جامـــــعة المـــستـقـبـل
AL MUSTAQBAL UNIVERSITY

قـســــم الامــــــــــن الــــــــــــــــــسيبرانــــــــــــــــــي

Department of Cyber Security

Subject:

Authentication and access control

Class:

second

Lecturer:

Dr. Suha Alhussieny

Lecture: (6.2)

SSL/TLS Handshake

A session state is defined by the following parameters:-

- **Session identifier**: An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
- **Peer certificate**: An X509.v3 certificate of the peer. This element of the state may be null.
- **Compression method**: The algorithm used to compress data prior to encryption.
- **Cipher spec**: Specifies the bulk data encryption algorithm (such as null, AES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash size.
- **Master secret**: 48-byte secret shared between the client and server.
- **Is resumable**: A flag indicating whether the session can be used to initiate new connections.

A connection state is defined by the following parameters.

- **Server and client random**: Byte sequences that are chosen by the server and client for each connection.
- **Server write MAC secret**: The secret key used in MAC operations on data sent by the server.
- **Client write MAC secret**: The secret key used in MAC operations on data sent by the client.

- **Server write key**: The secret encryption key for data encrypted by the server and decrypted by the client.
- **Client write key**: The symmetric encryption key for data encrypted by the client and decrypted by the server.
- **Initialization vectors**: When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol. Thereafter, the final ciphertext block from each record is preserved for use as the IV with the following record.
- **Sequence numbers**: Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero. Sequence numbers may not exceed $2^{64} - 1$.

SSL/TLS Handshake

The **Handshake Protocol** is the process by which the **client** (usually a web browser) and the **server** (a website) establish a **secure, encrypted communication channel**. It happens *before* any actual data is exchanged.

Main Goals of the Handshake:

1. Authenticate the communicating parties (especially the server).
2. Agree on a set of cryptographic algorithms to use.
3. Generate a shared secret key to encrypt data securely

Step-by-Step Process

1- **Client Hello :** The client sends a "hello" message containing supported cryptographic algorithms, a random number, and protocol version (e.g., TLS 1.3).
2- **Server Hello :** The server responds with its own random number, chosen cryptographic algorithms, and its **digital certificate (X.509)** that contains its public key.
3- **Server Authentication :** The client verifies the server's certificate using a trusted **Certificate Authority (CA)**. If valid, it confirms the server's identity.
4- **Key Exchange :** The client and server exchange data to generate a **session key** (e.g., using RSA, Diffie–Hellman, or ECDHE).
5- **Client Authentication (optional) :** Some servers may also request a client certificate for two-way authentication (mutual TLS).
6- **Finished Messages :** Both parties send an encrypted "Finished" message to confirm that the handshake succeeded.
7- **Secure Session Established :** From now on, all communication is encrypted using the shared session key.

SSL Record Protocol

The **SSL Record Protocol** is the core layer of SSL/TLS responsible for **securing and managing the actual data transmission** between the client and the server. While the **Handshake Protocol** establishes a secure *session* and negotiates the cryptographic parameters, the **Record Protocol** operates during the *connection*

phase to ensure that all application data (e.g., web pages, emails, login information) is transmitted **confidentially and intact**.

Main Goal:

To provide ***confidentiality***, ***integrity***, and ***authentication*** for the data exchanged after the handshake is completed.

Step-by-Step Process

1- **Fragmentation** : The protocol divides large messages into smaller blocks called *records* (typically up to 16 KB) to simplify encryption and transmission.
2- **Compression (optional) :** Each record can be compressed to reduce its size and improve efficiency. However, in modern TLS versions, compression is usually disabled to avoid security attacks (e.g., CRIME attack).
3- **Message Authentication Code (MAC) or AEAD Tag :** A *MAC* or an *Authenticated Encryption Tag* is added to ensure **integrity** — that no attacker has modified the message.
4- **Encryption :** The record is encrypted using symmetric encryption (e.g., AES, ChaCha20, or 3DES) with the keys generated during the Handshake phase.
5- **Transmission :** The encrypted records are sent over the TCP connection to the receiver.

On the receiving side: The Record Protocol reverses these steps — decrypts the data, verifies the MAC, decompresses (if needed), and reassembles the message before delivering it to the application layer.

Figure below indicates the overall operation of the SSL Record Protocol.

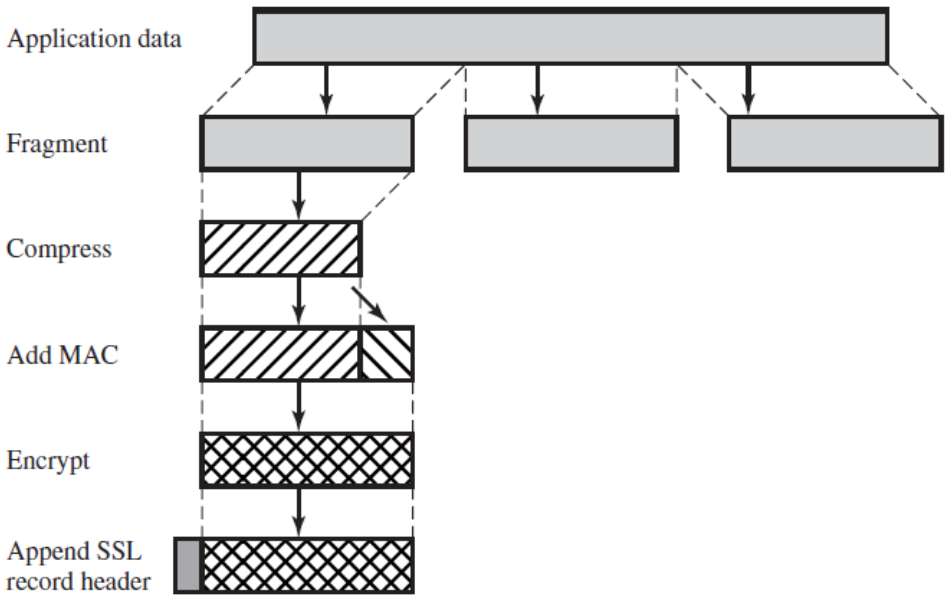

Figure /SSL Record Protocol Operation

H.W/

1. What is the main purpose of TLS and SSL protocols?
A. To compress data B. To provide secure communication over a network
C. To increase transmission speed D. To manage routing tables E. To translate IP addresses
Correct Answer: B

2. Which protocol provides security services between TCP and applications that use TCP?
A. IPsec B. HTTPS C. SSL D. SSH E. DNS
Correct Answer: C

3. What type of encryption is used by SSL/TLS for confidentiality?
A. Asymmetric encryption B. Hashing C. Symmetric encryption D. Quantum encryption
E. None of the above
Correct Answer: C

4. Which of the following provides message integrity in SSL/TLS?
A. MAC B. RSA C. AES D. HTTPS E. TLS record
Correct Answer: A

5. HTTPS stands for:
A. Hyper Text Transfer Packet System B. High Transfer Protocol Secure C. Hypertext Transfer Protocol Secure D. Hypertext Transmission Protocol Service E. None of these
Correct Answer: C

6. Which protocol provides secure remote logon and other secure client/server facilities?
A. IPsec B. SSH C. SSL D. TLS E. DNSSEC
Correct Answer: B

7. The SSL Record Protocol operates during which phase?
A. Session phase B. Connection phase C. Initialization phase D. Handshake phase E. Authentication phase
Correct Answer: B

8. Which layer protocol does SSL use to provide reliable service?
A. UDP B. IP C. TCP D. ICMP E. HTTP
Correct Answer: C

9. What is an SSL session?
A. A temporary connection between client and server B. A permanent connection
C. An association defining cryptographic parameters between client and server
D. A process for routing packets E. None of these
Correct Answer: C

10. What does the SSL Handshake Protocol mainly establish?
A. IP addresses B. Secure and encrypted session C. DNS records D. Data compression scheme
E. Routing paths
Correct Answer: B

11. In the Handshake Protocol, the message 'Client Hello' contains:
A. Server random number B. Encryption key only C. Supported algorithms and random number
D. Session certificate E. None of these
Correct Answer: C

12. The certificate used for server authentication in TLS is:
A. X.400 B. X.509 C. X.25 D. SHA-1 E. PGP
Correct Answer: B

13. The session key in SSL/TLS is generated using which phase?
A. Key Exchange phase
B. Record phase
C. Session state phase
D. MAC phase
E. None
Correct Answer: A

14. What does MAC stand for in SSL/TLS?
A. Message Authentication Code
B. Main Access Control
C. Media Access Channel
D. Multiple Authentication Cipher
E. Modular Algorithmic Code
Correct Answer: A

15. What happens after the SSL handshake is completed successfully?
A. The session is terminated
B. All communication becomes encrypted
C. Only authentication continues
D. Compression begins
E. None
Correct Answer: B

16. The SSL Record Protocol divides large messages into smaller units called:
A. Keys B. Packets C. Records D. Frames E. Blocks
Correct Answer: C

17. Which of the following is TRUE about TLS compression?
A. Always used for efficiency B. Disabled in modern TLS to prevent attacks C. Required by HTTPS
D. Increases packet size E. None
Correct Answer: B

18. The Handshake Protocol uses which type of encryption algorithms?
A. Symmetric only

B. Asymmetric only
C. Both symmetric and asymmetric
D. Hash functions only
E. Stream ciphers only
Correct Answer: C

19. The master secret in SSL session is how many bytes long?
A. 16 bytes B. 24 bytes C. 32 bytes D. 48 bytes E. 64 bytes
Correct Answer: D

20. Which field in SSL maintains sequence numbers for transmitted messages?
A. Initialization vector
B. Cipher spec
C. Session identifier
D. Sequence numbers field
E. Peer certificate

Correct Answer: D

Answer Key

1. B
2. C
3. C
4. A
5. C
6. B
7. B
8. C
9. C
10. B
11. C
12. B
13. A
14. A

15. B
16. C
17. B
18. C
19. D
20. D