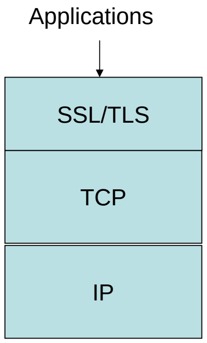
Secure Sockets Layer/ Transport Layer Security

General Principles

SSL/TLS and the OSI Model

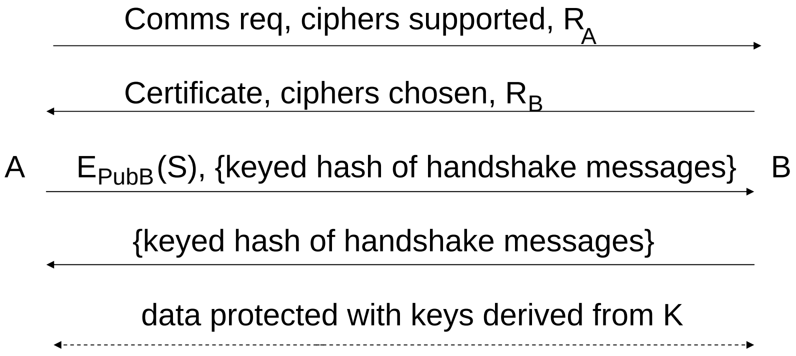


NB SSL/TLS designed to work on reliable transport protocol TCP and not UDP

Historical Overview

- SSL V2 produced by Netscape 1995 and later reworked as SSL V3
- TLS introduced by IETF following similar offering from Microsoft
- TLS required unencumbered algorithms such as Diffie-Hellman and DSS
- SSL V3 most commonly deployed, is similar to TLS, but non-interoperable

SSL/TLS Protocol (I)


Comms req, ciphers supported, R_A
Certificate, ciphers chosen, R_B
A
E_{PubB}(S), {keyed hash of handshake messages}
B
{keyed hash of handshake messages}
data protected with keys derived from K

$K = f(S, R_A , R_B)$ computed by A and B

SSL/TLS Protocol (II)

- A initiates session
- B sends public key certificate
- A verifies certificate and B’s public key
- A chooses random number S, the “pre-master secret”, and sends to B encrypted under B’s public key
- Various session keys derived from S
- Data privacy and integrity protected by session keys

SSL/TLS Protocol (III)

- First two messages provide crypto negotiation
- Random numbers R_A , R_B used in derivation of session keys
- $K = f (S, R_A , R_B)$ is the master key
- A, B include K and a text string in hash of handshake messages so that (a) they prove they know master, and (b) they have different proofs

SSL/TLS (IV)

- Session keys are encryption, integrity and IV in each direction – 6 in total
- B needs its own private key to find S and session keys and therefore authenticates itself with the keyed hash
- B does not authenticate A in standard protocol but authentication may be arranged outside protocol