Lecture TLS

Riccardo Torre

29 novembre 2025

TLS È un protocollo di sicurezza con l'obbiettivo di rendere una connessione TCP sicura, autentica. Kerberos lavora al livello applicativo, mentre TLS al livello di trasporto dello stack TCP/IP. Gli attacchi interessano i Web server. Se viene fornito come parte di TCP, tutti i servizi che lavorano con TCP ne fanno uso, o fornito come una dipendenza delle applicazioni. È il discendente di SSL.

Architettura dello stack protocollare Record protocol stabilisce come i pacchetti devono essere spediti criptati e autenticati. L'handshake protocol permette di comunicare i parametri di crittografia per creare la connessione sicura, l'alert protocol chiude una connessione quando avviene qualcosa di anomalo (MAC scorretto, certificato non supportato, fallimento dell'handshake), Change cipher protocol per cambiare la suite crittografica.

Record protocol Il dato viene tagliato in frammenti, che vengono compressi, a cui vengono aggiunti un MAC , criptati e a cui si aggiunge un TLS record header.

Sessione TLS Associazione di criteri su come client e server devono comunicare. Viene creata con l'handshake protocol. Definisce un insieme di parametri crittografici di sicurezza che possono essere condivise tra connessioni multiple. Le sessioni TLS vengono create per evitare la negoziazione dei parametri di sicurezza per ogni connessione perché è dispendioso.

Connssione TLS Sfruttando le informazioni crittografiche scambiate durante l'handshake. Le connessioni sono transienti; ciascuna connessione è associata ad un'unica sessione.

Stato di una sessione È caratterizzata da un identificatore di sessione, certificati x509.v3, metodi di compressione, specifiche degli algoritmi crittografici, un **master secret**[1], is resumable è un flag per riattivare una connessione se viene interrotta.

Stato di una connessione È caratterizzata dalle chiavi per calcolare i MAC del server e del client, e le relative chiavi per fare l'encryption, gli initialization vectors (stabiliti nell'handshake) che vengono utilizzati nel CBC (cipher block chain), e i sequence numbers per non perdere traccia della sequenza della comunicazione.

Servizi del Record Protocol Confidenzialità (AES e chiave segreta handhake protocol) e integrità (stabilendo durante l'hanshake protocol una chiave condivisa per formare i MAC).

L'handshake protocol

[1] chiamato così perché da esso vengono derivati diversi secret. È lungo 48 byte.