Unit 2. Task 4: SSL Protocol

Javier Aguilera Aguilera 2º CFGS DAW

SSL protocol was created originally in the 90's by Netscape Communications. It avoids integrity and confidentiality attacks or authentication like Man-in-the-middle. When conexion isn't secure the attacker con modify the transit information or make an identification thief of the extremes. For example, with a HTTP session hijacking attack which consist of stealing the cookie session of the user allowing its suplantation. TLS is based on SSL with some protection improves.An example of ssl functioning is a simple tls handshake, It consists of a negotiation of the encrypt algoritmos, key interchange and authentication and cifrado of traffic. Phases:

1. Client Hello : Information that the server needs to communicate with the client using SSL. This includes the SSL version number, cipher settings, session-specific data.
2. Server Hello: Information that the server needs to communicate with the client using SSL. This includes the SSL version number, cipher settings, session-specific data.
3. Authentication and Pre-Master Secret: Client authenticates the server certificate
4. Decryption and Master Secret: Server uses its private key to decrypt the pre-master secret.
5. Encryption with Session Key: Both client and server exchange messages to inform that future messages will be encrypted.

SSL protocol has several applications in electronic commerce (safe payment) or to tunnel a complete network also called VPN.