Harshita Sati

Overview of Session Layer:

The Session Layer is the 5th layer in the Open System Interconnection (OSI) model. This layer allows users on different machines to establish active communications sessions between them. It is responsible for establishing, maintaining, synchronizing, terminating sessions between end-user applications. In Session Layer, streams of data are received and further marked, which is then resynchronized properly, so that the ends of the messages are not cut initially and further data loss is avoided. This layer basically establishes a connection between the session entities. This layer handles and manipulates data which it receives from the Session Layer as well as from the Presentation Layer.

Session Layer Protocols :

Session Layer uses some protocols which are required for safe, secure and accurate communication which exists between two-ender user applications.

Following are some of the protocols provided or used by the Session Layer –

- AppleTalk Data Stream Protocol (ADSP): ADSP is that type of protocol which was developed by Apple Inc. and it includes a number of features that allow local area networks to be connected with no prior setup. This protocol was released in 1985.

- Real-time Transport Control Protocol (RTCP): RTCP is a protocol which provides out-of-band statistics and control information for an RTP (Real-time Transport Protocol) session. RTCP's primary function is to provide feedback on the quality of service (QoS) in media distribution by periodically sending statistical information such as transmitted octet and packet counts or packet loss to the participants in the streaming multimedia session.

- Point-to-Point Tunneling Protocol (PPTP): PPTP is a protocol which provides a method for implementing virtual private networks. PPTP uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP (Point-to-Point Protocol) packets.

- Password Authentication Protocol (PAP): Password Authentication Protocol is a password-based authentication protocol used by Point to Point Protocol (PPP) to validate users. Almost all network operating systems, remote servers support PAP. PAP authentication is done at the time of the initial link establishment and verifies the identity of the client using a two-way handshake (Client-sends data and server in return sends Authentication-ACK (Acknowledgement) after the data sent by client is verified completely).

- Remote Procedure Call Protocol (RPCP): Remote Procedure Call Protocol (RPCP) is a protocol that is used when a computer program causes a procedure (or a sub-routine) to execute in a different address space without the programmer explicitly coding the details for the remote interaction.
- Sockets Direct Protocol (SDP): Sockets Direct Protocol (SDP) is a protocol that supports streams of sockets over Remote Direct Memory Access (RDMA) network fabrics.The purpose of SDP is to provide an RDMA-accelerated alternative to the TCP protocol. The primary goal is to perform one particular thing in such a manner which is transparent to the application.

Common attack Vectors :

Sometimes also known as cookie hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

These explosions can be carried out by these attacks-

- Cross-site scripting: XSS attacks enable attackers to inject client-side scripts into web pages. It causes running codes, which is treated as trustworthy because it appears to belong to the server, on the victim computer. It allows the attacker to obtain a copy of the cookie or perform other operations.
- Session side jacking: where the attacker uses packet sniffing to read network traffic between two parties to steal the session cookie.
- Malware and unwanted programs can use browser hijacking to steal a browser’s cookie files without a user’s knowledge.

Case studies on session layer attacks :

Attacks targeting the session layer are relatively rare compared to other layers, they can still pose significant security risks. Here's a case study highlighting session layer attacks and their implications over the years:

1. In 2007, a session hijacking attack known as the Firesheep attack gained prominence. This attack exploited the lack of encryption on unsecured Wi-Fi networks, allowing attackers to intercept session cookies and gain unauthorized access to users' online accounts.

2. Session fixation is an attack where an attacker forces a user's session identifier (SID) to a known value, enabling them to hijack the session later. In 2011, an exploit was discovered in a widely used open-source PHP framework called CodeIgniter. This vulnerability allowed attackers to set the session ID before the session was created, potentially granting them unauthorized access to user accounts.

3. Session sidejacking, also known as session sniffing or session hijacking over non-secure connections, refers to attackers intercepting and stealing session cookies transmitted over unencrypted networks. In 2014, a security researcher demonstrated the ease of performing session sidejacking using a tool called Firesheep. The researcher highlighted the importance of using secure connections (HTTPS) to protect session data.

Mitigation strategies:

To mitigate session layer attacks and enhance the security of communication sessions, several strategies can be implemented. Here are some common mitigation strategies for the session layer:

- Encryption: Implement strong encryption protocols, such as Transport Layer Security (TLS) or Secure Socket Layer (SSL), to protect session data from unauthorized access or interception. Encryption ensures the confidentiality and integrity of session information.

- Secure Session Management: Implement robust session management practices, including session timeouts, strong session ID generation, and secure session storage. Session timeouts automatically terminate idle sessions, reducing the risk of session hijacking or fixation.

- Two-Factor Authentication (2FA): Implement 2FA to add an extra layer of security to session authentication.By requiring users to provide a second form of verification, such as a one-time password (OTP) or biometric authentication, the risk of unauthorized access to sessions is significantly reduced.

- Secure Cookie Handling: Use secure techniques for handling session cookies. Ensure that session cookies are marked as secure and have the "Secure" attribute set, meaning they are only transmitted over secure (HTTPS) connections.

Future trends and emerging dangers on session layer:

As technology continues to advance, new trends and emerging dangers on the session layer are likely to emerge. Here are some potential future trends and emerging dangers to consider:

- Internet of Things (IoT) Security: With the proliferation of IoT devices, session layer security becomes crucial. IoT devices often communicate through sessions, and vulnerabilities in session management could lead to unauthorized access, data breaches, or device manipulation.

- Quantum Computing Threats: Quantum computing has the potential to break many of the cryptographic algorithms that currently secure session layer communications.

- 5G Network Vulnerabilities: The rollout of 5G networks brings increased speed and connectivity, but it also introduces new security challenges. As session management protocols evolve to support 5G networks, it becomes crucial to address potential vulnerabilities that may arise from the complex network architecture and increased attack surface.

- Session-Based Attacks on Cloud Infrastructure: Cloud computing has become a popular choice for businesses, and session-based attacks targeting cloud infrastructure can have severe consequences. Attackers may attempt session hijacking, session fixation, or session DoS attacks to compromise cloud-based services.