SSL

Protocollo che garantisce la *confidenzialità* delle trasmissioni attraverso internet: chiave di sessione per la cifratura simmetrica scambiata con cifrario simmetrico.

Su due livelli:

record livello più basso, connesso al protocollo di trasporto (TCP/IP): divide in blocchi, numera, autentica, cifra e invia i dati;

handshake crea un canale sicuro per la comunicazione: autenticazione, negoziazione degli algoritmi di cifratura e firma, creazione delle chiavi.

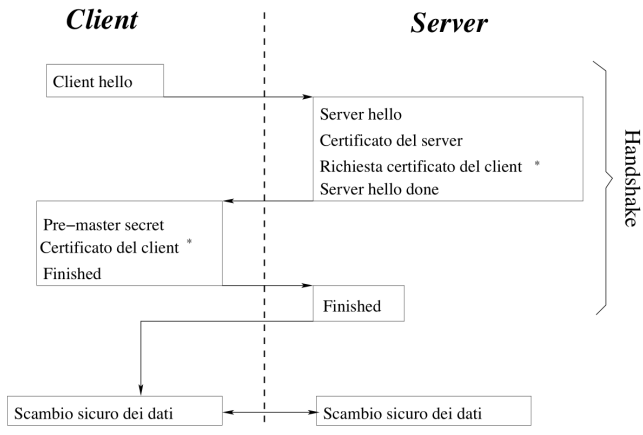
Handshake

Obiettivi:

- identificazione vicendevole di client e server;
- creazione congiunta delle chiavi segrete.

Protocollo:

- *client hello*: U richiede la creazione di una connessione SSL, specificando i cifrari e meccanismi di autenticazione supportati (*cipher suite*, e.g. `SSL_RSA_WITH_AES_CBC_SHA1`) e una sequenza di byte casuali;
- *server hello*: S seleziona una cipher suite compatibile e la comunica a U, insieme a una sequenza di byte casuali. Se U non riceve il *server hello* allora interrompe la comunicazione;
- S si autentica con U inviandogli il proprio certificato digitale (ed eventualmente i certificati della catena di certificazione dalla sua CA fino alla CA radice);
- S può chiedere a U di fornire un certificato, ma solitamente l'autenticazione dell'utente avviene a livello di applicazione (e.g. password);
- *server hello done*: S termina la fase di accordo su cipher suite e parametri;
- U autentica il certificato di S;
- U genera un *pre-master secret*, lo cifra con la chiave pubblica di S e lo spedisce;
- U calcola il *master secret* a partire dalle sequenze casuali dei due *hello* e dal *pre-master secret*;
- S riceve e decifra il *pre-master secret* e lo usa per calcolare il *master secret*;
- U invia il suo certificato se era stato richiesto, allegando cifrate (con la chiave pubblica di S) e firmate il master secret e tutti i messaggi scambiati fino a quel momento (*SSL-history*);
- S controlla il certificato e la SSL-history;
- *finished*: primo messaggio protetto con master secret e cipher suite accordati, inviato prima da U e poi da S. È un hash della concatenazione di master secret, SSL-history e identità del mittente;
- ciascun destinatario del *finished* lo calcola indipendentemente (ha a disposizione tutti i dati per farlo) e lo confronta con quello ricevuto (non può confrontare direttamente i dati perché riceve solo un hash);
- il master secret viene utilizzato per generare la chiave segreta per il cifrario simmetrico, quella per il MAC e il valore iniziale nel CBC. Client e server hanno due triple distinte con questi dati, e sono a conoscenza della tripla dell'altro.



Sicurezza

- il master secret dipende da dati casuali, quindi un crittoanalista non può catturare e riutilizzare i messaggi di handshake perché sono diversi per ogni sessione;
- SSL record autentica ogni blocco attraverso un MAC calcolato come hash della concatenazione di contenuto e numero del blocco, chiave del MAC e altre stringhe note. Il MAC viene cifrato, quindi modificarlo è tanto difficile quanto decifrare la comunicazione;
- immune ad attacchi MITM per l'utilizzo dei certificati, il messaggio *finished* garantisce un controllo finale. Non si può intercettare il *finished* e rispedirlo indietro perché nel calcolo dell'hash è inclusa anche l'identità del mittente;
- il pre-master secret viaggia cifrato, quindi solo S e U possono costruire il master secret.

È sicuro quanto il più debole cipher suite supportato.