

1 Overview about TLS and IPsec

TLS ha come progenitore il protocollo SSL da un certo momento in poi cambiò nome a seguito di importanti aggiornamenti al protocollo. Nelle varie versioni di TLS hanno aggiunto notevoli funzionalità aggiuntive tra cui il supporto al protocollo di trasporto dati UDP, l'utilizzo (per poi esser abbandonati in TLS v.1.3) di algoritmi di encrypt come MD5 e SHA-1 ed infine, in TLS v.1.3 (la versione ad oggi in uso) di utilizzare i protocolli AEAD: protocolli che garantiscono confidenzialità e integrità dei dati. Dato che TLS utilizza TCP (o nella versione DTLS UDP), si assegna ad ogni processo una socket per rendere sicuri i dati di livello applicativo è considerato un protocollo che opera tra il livello di trasporto e il livello applicativo. Il suo nome, quindi, è fuorviante *Transport Layer Security*. Come vedremo in seguito questa possibilità di aprire una socket per ogni applicazione risulta problematica. Infine, TLS protegge solamente il payload di TCP e non l'intero pacchetto poiché per come è stato progettato, se così non fosse, non si saprebbe dove e a chi inviare i pacchetti. Da questo aspetto se ne conclude che l'header del pacchetto TCP può essere modificato e quindi si è soggetti ad attacchi di tipo TCP spoofing, MITM, CCA etc. . .

Un altro protocollo, sviluppato di pari passi a TLS, è IPsec. Esso viene considerato una versione molto più crittograficamente sicura e, data la problematica di TLS nell'utilizzare socket diverse per le varie applicazioni, si pone tra il livello di trasporto e di rete. Infatti, "monta" sopra IP e, grazie a questa proprietà, è possibile rendere crittograficamente sicuro l'intero pacchetto TCP/UDP/Altro incapsulando il pacchetto crittografato IP in un altro pacchetto così da nascondere l'intero contenuto di quello che si voleva mandare.

Da qui il concetto di **traffic flow confidentiality** che rappresenta un nuovo requisito di sicurezza: la cifratura del pacchetto deve aggiungere sicurezza al protocollo.

Una differenza tra TLS e IPsec è che nella loro progettazione hanno sviluppato il set-up dell'ambiente e il modo in cui si trasferiscono i dati in maniera differente. Questi due aspetti, infatti, rappresentano due concetti cardini nello sviluppo di un protocollo di sicurezza.

Quindi, TLS decise di unire il set-up dell'ambiente e il trasferimento di dati delegando il primo aspetto venne realizzato tramite una fase di handshake in cui si negoziano gli algoritmi e, tramite crittografia asimmetrica, si comunicano tali chiavi, necessarie a garantire integrità e confidenzialità, la seconda fase, invece viene detta record phase; mentre in IPsec, si decise di disaccoppiare questi due aspetti: la prima fase di set-up è delegata ad un protocollo automatico detto IKE (Internet Key Exchange); la seconda fase, di trasferimento dati delegata al protocollo utilizzato a supporto di IPsec.

2 TLS Protocol Stack