Aspects of Security and Model for Network Security

1 Aspects of Security

Information security considers three key aspects:

1. Security Attack
2. Security Mechanism
3. Security Service

1.1 1. Security Attack

A security attack is defined as any action that compromises the security of information owned by an organization . Information security focuses on how to prevent attacks, or failing that, to detect attacks on information-based systems .

Attacks are broadly classified into two generic types :

1.1.1 A. 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 .

- **Release of message contents:** Reading the contents of a message from sender to receiver .
- **Traffic analysis:** Observing the pattern of messages between sender and receiver.

1.1.2 B. Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream . They are difficult to prevent; therefore, the goal is to detect attacks and recover from any disruption.

- **Masquerade:** Takes place when one entity pretends to be a different entity.
- **Replay:** Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- **Modification of messages:** Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect.
- **Denial of service:** Prevents or inhibits the normal use or management of communications facilities (e.g., disrupting service provided by a server).

1.2 2. Security Service (X.800)

A security service enhances the security of data processing systems and information transfers of an organization. It is intended to counter security attacks using one or more security mechanisms .

The specific security services defined include :

- **Authentication:** Assurance that the communicating 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:** Assurance that data received is as sent by an authorized entity.
- **Non-Repudiation:** Protection against denial by one of the parties in a communication.

1.3 3. Security Mechanism (X.800)

A security mechanism is a feature designed to detect, prevent, or recover from a security attack. No single mechanism supports all required services, but cryptographic techniques underlie many mechanisms .

- **Specific Security Mechanisms:** Encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization .
- **Pervasive Security Mechanisms:** Trusted functionality, security labels, event detection, security audit trails, security recovery .

2 Model for Network Security

The model for network security describes the flow of information between a sender and a recipient across an insecure channel.

2.1 Components of the Model

The model involves the following components and flows :

- **Sender:** Initiates the message.
- **Message:** The original data input.
- **Secret Information:** Used by the security-related transformation (e.g., keys).
- **Security-related Transformation:** Processes the message and secret information to create a secure message.
- **Information Channel:** The medium for transmission (subject to the Opponent).
- **Opponent:** An entity that may attempt to access or disrupt the secure message in the channel.

- **Trusted Third Party:** Responsible for distributing secret information to the Sender and Recipient (e.g., arbiter).
- **Recipient:** Receives the secure message and performs a transformation to retrieve the original message.

2.2 Requirements for Using the Model

To use this model effectively, the following four tasks are required :

1. Design a suitable algorithm for the security transformation.
2. Generate the secret information (keys) used by the algorithm.
3. Develop methods to distribute and share the secret information.
4. Specify a protocol enabling the principals to use the transformation and secret information for a security service.