TLS

Permette di stabilire un canale di comunicazione autenticato e cifrato tra un client e un server.

Handshake

Stabilisce chiavi simmetriche condivise, autentica il server e opzionalmente (ma raramente) anche il client.

Preparazione:

- il client C possiede un insieme di chiavi pubbliche di CA;
- il server S ha una coppia di chiavi $k_S[\text{pub}], k_S[\text{priv}]$ per la firma digitale e un certificato cert_S per $k_S[\text{pub}]$ rilasciato da una CA nota a C.

Il client avvia lo scambio di chiavi inviando in chiaro il messaggio iniziale del protocollo Diffie-Hellman, che include:

- il gruppo G ($\mathbb{Z}/p\mathbb{Z}^*$ o una curva ellittica) e il generatore/punto base g;
- g^x, calcolato con un x segreto scelto casualmente;
- un nonce (sequenza casuale di bit) N_C;
- cipher suite supportate

Il server:

- calcola e invia g^y, con un y segreto scelto casualmente;
- invia un nonce N_S;
- calcola $k = g^{xy}$ e applica una *key-derivation function* per estrarre da k le chiavi simmetriche k'_S, k'_C, k_S, k_C;
- invia $k_S[\text{pub}]$, cert_S, una firma σ calcolata con $k_S[\text{priv}]$ su tutti i messaggi dell'handshake inviati.

Tutti i dati sono inviati nello stesso momento *cifrati con* k'_S (eccetto g^y).

Il client:

- calcola k e deriva k'_S, k'_C, k_S, k_C;
- decifra la risposta del server con k'_S;
- verifica $k_S[\text{pub}]$ con cert_S;
- verifica la firma σ sui messaggi di handshake usando $k_S[\text{pub}]$;
- calcola il MAC dei messaggi di hasdshake scambiati usando k'_C e lo invia a S.

k'_S e k'_C sono utilizzate solo durante l'handshake.

Record layer

C usa k_C per cifrare e autenticare (MAC-then-encrypt) i messaggi che invia, S usa k_S. I record sono numerati.

Sicurezza

- C ha la certezza di comunicare con S perché verifica σ utilizzando una chiave pubblica certificata;
- DH garantisce la sicurezza contro attacchi passivi;
- C è in grado di individuare attacchi MITM perché conosce i messaggi inviati da entrambe le parti (ha ricevuto, firmata, la versione di S);
- TLS 1.3 (differenza delle versioni precedenti e di SSL) proibisce lo scambio della chiave tramite cifrario a chiave pubblica (cifrario ibrido) per garantire *forward secrecy*.