TLS e SSH

Riccardo Longo

Sicurezza Online

- Internet è un canale insicuro
- Tramite *sniffing* della rete è facile intercettare le comunicazioni
- La complessità dell'architettura semplifica l'attuazione di attacchi del tipo Man In The Middle
- Serve integrare il protocollo di trasporto con uno che fornisce sicurezza

Obiettivi di Sicurezza

- Confidenzialità: le comunicazioni sono cifrate, i nuovi standard prevedono anche la *Forward Secrecy*
- Autenticazione: il client è sicuro dell'identità del server, prevenzione di MITM
- Integrità: la comunicazione è autenticata, assicurando l'integrità dei messaggi

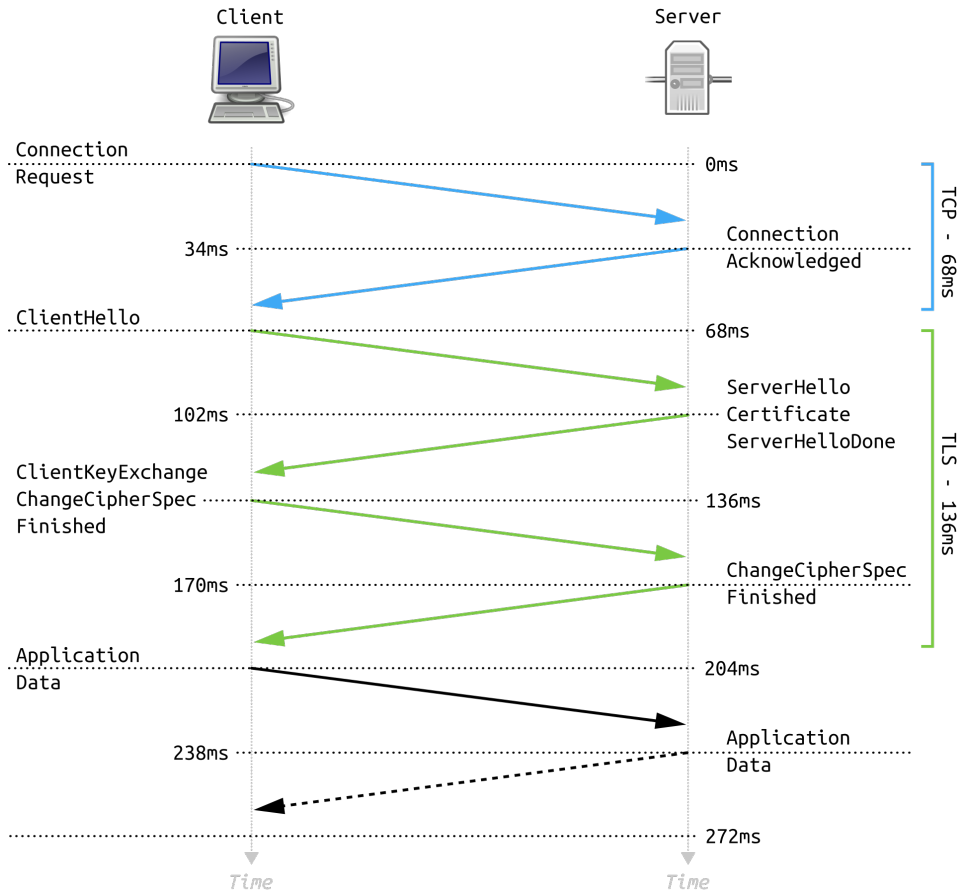
Negoziazione Protocolli

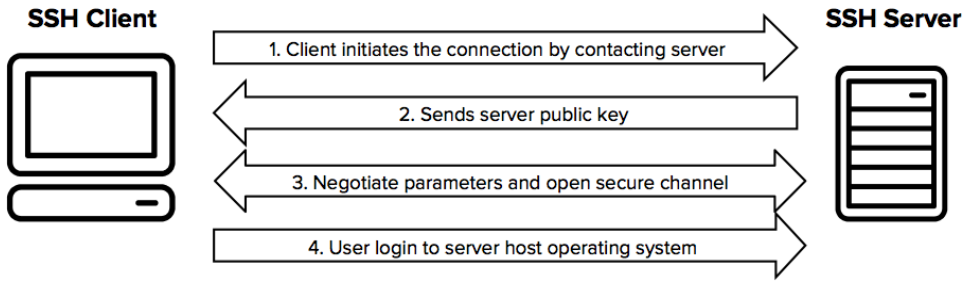
- Applicazioni e sistemi operativi diversi possono supportare differenti algoritmi crittografici
- L'obiettivo è ottenere alti livelli di compatibilità e di sicurezza
- una *ciphersuite* è un insieme di algoritmi crittografici che insieme permettono di istanziare il protocollo
  - cifrario simmetrico
  - firma digitale
  - key agreement
  - hash crittografica
- Ognuno dichiara quali algoritmi supporta, poi si seleziona una ciphersuite supportata da entrambi incrociando le liste e aggregando i migliori protocolli

Struttura Generale

- Il client inizia la connessione, comunica le ciphersuite che supporta
- Il Server risponde mandando:
  - Il proprio certificato
  - La ciphersuite selezionata
  - Il primo passaggio del *key agreement*
- Il client verifica il certificato e risponde completando il key agreement
- Entrambi calcolano la chiave di sessione
- Inizia la comunicazione cifrata, usando cifrari simmetrici autenticati (AEAD)

Struttura TLS e SSH





Handshake

- Allineamento sulla versione del protocollo
- Stabilimento ID di sessione *random*
- Negoziazione ciphersuite
- Autenticazione Server (e Client in alcuni casi)

Crittografia in TLS 1.3

Autenticazione Per autenticare lo scambio di chiavi

- ECDSA
- EdDSA
- RSA
- PSK (Pre-Shared Key)

Key Agreement Per stabilire chiavi di sessione (Forward Secrecy)

- ECDHE (Elliptic-Curve Diffie-Hellman Epehemeral)
- DHE (Diffie-Hellman Epehemeral)

Cifratura (AEAD) Per garantire confidenzialità ed integrità

- AES GCM
- AES CCM
- ChaCha20-Poly1305