[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Manas Jitendrakumar Ingle (202151086)

Winter 2023-2024
Lecture (Week 12)

1 Secured Sockets Layer Protocol

The Secure Socket Layer (SSL) is a cryptographic protocol designed to provide secure communication over a computer network. It ensures privacy, integrity, and authentication of data transmitted between a client and a server. SSL uses cryptographic algorithms to encrypt data, preventing unauthorized access and tampering. It's commonly used in web browsers for secure online transactions, such as online banking or shopping.

1.1 Symmetric Key Encryption Algorithms

Preferred for their computational efficiency compared to Public Key Cryptography.

1.2 Key Exchange Protocol, Signature Mechanism, and Message Authentication Code

Ensure secure communication, authentication, and integrity of transmitted data.

SSL, implemented in HTTPS, enables secure communication by facilitating key exchange, symmetric key encryption, public key authentication, and message authentication code verification between two parties.

1.2.1 Session

An SSL session represents a connection between a client and server, established through the Handshake protocol. It defines a collection of cryptographic security settings that can be utilized across various connections. A session state is defined by the following parameters:

1. Session identifier: An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
2. Peer certificate: An x509.v3 certificate from the peer, which may sometimes be absent. Typically, this certificate is signed by a certified authority to validate the correctness of the public key.
3. Compression method: The algorithm used to compress data prior to encryption.
4. Cipher Spec (Specification short form): It specifies the bulk data encryption algorithm (such as null, AES, etc.), a hash algorithm (such as MD5 or SHA-1) used for MAC calculation, a mechanism for key exchange (Diffie-Hellman, ECDH). It also defines cryptographic attributes such as the hash size.
5. Master secret key: 48-byte secret shared between the client and server used to generate certain keys such as key for encrypting the data and a key for generating MAC.
6. Is resumable: A flag indicating whether the session can be used to initiate new connections.

1.2.2 Connection

Parameters for connection state:

1. Server and client random: Byte sequences that are chosen by the server and client for each connection. These are generated individually at the client and the server side.
2. Server write MAC secret: The secret key used in MAC operations on data sent by the server.
3. Client write MAC secret: The symmetric key used in MAC operations on data sent by the client.
4. Server write key: The symmetric encryption key for data encrypted by the server and decrypted by the client.
5. Client write key: The secret encryption key for data encrypted by client and decrypted by server.
6. Initialization vectors: In CBC mode with a block cipher, each key is associated with an initialization vector (IV). This IV is initially set during the Handshake Protocol. Subsequently, the last ciphertext block from each record serves as the IV for the next record.
7. Sequence numbers: For each connection, both parties keep track of separate sequence numbers for messages sent and received. When a party sends or receives a "change cipher spec message," the relevant sequence number is reset to zero. Sequence numbers are limited to a maximum value of $2^{64} - 1$.

1.3 SSL Record Protocol

The SSL (Secure Sockets Layer) record protocol is responsible for fragmenting and encapsulating higher-level protocol data into manageable chunks called records for secure transmission over a network. It also handles encryption, authentication, and integrity checks of these records to ensure secure communication between the client and server. This protocol provides services for connection:

1. Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
2. Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

The list of encryption algorithms supported by SSL is given below:

- AES
- IDEA
- RC2-40
- DES-40
- DES
- 3DES

- Fortezza
- RC4-40
- RC4-128

The header contains the following information:

- Content Type (8 bits): The type of data
- Major Version (8 bits)
- Minor Version (8 bits)
- Compressed Length (16 bits): length of the compressed data

1.3.1 Change Cipher Spec Protocol

Another protocol within SSL is the Change Cipher Spec Protocol, which facilitates updating the encryption method used in a connection.

1.3.2 Alert Protocol

The Alert Protocol handles various alerts such as:

- unexpected message
- bad record mac
- decompression failure
- handshake failure
- illegal parameter
- close notify
- bad certificate
- unsupported certificate
- certificate revoked
- certificate expired
- certificate unknown

1.3.3 Handshake Protocol

The Handshake Protocol performs the handshaking between the two parties and generates a common secret key.

1.4 An Overview on Signal Protocol

In messaging applications, ensuring that messages are only readable by the intended recipient over a public channel requires End-to-End Encryption. In this setup, a server facilitates message transmission but remains unaware of the message content, as it lacks the ability to decrypt the messages. The encryption relies on a shared key exclusively known to the communicating parties.

1.4.1 Authenticated Encryption with Associated Data (AD)

- Associated Data (AD) is authenticated but not encrypted.
- Schemes are nonce-based (and deterministic).

Sender:

$$C = \text{Enc}(K, N, \text{AD}, M)$$

- K: key
- N: Nonce (random number to be only used once)
- AD: Associated Data
- M: Message

Receiver:

$$M = \text{Dec}(K, N, \text{AD}, C)$$

When sending a message along with an Additional Data (AD) over the server, the AD is transmitted without encryption. The receiver validates the received AD to ensure the integrity of the message. Thus, the AD serves to authenticate the source of the message.

1.4.2 Main Cryptographic modules of Signal Protocol

- X3DH (Extended Triple Diffie-Hellman)
- ECDSA
- Double Ratchet

X3DH facilitates shared key generation, while ECDSA signs public keys to prevent unauthorized production of valid keys on behalf of a user. The Double Ratchet algorithm is employed for encryption, generating unique keys for each message exchanged.

1.4.3 Registration

Alice registers himself to the Server. He has to provide the id to register.

Alice

- Identity key (IKA)
- Signed prekey (SPKA)
- Optionally, a set of one-time prekeys (OPK1A, OPK2A, OPK3A)

Bob

- Identity key (IKB)

1.4.4 Registration (Continued)

Server stores both the packets.

1.4.5 Key Exchange

Alice generates an ephemeral key (EKA) and performs Diffie-Hellman (DH) key exchange. Then, using the shared secret key (SKA), Alice encrypts the initial message, resulting in the generation of the corresponding initial ciphertext.

Bob

- Retrieves Alice's Identity Key (IKA) and her Encrypted Key (EKA)
- Engages in Diffie-Hellman (DH) key exchange
- Utilizes Key Derivation Function (KDF) with his secret keys, resulting in the generation of his shared secret key (SKB)
- Constructs the associated data (AD) and decrypts the initial ciphertext using SKB, along with AD, successfully recovering the original message