SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

AN AUTONOMOUS INSTITUTION

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

OSI Security Architecture

The OSI Security Architecture is internationally recognized and provides a standardized technique for deploying security measures within an organization. It focuses on three major concepts: security attacks, security mechanisms, and security services, which are critical in protecting data and communication processes. In this article, we will discuss OSI Security Architecture.

The OSI model can be considered a universal language for computer networking. It is based on the concept of divide and conquer, it splits up the communication system into 7 abstract layers, and the layer is stacked upon the previous layer. OSI model has seven layers which are as follows:

- The Physical Layer
- The Data Link Layer
- The Network Layer
- The Transport Layer
- The Session Layer
- The Presentation Layer
- The Application Layer

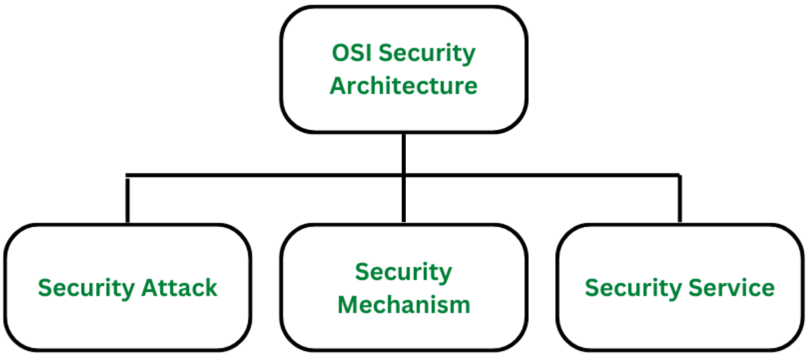
What is OSI Security?

OSI (Open Systems Interconnection) security refers to a set of protocols, standards, and techniques used to ensure the security of data and communications in a network environment based on the OSI model. The International Organisation for Standardisation (ISO) established this model to provide a conceptual framework for understanding how different networking protocols interact within a layered architecture.

Classification of OSI Security Architecture

The OSI (Open Systems Interconnection) Security Architecture defines a systematic approach to providing security at each layer. It defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network. These security services and mechanisms help to ensure the confidentiality, integrity, and availability of the data. OSI architecture is internationally acceptable as it lays the flow of providing safety in an organization. OSI Security Architecture focuses on these concepts:

- Security Attack
- Security mechanism
- Security Service



Classification of OSI Security Architecture

OSI Security Architecture is categorized into three broad categories namely **Security Attacks, Security mechanisms**, **and Security Services**. We will discuss each in detail:

1. Security Attacks

A security attack is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the security of a system, network, or device. These are defined as the actions that put at risk an organization's safety. They are further classified into 2 sub-categories:

- **Passive Attack:** Attacks in which a third-party intruder tries to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission or eave-dropping the transmission is called Passive Attacks. These types of attacks involve the attacker observing or monitoring system, network, or device activity without actively disrupting or altering it. Passive attacks are typically focused on gathering information or intelligence, rather than causing damage or disruption. Here, both the sender and receiver have no clue that their message/ data is accessible to some third-party intruder. The message/ data transmitted remains in its usual form without any deviation from its usual behavior. This makes passive attacks very risky as there is no information provided about the attack happening in the communication process. Passive attacks are further divided into two parts based on their behavior:
  - **Eavesdropping:** Eavesdropping involves the attacker intercepting and listening to communications between two or more parties without their

knowledge or consent. Eavesdropping can be performed using a variety of techniques, such as packet sniffing, or man-in-the-middle attacks.

  - **Traffic analysis:** This involves the attacker analyzing network traffic patterns and metadata to gather information about the system, network, or device. Here the intruder can't read the message but only understand the pattern and length of encryption. Traffic analysis can be performed using a variety of techniques, such as network flow analysis, or protocol analysis.

- **Active Attacks:** Active attacks refer to types of attacks that involve the attacker actively disrupting or altering system, network, or device activity. Active attacks are typically focused on causing damage or disruption, rather than gathering information or intelligence. Here, both the sender and receiver have no clue that their message/ data is modified by some third-party intruder. The message/ data transmitted doesn't remain in its usual form and shows deviation from its usual behavior. This makes active attacks dangerous as there is no information provided of the attack happening in the communication process and the receiver is not aware that the data/ message received is not from the sender. Active attacks are further divided into four parts based on their behavior:
  - **Masquerade:** Masquerade is a type of attack in which the attacker pretends to be an authentic sender in order to gain unauthorized access to a system. This type of attack can involve the attacker using stolen or forged credentials, or manipulating authentication or authorization controls in some other way.
  - **Replay:** Replay is a type of active attack in which the attacker intercepts a transmitted message through a passive channel and then maliciously or fraudulently replays or delays it at a later time.
  - **Modification of Message:** Modification of Message involves the attacker modifying the transmitted message and making the final message received by the receiver look like it's not safe or non-meaningful. This type of attack can be used to manipulate the content of the message or to disrupt the communication process.
  - **Denial of service (DoS):** **Denial of Service** attacks involve the attacker sending a large volume of traffic to a system, network, or device in an attempt to overwhelm it and make it unavailable to users.

2. Security Mechanism

The mechanism that is built to identify any breach of security or attack on the organization, is called a security mechanism. Security Mechanisms are also responsible for protecting a system, network, or device against unauthorized access, tampering, or other security threats.

- **Encipherment (Encryption):** Encryption involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key. Encryption can be used to protect data it is transmitted over a network, or to protect data when it is stored on a device.
- **Digital signature:** Digital Signature is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.
- **Traffic padding:** Traffic Padding is a technique used to add extra data to a network traffic stream in an attempt to obscure the true content of the traffic and make it more difficult to analyze.
- **Routing control:** Routing Control allows the selection of specific physically secure routes for specific data transmission and enables routing changes, particularly when a gap in security is suspected.

3. Security Services

Security services refer to the different services available for maintaining the security and safety of an organization. They help in preventing any potential risks to security. Security services are divided into 5 types:

- **Authentication:** Authentication is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.
- **Access control:** Access Control involves the use of policies and procedures to determine who is allowed to access specific resources within a system.
- **Data Confidentiality:** Data Confidentiality is responsible for the protection of information from being accessed or disclosed to unauthorized parties.
- **Data integrity:** Data Integrity is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.
- **Non- repudiation:** Non-repudiation involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message.

Benefits of OSI Security Architecture

- **Providing Security**: OSI Architecture in an organization provides the needed security and safety, preventing potential threats and risks.
- **Organising Task:** The OSI architecture makes it easy for managers to build a security model for the organization based on strong security principles.
- **Meets International Standards:** Security services are defined and recognized internationally meeting international standards.
- **Interoperability:** By dividing network functions into multiple levels, the OSI model makes it easier for different hardware and software components to work together.
- **Scalability:** The layered method makes networks scalable. New technologies and protocols can be seamlessly added without interrupting the overall system.
- **Flexibility:** Each layer can evolve separately, providing flexibility for technology and application changes.