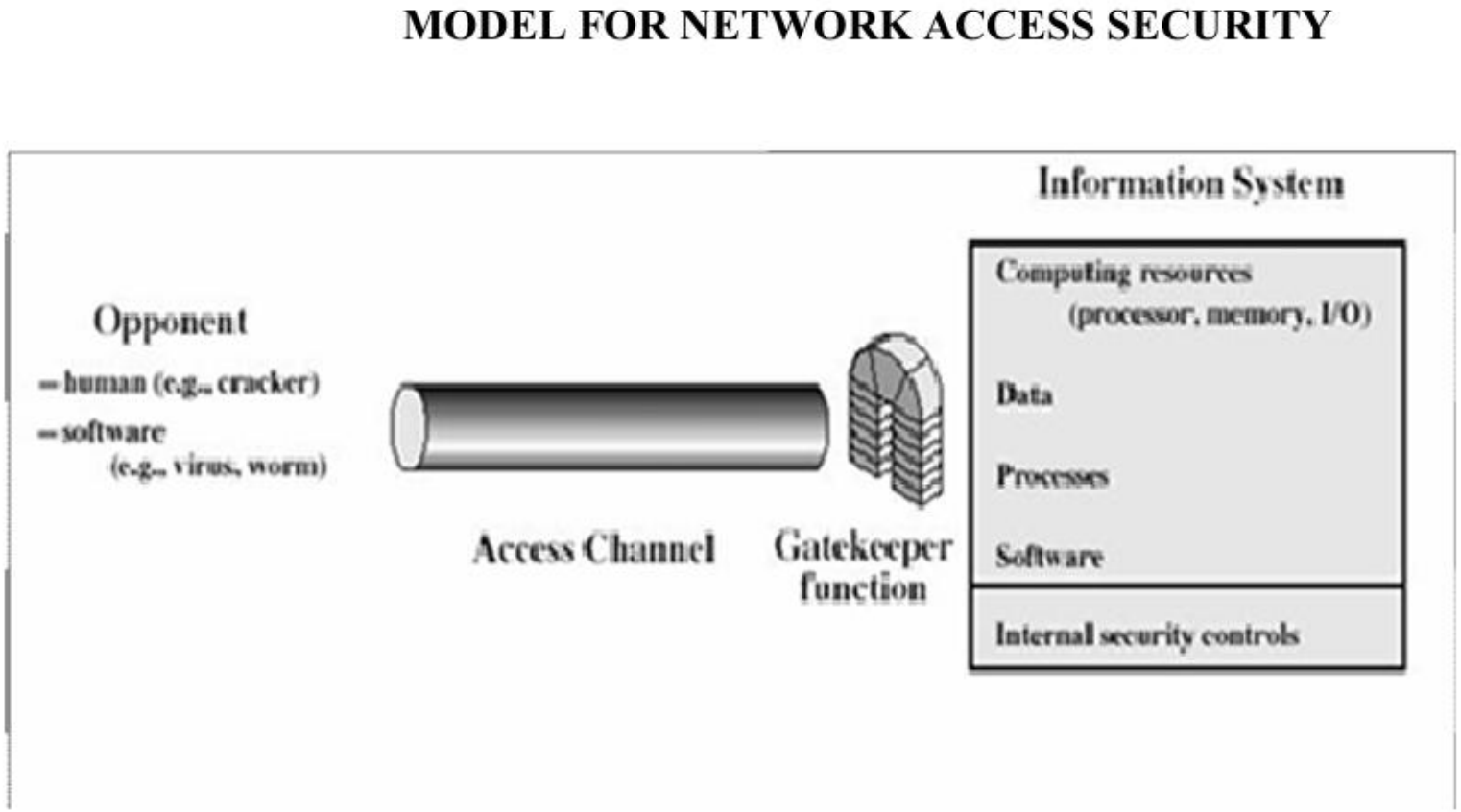
# Network Security Model



# Network Security Model

- A message is to be transferred from one party to another across some sort of internet.
- 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 (e.g., TCP/IP) by the two principals.
- Using this model requires us to:
- design a suitable algorithm for the security transformation
- generate the secret information (keys) used by the algorithm
- develop methods to distribute and share the secret information
- specify a protocol enabling the principals to use the transformation and secret information for a security service

# Network Security Access Model



# Network Security Access Model

- Using this model requires us to
- select appropriate gatekeeper functions to identify users
- implement security controls to ensure only authorized users access designated information or resources
- Trusted computer systems can be used to implement this model

# THANK YOU