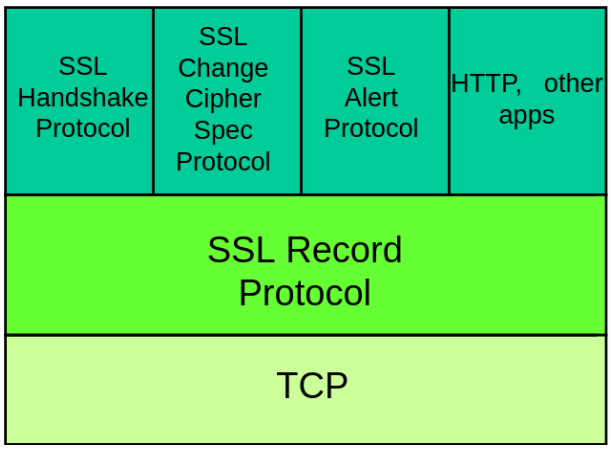
SSL/TLS Presentation

Federico Luisetto

May 26, 2021

1 What's SSL/TLS

Transport Layer Security (TLS), the successor of the now-deprecated Secure Sockets Layer (SSL), is a cryptographic protocol designed to provide communications security over a computer network. Several versions of the protocol are widely used in applications such as email, instant messaging, and voice over IP, but its use as the Security layer in HTTPS remains the most publicly visible.
The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications.
The TLS protocol comprises two layers: the SSL record protocol and the Upper Layer Carrying.



2 SSL Record Protocol

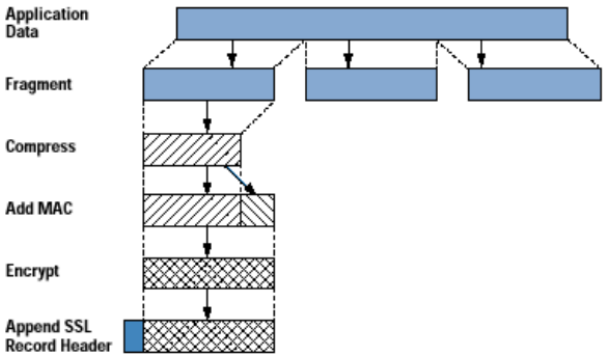
SSL Record Protocol provides secure, reliable channel for upper layer. It carries application data and SSL 'management' data.
It provides:

- Data origin authentication and integrity
  - MAC using algorithm similar to HMAC
  - Based on MD5 or SHA-1 hash algorithms
  - MAC protects 64 bit sequence number for anti-replay
- Confidentiality
  - Bulk encryption using symmetric algorithm
    - DEA, RC2-40, DES-40 (exportable), DES, 3DES
    - RC4-40 and RC4-128

Process:

1. Data from application/upper layer SSL protocol partitioned into fragments (max size 214 bytes)
2. MAC first then pad (if needed)
   - MAC (Message Authentication Code) is a short piece of information used to authenticate a message

3. Encrypt
4. Append header (Content type, version, length of fragment)
5. Submit to TCP



3 Upper Layer Carrying

3.1 SSL Handshake Protocol

1. Client *hello* packet
   - Client announces its capabilities (cipher list, compression methods, highest SSL/TLS version). es: TLS_RSA_WITH_3DES_EDE_CBC_SHA
   - Sends ClientNonce (28 random bytes plus 4 bytes of time)
   - Session ID
2. Server *hello* packet
   - Selects single ciphersuite from list offered by client es: TLS_RSA_WITH_3DES_EDE_CBC_SHA
   - Sends ServerNonce and SessionID
3. Server sends its public certificate to client
4. Server *hello done* packet
5. Client send `pre_master_secret` key to server
   - This key is encrypted using server's public key
6. Generation of symmetric key
   - Client and server generate the Master Secret and session keys based on the Pre-Master Secret
7. Update of ChipherSpec for this session
   - Client and server change the ChipherSpec to symmetric encryption using the session key

3.2 SSL Change Cipher Spec

The Change Cipher Spec Protocol is used to change the encryption being used by the client and server. It is normally used as part of the handshake process to switch to symmetric key encryption. The CCS protocol is a single message that tells the peer that the sender wants to change to a new set of keys, which are then created from information exchanged by the handshake protocol.

3.3 SSL Alert Protocol

The alert protocol is used to alert status changes to the peer. The primary use of this protocol is to report the cause of failure. Status changes include such things as error condition like invalid message received or message cannot be decrypted, as well as things like the connection has closed. One thing that TLS has over SSL is that TLS has more alert messages than SSL does.