TRANSPORT LAYER

1.INTRODUCTION

The transport layer is one of the seven layers in the OSI (Open Systems Interconnection) model, which is a conceptual framework used to understand and describe how different network protocols interact and work together. The transport layer is responsible for ensuring reliable and efficient end-to-end communication between applications running on different hosts (computers) in a network.

1.1FUNCTIONS OF TRANSPORT LAYER

1. **Segmentation and reassembly: T**he transport layer breaks down data received from the session layer into smaller units called segments or datagrams. It also reassembles these segments at the receiving end to deliver the complete data to the session layer.

2. **Connection establishment, maintenance, and termination:** The transport layer provides mechanisms for establishing and terminating connections between applications. It manages the flow of data and ensuresthat data is reliably transmitted between the sender and the receiver.

3. **Error detection and correction:** The transport layer detects errors in the received data and takes corrective measures to ensure data integrity. It uses techniques like checksums to verify the integrity of the data and retransmits any lost or corrupted segments.

4. **Flow control:** The transport layer manages the flow of data between the sender and receiver to prevent the receiver from being overwhelmed by a fast sender. It regulates the rate at which data is sent, ensuring efficient and reliable transmission.

5. **Multiplexing and demultiplexing**: The transport layer enables multiple applications to use the network simultaneously by assigning unique identifiers to each application. These identifiers, called port numbers,allow the transport layer to deliver the data to the appropriate application on the receiving host.

1.2 TRANSPORT LAYER PROTOCOLS

1. **Transmission Control Protocol (TCP)**: TCP provides reliable, connection-oriented communication. It ensures that data is delivered in the correct order and guarantees its reliability through mechanisms like acknowledgment, retransmission, and flow control. TCP is commonly used for applications that require error-free and ordered delivery of data, such as web browsing, email, and file transfer

2. **User Datagram Protocol (UDP**): UDP is a connectionless, unreliable transport protocol. It provides a simple and lightweight communication mechanism without the overhead of establishing and maintaining connections. UDP is often used for real-time applications like video streaming, voice-over-IP (VoIP), and online gaming, where speed and low latency are more important than reliability.

1.3 WORKING PROCEDURE OF TCP PROTOCOL

1. **Connection establishment:** Before any data transfer can occur, the web browser and the web server establish a TCP connection. This involves a three-way handshake, where the browser and server exchange control messages to synchronize and agree on communication parameters.

2. **Data segmentation and reassembly:** The web browser divides the web page data into smaller segments and adds a TCP header to each segment. These segments are then passed down to the network layer for transmission.

3. **Reliable data transfer:** TCP ensures reliable delivery of the data. It employs mechanisms like sequence numbers, acknowledgments, and retransmission of lost or corrupted segments to guarantee that the webpage data arrives at the browser in the correct order and without errors.

4. **Flow control:** TCP manages the flow of data between the browser and the server. It ensures that the server does not overwhelm the browser with data by regulating the rate at which segments are sent. If the browser's receiving buffer becomes full, TCP signals the server to slow down its transmission rate.

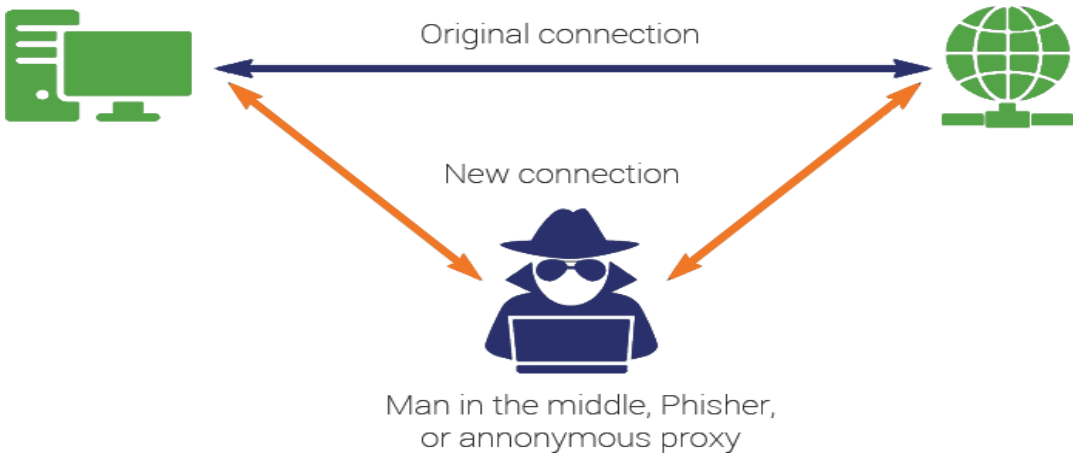
5. **Connection termination: O**nce the web page has been fully transferred, the TCP connection is terminated. This involves a four-way handshake, where both the browser and the server exchange control messages to close the connection gracefully.

By handling the reliable and ordered delivery of data between the browser and the web server, the transport layer (TCP) enables the successful retrieval and display of web pages over the internet.

1.4 TYPES OF ATTACK ON TRANSPORT LAYER OF OSI MODEL

1. **Denial of Service (DoS)** attacks: These attacks aim to disrupt the availability of network services by overwhelming the target system or network with a flood of traffic. In the transport layer, attackers may launch a flood of connection requests (SYN flood) or flood the target with excessive data (UDP flood or TCP flood). This can exhaust system resources, making the network or service inaccessible to legitimate users.

2. **Man-in-the-Middle attacks**: In a MitM attack, an attacker intercepts and alters the communication between two parties without their knowledge. In the transport layer, an attacker can intercept TCP connections and act as a proxy, capturing or manipulating the data transmitted between the parties. This allows the attacker to eavesdrop on sensitive information, inject malicious content, or impersonate one of the parties involved.



3. **TCP session hijacking:** TCP session hijacking involves an attacker gaining unauthorized access to an established TCP session. By intercepting and manipulating packets, the attacker can take control of the session, bypassing authentication mechanisms. This can lead to unauthorized access, data tampering, or session termination.

4. **TCP/IP spoofing:** In TCP/IP spoofing attacks, the attacker falsifies the source IP address in the TCP packets to impersonate a trusted entity. By spoofing the IP address, the attacker can deceive the recipient into thinking that the packets originate from a legitimate source. This can be used for various malicious purposes, such as bypassing access controls, launching DoS attacks, or gaining unauthorized access.

5. **SYN/ACK flooding:** This type of attack targets the TCP three-way handshake process. By flooding the target system with a large number of SYN or SYN/ACK packets, the attacker aims to exhaust the system's resources, leading to a denial of service. The target system becomes overwhelmed with pending connection requests, making it difficult for legitimate connections to be established

CONCLUSION

These are just a few examples of attacks that can occur at the transport layer. It's important to note that the security of the transport layer protocols (e.g., TCP and UDP) can be strengthened through various measures such as encryption (e.g., TLS/SSL) and implementing proper network security practices to mitigate these attacks.