SSL and fundamentals very-secure-web-server
Hardik Gupta

SSL (Secure Sockets Layer)

---

1. Protocol developed to secure connections/communication over the internet. Why Protocol? Protocol: set of rules/standards that define how data is transmitted between devices. SSL is also protocol as it defines such rules.
2. established encrypted link between server and client -most commonly a web server (website) and browser or mail service.
3. now replaced by TLS (Transport Layer Security)

Purpose: encrypts data transmitted between client and server to ensure sensitive info such as credit card numbers, personal info remains private. **Authentication**: provides a way for client to confirm identity of the server (through certificates issued by trusted certificate authorities).

Definitions

Server is any host/machine that hosts a service, website or application and waits for requests. Provides resources, services or data Web Server: Apache, Nginx Mail Server: Gmail, Outlook Server

Client is a device/application that initiates connection to server to access services/data. Requests access to those resources/services Browser: Chrome, Firefox Mail Client: Apple Mail

SSL Handshake

1. Server presents its SSL certificate to verify its identity
2. Client verifies the certificate against trusted CAs
3. A secure connection is established using symmetric key for faster encrypt-decrypt

Steps

1. Client sends:
   (a) a list of cipher suits that client supports
   (b) SLS version preference
   (c) random number used to generate symmetric key later
2. Server sends
   (a) cipher suite chosen
   (b) SLS version agreed upon
   (c) random number used in key generation
3. Now, client and server has agreed upon the encryption settings they will use.
4. Server now sends its digital certificate to client. This certificate contains:
   (a) Server's public key
   (b) Identity of server, signed by a trusted certificate
5. Client verifies,
   (a) Certificate is signed by trusted CA
   (b) Certificate's expiration data
   (c) Also matching server name to certificate
6. Client Key Exchange (Pre-Master Secret): Client creates this pre-master secret which only client knows and uses server public key (which only server can decrypt) to encrypt and sends to server.

Symmetric Key

Both have now:

- Client random
- Server random
- Pre-master Secret

Using these 3 values they compute session key and end up with identical symmetric keys on both sides and both now switch to symmetric key for further communication.

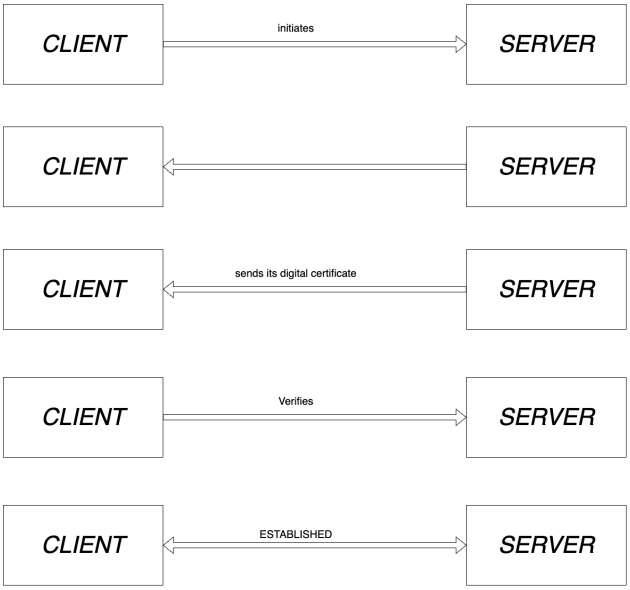

Figure 1: