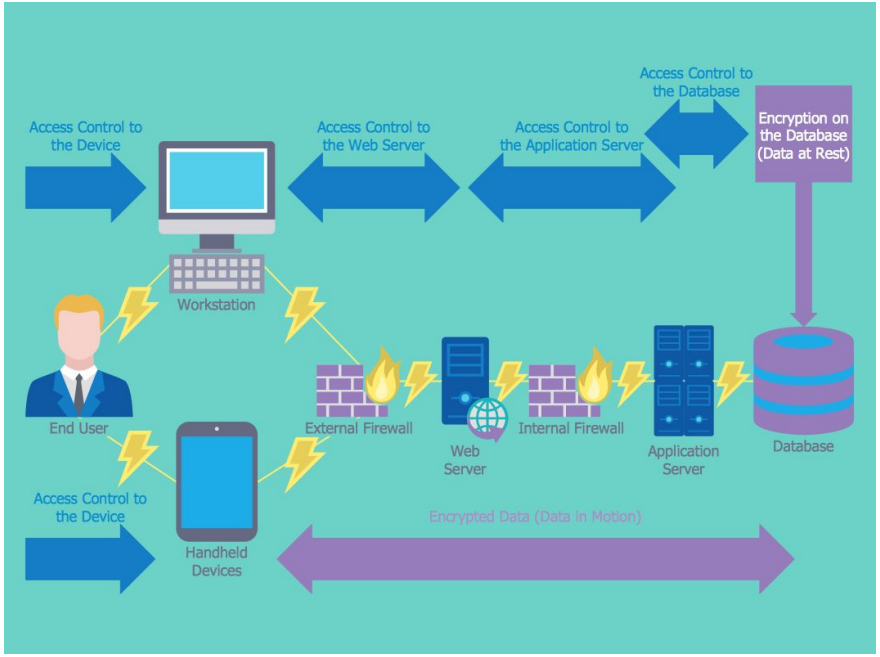
UNIT 1 Introduction to Network Security



Introduction to Network Security

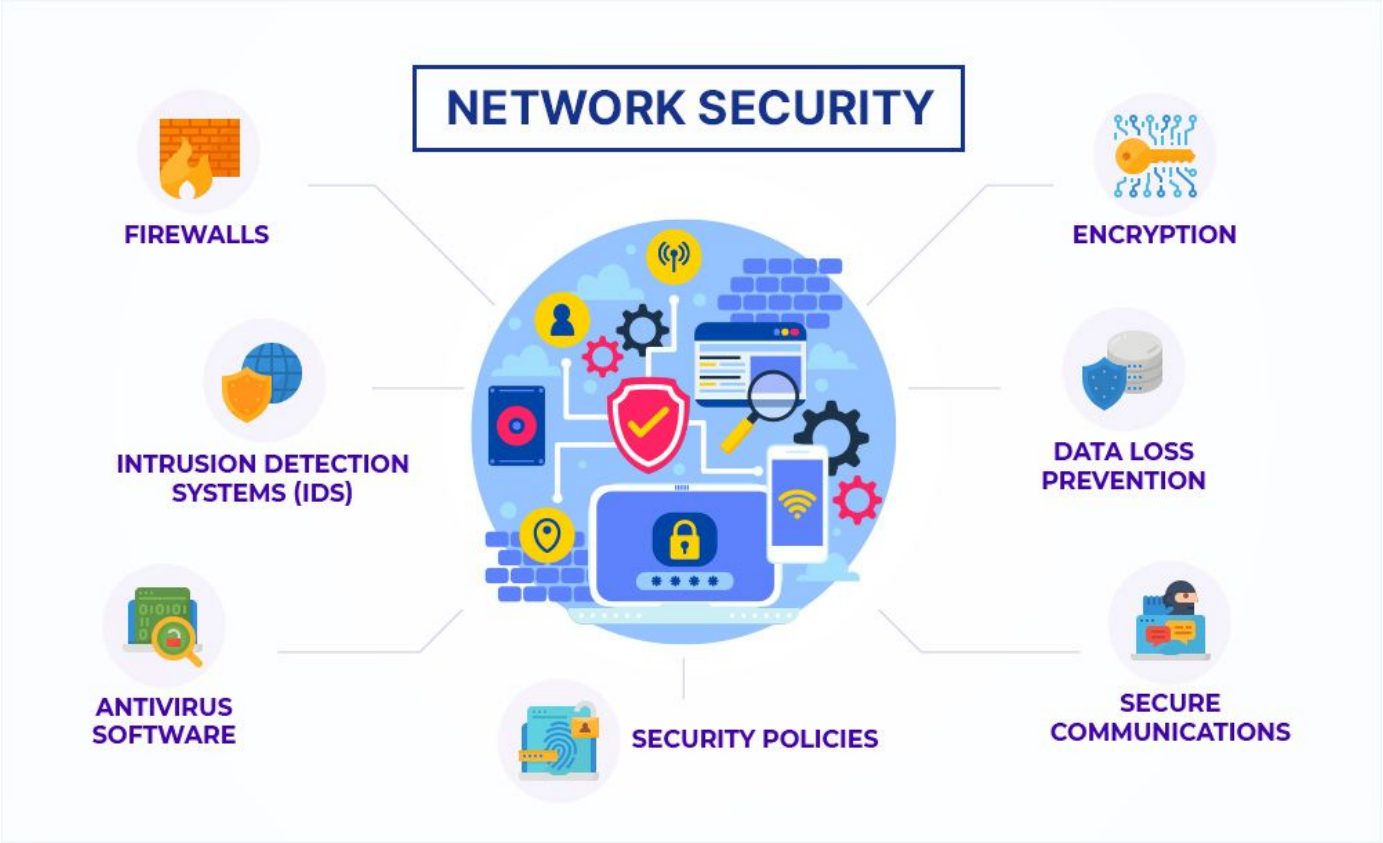
- Introduction to Network Security
- Definition and objectives of network security
- CIA Triangle
- Challenges of Security
- Security Attacks

Introduction to Network Security

What is Network Security?

- Any action intended to safeguard the integrity and usefulness of your data and network is known as network security.
- Network security is defined as the activity created to protect the integrity of your network and data.
- Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks.
- It involves using tools, technologies, and policies to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.

Introduction to Network Security



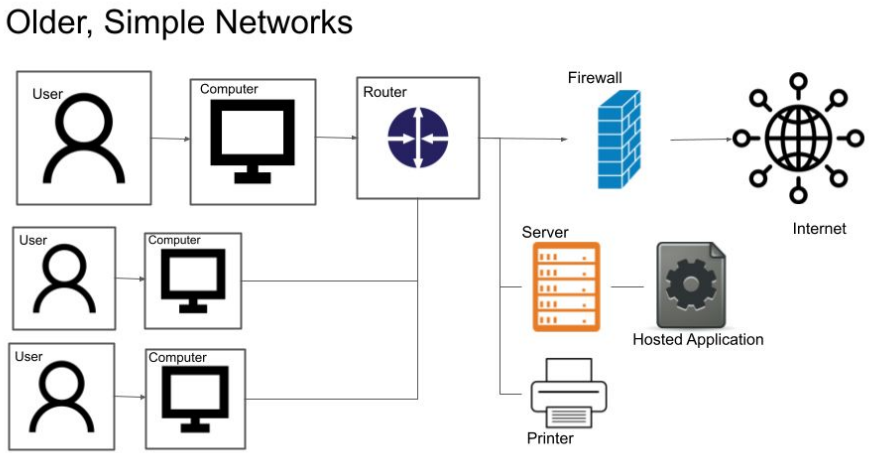
CIA Triangle

What are the 3 components of the CIA triad?

- **Confidentiality**. Roughly equivalent to privacy, confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It's common for data to be classified according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent data security measures can then be implemented according to those categories.
- **Integrity**. The consistency, accuracy and trustworthiness of data must be maintained over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure it can't be altered by unauthorized people -- for example, in data breaches.
- **Availability**. Information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

Challenges of Security

1. **Evolving Threat Landscape**
   New threats and rapid adaptation required.
2. **Complexity of Modern Networks**
   Diverse devices and integration challenges.
3. **Insider Threats**
   Malicious and unintentional insider breaches.
4. **Resource Constraints**
   Budget, personnel, and skills shortage.
5. **Regulatory Compliance**
   Complex regulations and penalties.
6. **User Behavior**
   Lack of awareness and resistance to measures.



Threats and Attacks (RFC 4949)

Threat

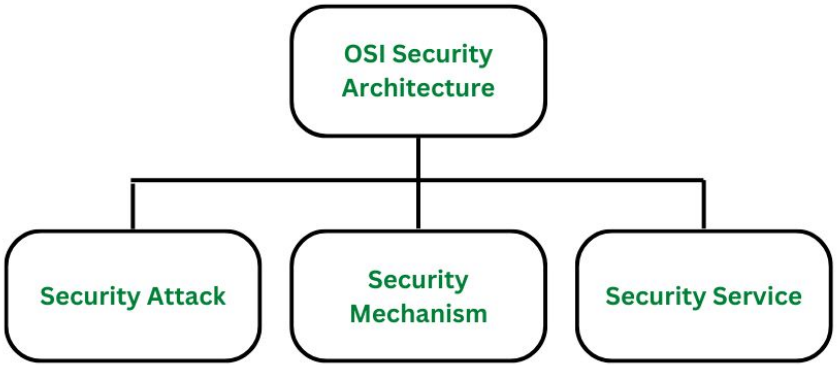
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

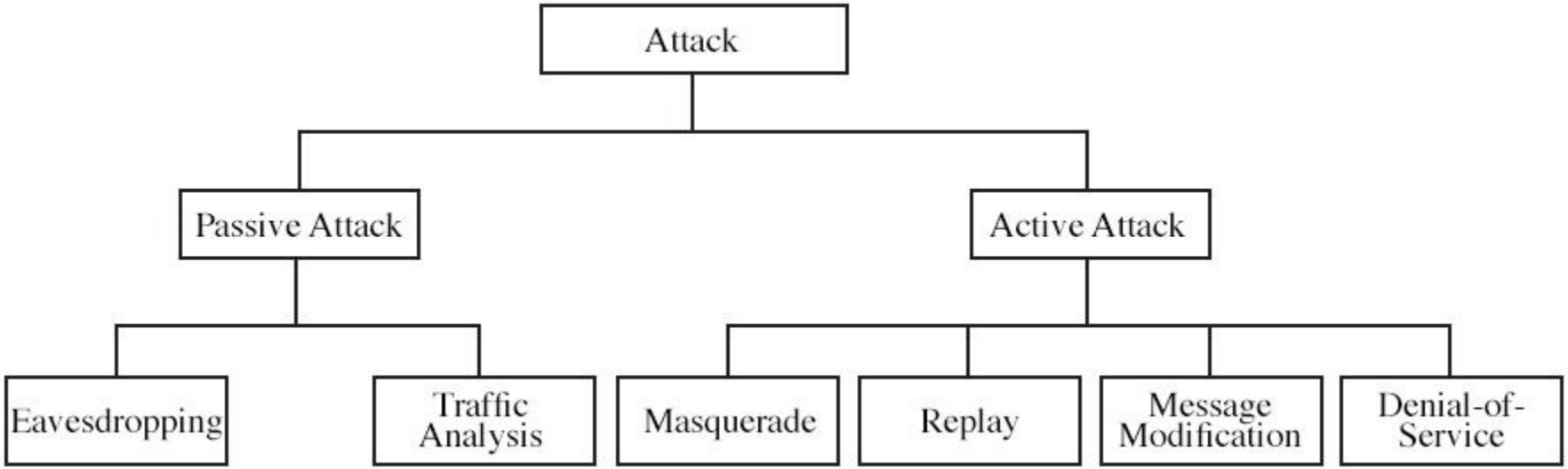
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

THE OSI SECURITY ARCHITECTURE

- **Security attack**: Any action that compromises the security of information owned by an organization.
- **Security mechanism**: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.



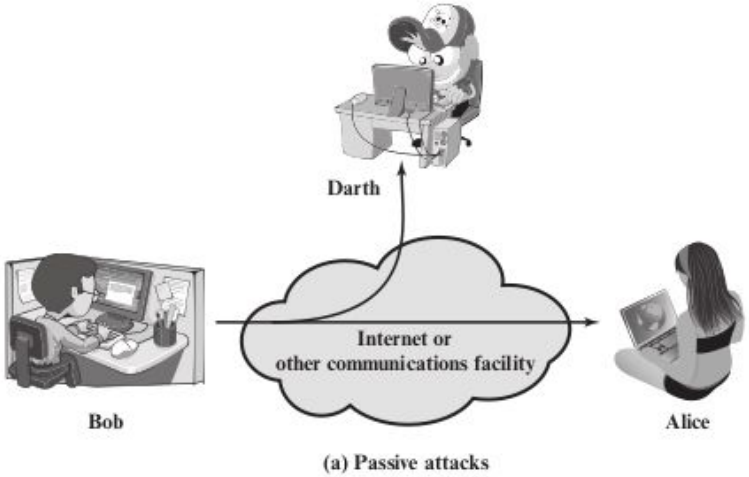
Security Attacks



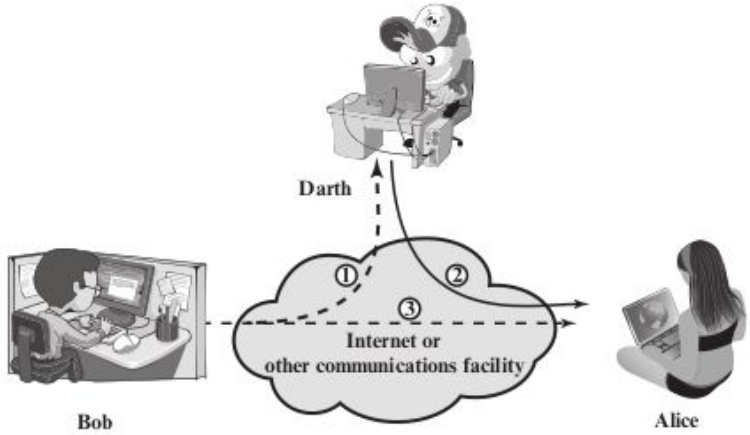
SECURITY ATTACKS

- **Any action that comprises the security of information owned by an organization.**

- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- An active attack attempts to alter system resources or affect their operation.



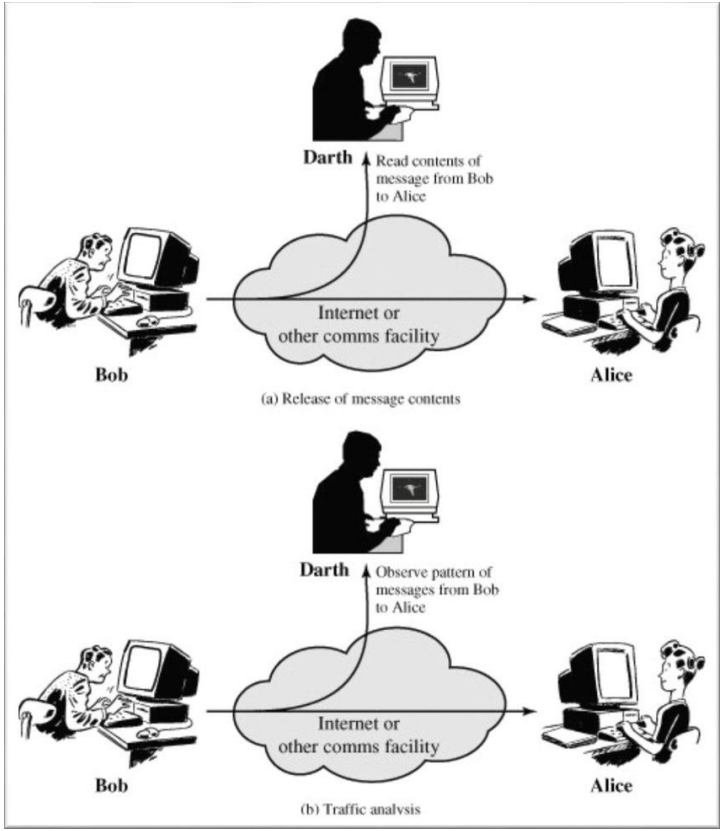
(a) Passive attacks



(b) Active attacks

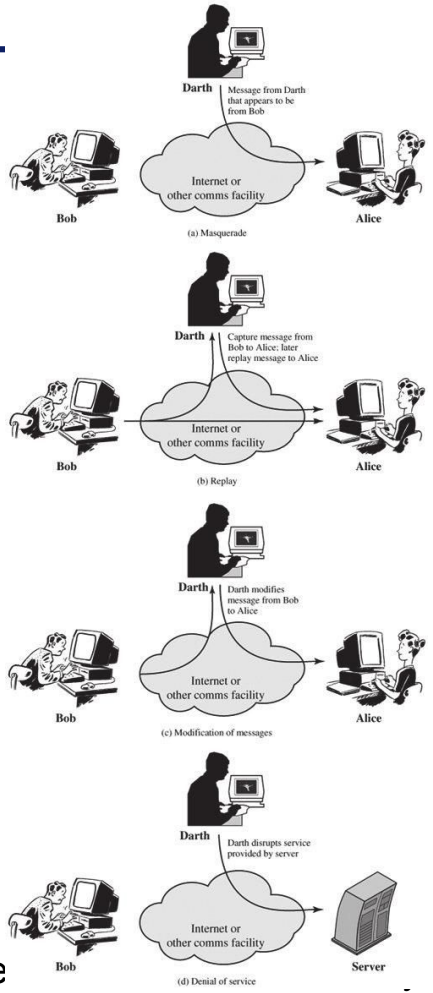
Passive Attacks

- 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 and traffic analysis.
- The **release of message contents** is easily understood. 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 contents of these transmissions.
- A second type of passive attack, **traffic analysis**, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.



Active Attacks

- A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.
- 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.
- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- **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.
- The **denial of service** prevents or inhibits the normal use or management of communications facilities (path 3 active). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). 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.



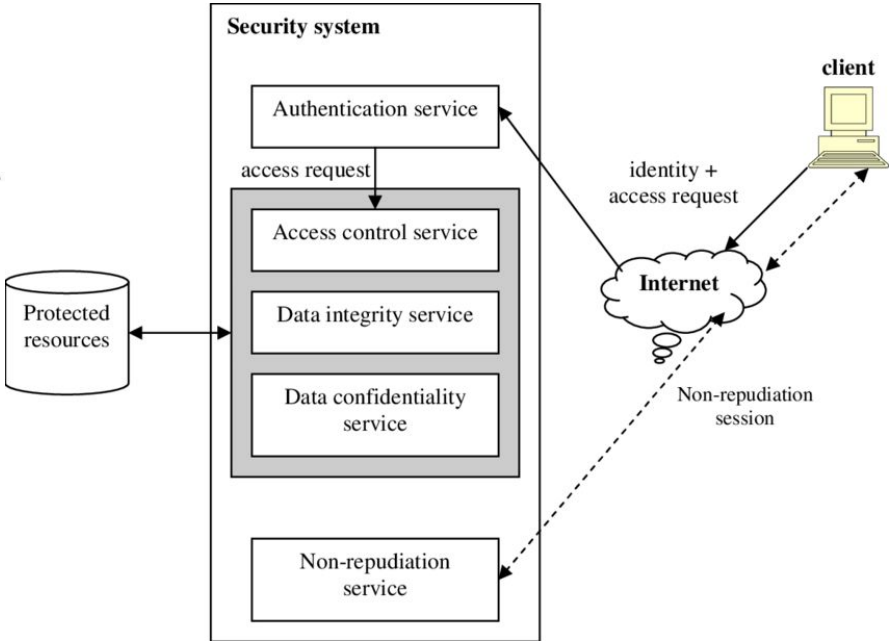
Active Attacks v/s Passive Attacks

No	Active Attack	Passive Attack
1	Attacker needs to have control media or network.	Attacker observe the communication in media or network.
2	It can be easily detected.	It cannot be easily detected.
3	It affects the system.	It does not affect the system.
4	It involves modification in data.	It involves in monitoring in data.
5	It does not check for loopholes or vulnerabilities.	It scans the ports and network in search for loopholes and vulnerabilities.
6	It is difficult to prevent network from active attack.	Passive attack can be prevented.
7	Types of active attack: Masquerade, replay, denial of service, modification of message.	Types of passive attack: release of message content, Traffic analysis.

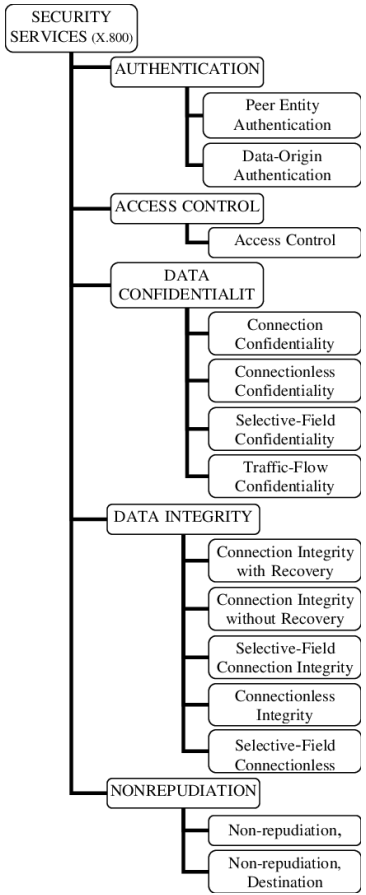
Security Services X.800

- **A processing or communication service that is provided by a 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.

- **Authentication** – assure that communication entity is the one claimed
- **Access Control** – prevention of the unauthorized use of a resource
- **Data Confidentiality** – protection of data from unauthorized disclosure
- **Data Integrity** – assure that data received is as sent by an authorized entity
- **Non-Repudiation** – protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable.



Security Services X.800



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.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

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.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

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. Additionally, a limited form of replay detection may be provided.

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.

NONREPUDIATION

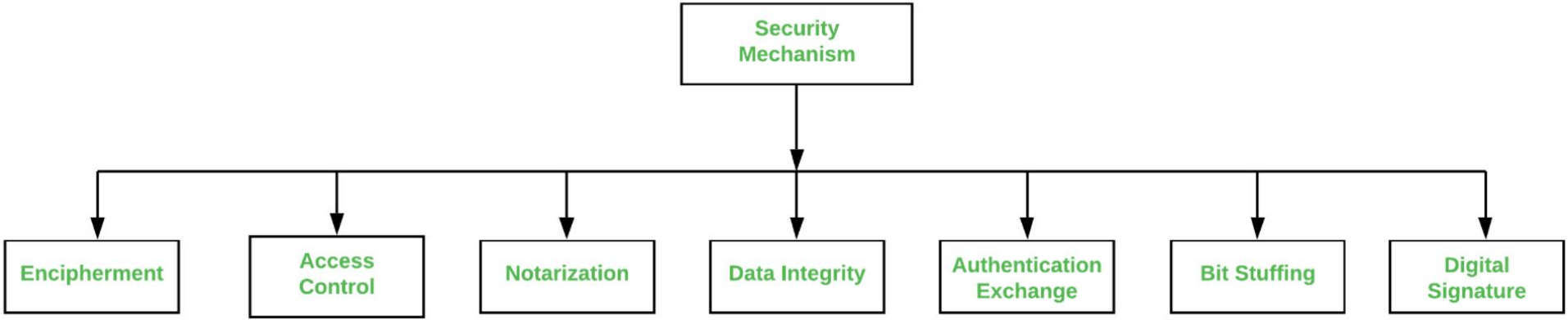
Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Security Mechanisms

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



Security Mechanisms

- 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.

- Access Control :

  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.

- 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.

- 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.

Security Mechanisms

- 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

- Bit stuffing :

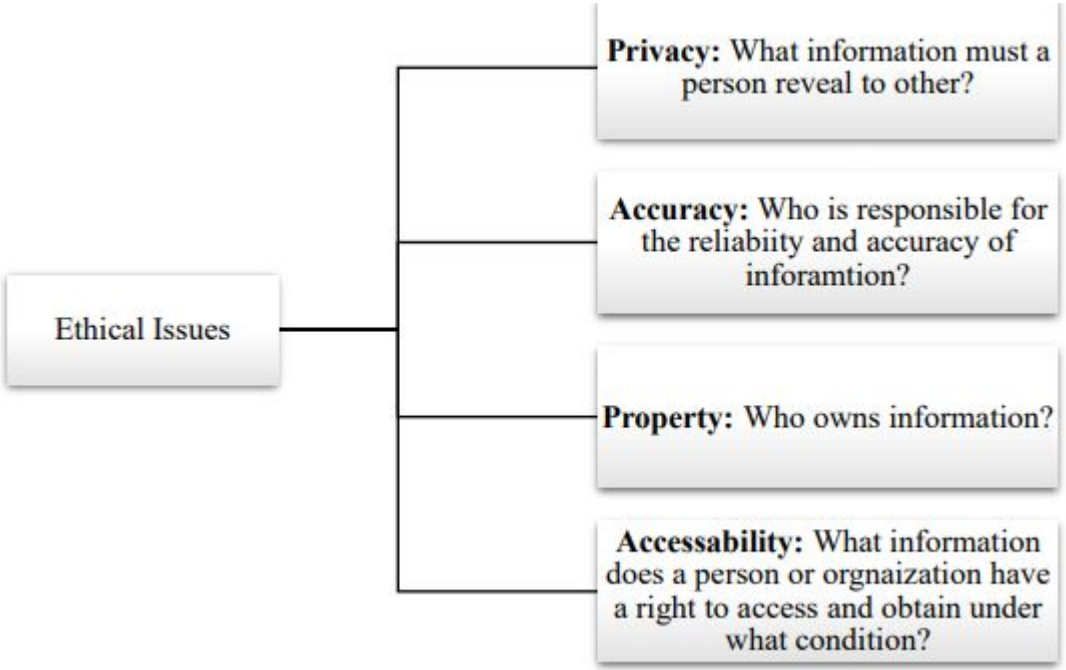
  This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

- Digital Signature :

  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.

Security service	Security mechanisms
Data confidentiality	Encipherment, Routing control
Data integrity	Encipherment, Data integrity, Digital signature
Authentication	Authentication exchanges, Digital signature, Encipherment
Non repudiation	Data integrity, Digital signature, Notarisation
Access control	Access control mechanisms

Ethical and Legal Issues



THANK YOU