CMR INSTITUTE OF TECHNOLOGY	USN									

Sub: Network Security Code:

Date: 20/11/2024 Duration: 90 mins Max Marks: 50 Sem: 7th Branch:

Marks

1. Explain the phases of the SSL/TLS handshake protocol to establish secure communication between a client and a server? [10]

Answer:

The SSL/TLS handshake is a multi-step process used to establish a secure communication channel between a client and a server. The handshake involves the following phases:

1. Hello Phase (ClientHello and ServerHello)

ClientHello:

The client initiates the handshake by sending a ClientHello message to the server.

This message includes:

Supported SSL/TLS versions.

Supported cipher suites (encryption algorithms).

A randomly generated value (client random).

ServerHello:

The server responds with a ServerHello message.

This message includes:

The SSL/TLS version and cipher suite selected by the server.

2. A randomly generated value (server random).

Certificate Exchange and Server Authentication

The server sends its digital certificate to the client. This certificate:

Confirms the server's identity using a trusted Certificate Authority (CA).

Contains the server's public key and information about the server.

If mutual authentication is required, the server might request the client's certificate at this stage.

3. Key Exchange and Pre-Master Secret Generation

Depending on the chosen cipher suite, the method for exchanging keys differs:

RSA Key Exchange:

The client encrypts a randomly generated pre-master secret using the server's public key and sends it to the server.

Diffie-Hellman (DH/ECDH):

Both the client and server exchange Diffie-Hellman public keys to compute a shared pre-master secret.

The pre-master secret is used by both parties, along with the client and server random values, to derive the session keys for encryption and integrity.

4. Server Finished

The server may send a ServerKeyExchange message (if additional key exchange parameters are needed).

The server sends a Finished message that includes a hash of all handshake messages exchanged so far. This ensures the handshake's integrity.

5. Client Finished

The client verifies the server's Finished message and sends its own Finished message.

This message also contains a hash of the handshake messages to confirm the integrity and successful completion of the handshake.

6. Secure Communication Begins

At this point, both the client and server have agreed on:

The encryption and hash algorithms (cipher suite).

Session keys for encrypting and authenticating the data.

Secure communication begins, with all subsequent messages encrypted using the agreed session keys.

2. What is HTTPS, and how does it enhance the security of HTTP? Explain the encryption mechanisms used and their significance. [10]

Answer:

HTTPS (Hypertext Transfer Protocol Secure) is a secure version of HTTP that uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols to encrypt the communication between a client (browser) and a web server. This ensures confidentiality, integrity, and authentication of the data exchanged over the internet.

1.Encryption (Confidentiality):

HTTPS encrypts the data transmitted between the client and server, making it unreadable to unauthorized parties, such as attackers or intermediaries.

This protects sensitive information like passwords, credit card numbers, and personal data from being intercepted (e.g., during a man-in-the-middle attack).

2.Authentication:

HTTPS uses digital certificates issued by trusted Certificate Authorities (CAs) to verify the identity of the server.

This ensures users are communicating with the intended server and not with a malicious actor impersonating it.

3.Integrity:

HTTPS ensures that the data transmitted is not altered or tampered with during transit.

TLS/SSL protocols use hash functions and message authentication codes (MACs) to detect any modifications.

Working of HTTPS:

Client sends an HTTPS request:

The browser requests a secure connection to the server.

SSL/TLS Handshake:

The server sends its SSL/TLS certificate to the client.

The client verifies the certificate's validity (via CA signatures).

A shared session key is securely exchanged using asymmetric encryption or Diffie-Hellman.

Encryption Mechanisms Used in HTTPS

Symmetric Encryption:

Once the handshake is complete, symmetric encryption is used for encrypting the actual data being transmitted.

A single shared key (session key) is used for both encrypting and decrypting the data.

Algorithms used: AES (Advanced Encryption Standard), ChaCha20, etc.

Significance:

Efficient for large amounts of data.

Provides fast and secure encryption for ongoing communication.

Asymmetric Encryption:

Used during the initial handshake process for secure exchange of the symmetric session key.

Involves a pair of keys: a public key (for encryption) and a private key (for decryption).

Algorithms used: RSA, ECDSA, etc.

Significance:

Ensures that the session key is securely shared between the client and the server.

Key Exchange Algorithms:

Securely negotiates the session key using algorithms like:

Diffie-Hellman (DH/ECDH): Provides perfect forward secrecy (PFS), ensuring that even if the private key is compromised, past sessions remain secure.

Significance:

Prevents interception or tampering with the session key exchange.

Message Authentication (Integrity):

Uses cryptographic hash functions (e.g., SHA-256) and Message Authentication Codes (MACs) to verify data integrity.

Significance:

Ensures that data is not altered or corrupted during transmission.

3.a) Discuss the role of the SSL Record Protocol in ensuring confidentiality and message integrity. How does it process and secure application messages? [05]

Answer:

The SSL Record Protocol provides two services for SSL connections:

Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.

Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment.

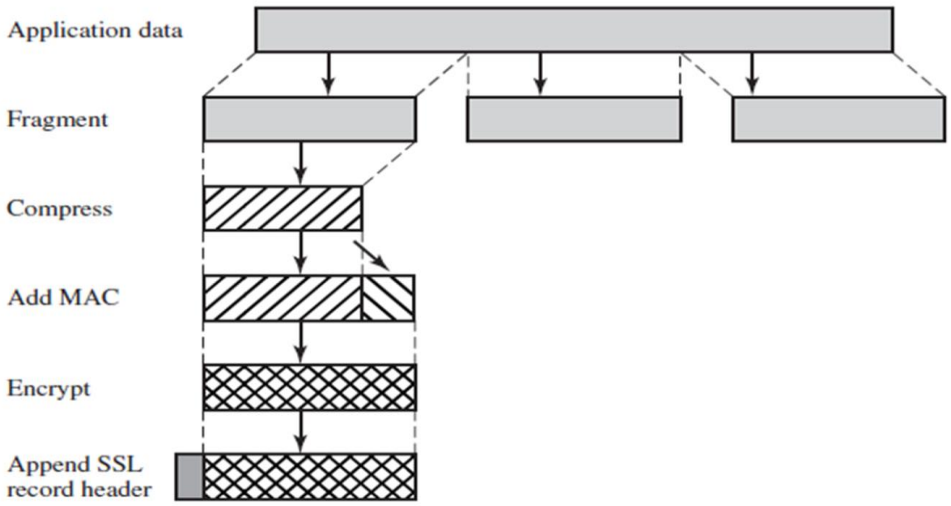

Figure 17.3 SSL Record Protocol Operation

b) What is the significance of the AH and ESP in IPsec? How do they differ in providing security? [05]

Answer:

The Authentication Header (AH) and Encapsulating Security Payload (ESP) are two core protocols in the IPsec (Internet Protocol Security) suite, designed to provide security for IP communications. They offer distinct functionalities and differ in the types of security they provide.

Authentication Header (AH)

AH provides integrity, data origin authentication, and optional anti-replay protection for IP packets. However, it does not provide confidentiality (encryption of the payload).

Key Features:

Integrity:

Ensures that the data has not been tampered with during transit.

Uses cryptographic hash functions (e.g., HMAC with SHA-256) to calculate a hash over the packet.

Authentication:

Verifies the source of the packet to ensure it is from a trusted sender.

Helps prevent spoofing attacks.

Anti-Replay Protection:

Prevents attackers from re-sending captured packets by using sequence numbers.

Modes:

Transport Mode:

Only the payload and some header fields are authenticated.

Tunnel Mode:

The entire IP packet (header + payload) is authenticated and encapsulated in a new IP header.

Encapsulating Security Payload (ESP)

ESP provides confidentiality (encryption), in addition to integrity, authentication, and

optional anti-replay protection. It is commonly used when encryption of the payload is required.
Confidentiality:
Encrypts the packet's payload to ensure it cannot be read by unauthorized parties.
Uses symmetric encryption algorithms such as AES (Advanced Encryption Standard).
Integrity:
Similar to AH, ensures the payload is not tampered with during transit.
Authentication:
Verifies the source of the packet, though this applies only to the payload, not the outer IP header.
Anti-Replay Protection:
Like AH, ESP also includes mechanisms to prevent replay attacks.

4. Explain the process of Internet Key Exchange in IPsec, the role of the Diffie-Hellman algorithm, and how it addresses various security challenges. [10]

Answer:
The Internet Key Exchange (IKE) is a protocol used in IPsec to establish a secure and authenticated communication channel between two parties. It automates the negotiation and management of cryptographic keys, ensuring secure communication.
The Diffie-Hellman (DH) algorithm is fundamental to IKE for secure key exchange. It enables two parties to agree on a shared secret over an insecure channel without exposing the secret to eavesdroppers.

How DH Works in IKE:

1. Both parties agree on common parameters:
   - A large prime number p and a base g (publicly known values).
2. Each party generates a private key:
   - Party A generates a secret a and computes $A = g^a \mod p$.
   - Party B generates a secret b and computes $B = g^b \mod p$.
3. Public keys are exchanged:
   - Party A sends A to Party B, and Party B sends B to Party A.
4. Each party computes the shared secret:
   - Party A computes $S = B^a \mod p$.
   - Party B computes $S = A^b \mod p$.

both parties derive the same shared secret *S*

5.a) Explain the role of IPsec and its three functional areas. Discuss the applications of IPsec in modern networks. [06]

Answer:
IPsec (Internet Protocol Security) is a suite of protocols that provides security for data transmitted over IP networks. It operates at the network layer, ensuring secure communication between devices across networks. IPsec can protect all application data, regardless of the underlying application,
Three Functional Areas of IPsec
Authentication:
Ensures that data is sent and received by verified parties.
Prevents impersonation (spoofing) attacks.
Uses the Authentication Header (AH) to provide data origin authentication and integrity.
Digital signatures and hash functions (e.g., HMAC with SHA-256) are used to verify the authenticity of the sender.

Confidentiality:
Ensures that data remains private during transmission.
Protects against eavesdropping or unauthorized access.
Uses the Encapsulating Security Payload (ESP) protocol to encrypt the payload of IP packets.
Prevents sensitive information from being intercepted or exposed.
Integrity:
Ensures that data is not altered during transmission.
Protects against tampering or modification attacks.
Both AH and ESP use cryptographic hash functions to detect any modifications to the data.
Message authentication codes (MACs) ensure that tampered data is rejected.
Detects and mitigates data corruption or unauthorized modifications.
Applications of IPsec in Modern Networks:
Virtual Private Networks
Secure Branch Connectivity

b) Compare and contrast the Transport and Tunnel Modes of IPsec. [04]

Answer:

Aspect	Transport Mode	Tunnel Mode
Encryption Scope	Only the payload is encrypted.	Entire original IP packet (header + payload) is encrypted.
Original IP Header	Retained and visible.	Encrypted and hidden.
Overhead	Lower, as only the payload is secured.	Higher, due to encryption of the full packet and addition of a new header.
Use Case	Host-to-host communication.	Gateway-to-gateway or site-to-site communication.