Azzolini Riccardo 2021-05-10

IPSec

1 Sicurezza in rete

La sicurezza in rete è un argomento molto ampio, poiché le problematiche di sicurezza sono affrontate in modi diversi a seconda di quali applicazioni devono girare su una rete. Alcuni dei principali meccanismi di sicurezza che la comunità Internet ha sviluppato per specifiche applicazioni sono:

- SSL/TLS per il Web;
- S/MIME e PGP per l'email;
- SSH per gli accessi remoti;
- FTPS (FTP con SSL) e SFTP (FTP su SSH) per il trasferimento dei file.

Nel seguito verranno analizzate tre delle soluzioni più significative, ciascuna relativa a un diverso livello della pila protocollare:

- livello di rete (network): IPSec;
- livello di trasporto: SSL/TLS;
- livello di applicazione: Kerberos (un protocollo di autenticazione).

2 Sicurezza a livello di rete

Al livello di rete si vogliono impedire la lettura e la modifica dei pacchetti IP in transito. In particolare, è necessario proteggere non solo il *payload*, ma anche l'*header*, perché alcuni dei possibili attacchi sono:

- la lettura dei payload, che (in assenza di altri meccanismi di sicurezza applicati ai livelli superiori) potrebbe contenere dati sensibili in chiaro;
- la contraffazione dei payload, che anche se cifrato ai livelli superiori potrebbe essere sostituito, o in generale modificato in qualche modo;
- la lettura degli indirizzi del mittente e del destinatario, che potrebbero fornire informazioni sui tipi di flussi di comunicazione che esistono tra diversi host nella rete, le quali potrebbero facilitare attacchi successivi;

- la modifica dell'indirizzo IP sorgente, al fine di falsificare l'identità del mittente (ad esempio un attaccante potrebbe fingere di essere un host che il destinatario considera fidato);
- la modifica dell'indirizzo IP di destinazione, ad esempio al fine di reindirizzare i pacchetti verso una macchina target per effettuare un attacco *denial of service*.

È importante notare che l'header IPv4 contiene già un checksum, ma questo serve solo a verificare l'assenza di *errori di trasmissione* sul *singolo hop*, da un nodo della rete al successivo, e non dal mittente al destinatario, perché il calcolo del checksum comprende il campo TTL (Time To Live), il cui valore viene decrementato a ogni hop, dunque anche il checksum varia a ogni hop e il destinatario non ha modo di sapere quale fosse il checksum generato dal mittente. Inoltre, il checksum non fornisce alcuna protezione contro modifiche intenzionali: esso non è cifrato in alcun modo (a differenza ad esempio di una firma digitale), dunque un attaccante che volesse modificare il pacchetto potrebbe sostituire liberamente il checksum con quello corretto per il pacchetto modificato.

3 IPSec

IPSec fornisce un framework (un insieme di elementi) per la comunicazione sicura su IP. Le sue specifiche sono complesse, definite in numerosi RFC. Esso deve obbligatoriamente essere supportato dalle implementazioni di IPv6, ma può essere usato anche con IPv4, e realizza servizi che riguardano tre aree:

- autenticazione;
- riservatezza/confidenzialità;
- gestione delle chiavi.

I servizi di autenticazione offerti da IPSec sono implementati tramite **intestazioni di estensione** (*extension header*) che seguono l'intestazione principale IP:

- **Authentication Header** (**AH**), che viene usato per l'autenticazione e integrità dei pacchetti e del flusso di traffico;
- **Encapsulating Security Payload** (**ESP**), che serve per la riservatezza dei contenuti dei pacchetti e del flusso di traffico.

AH e ESP possono essere utilizzati separatamente o insieme, e la presenza di queste intestazioni di estensione è segnalata:

- nell'header IPv4 usando il campo *Protocol*, nel quale si indica la prima delle intestazioni di estensione presenti invece di indicare normalmente il protocollo del pacchetto contenuto nel payload (ad esempio TCP);

- nell'header IPv6 usando il campo *Next Header*, che è analogo al campo Protocol di IPv4 ma è pensato appositamente per permettere l'uso di intestazioni di estensione.[1]

Siccome IPSec funziona al di sotto del livello di trasporto, esso è trasparente alle applicazioni e agli utenti finali.

4 Modalità trasporto e tunnel

AH e ESP possono essere utilizzati in due diverse modalità:

- **Trasporto**: AH e/o ESP vengono inseriti tra l'intestazione IP e il payload, e fornisce protezione solo al payload.[2] Nel caso di IPv6 sono protetti anche gli eventuali header di estensione inseriti dopo AH e/o ESP, mentre quelli inseriti prima non sono protetti.
- **Tunnel**: il pacchetto IP originale viene inserito come payload di un pacchetto IP "esterno",[3] dotato di una nuova intestazione IP seguita da AH e/o ESP. In questo caso viene protetto tutto il pacchetto originale, compreso l'header. Perché il pacchetto possa girare nella rete, nel nuovo header IP devono essere indicati degli opportuni indirizzi IP di sorgente e destinazione; questi potrebbero essere quelli del pacchetto originale oppure potrebbero essere diversi (come si vedrà a breve).

In sostanza, il servizio di sicurezza fornito da AH o da ESP si applica dal punto del pacchetto in cui tale header è inserito in poi.

4.1 Scenari tipici

Lo scenario più comune in cui si usa la modalità trasporto è la comunicazione end-to-end tra due host, ad esempio per garantire autenticazione e/o riservatezza tra un client e un server. In questo caso, entrambi gli host devono implementare IPSec.

L'applicazione più comune della modalità tunnel è invece il collegamento sicuro di reti locali diverse (ad esempio sedi di un'azienda) attraverso la rete pubblica (che normalmente è insicura). A tale scopo, al confine di ciascuna delle due reti locali (LAN) da collegare si mette un **security gateway** da cui tutti i pacchetti degli host nella LAN devono passare per arrivare nella rete pubblica. I pacchetti che gli host di una rete mandano agli

[1] Nella progettazione di IPv6 si è semplificato l'header "di base", tenendo al suo interno solo le informazioni che servono sempre e modellando le altre informazioni (frammentazione, servizi di sicurezza, ecc.) mediante appunto degli header di estensione inseriti tra l'header e il payload.

[2] In realtà, AH in modalità trasporto fornisce protezione anche a una parte dell'header IP.

[3] In generale, fare "tunneling" vuol dire inserire un pacchetto di un protocollo come payload di un altro pacchetto, che tipicamente è di un protocollo diverso. Nel caso della modalità tunnel di IPSec, invece, il pacchetto IP viene inserito in un altro pacchetto dello stesso protocollo IP.

host dell'altra vengono inviati da un security gateway all'altro tramite una connessione protetta applicando IPSec in modalità tunnel; gli indirizzi IP di sorgente e destinazione indicati negli header IP dei pacchetti esterni sono quelli dei due gateway. Così, grazie in particolare al servizio di segretezza fornito dall'header ESP, nessun router della rete pubblica è in grado di esaminare il pacchetto interno: un attaccante potrebbe vedere solo che c'è traffico tra i due gateway, ma non potrebbe ottenere alcuna informazione sugli quali host delle due reti locali stiano comunicando, sui tipi di protocolli impiegati, sui contenuti dei payload, ecc. Quando un pacchetto arriva al gateway di destinazione, questo estrae il payload, cioè il pacchetto originale, decifrandolo e/o verificando l'autenticazione, poi lo indirizza al destinatario originale nella LAN. In questo caso IPSec non deve essere implementato dai singoli host, ma solo dai security gateway, che realizzano un canale protetto utilizzabile in modo trasparente da tutti gli host nelle LAN.

Quest'ultimo scenario prende il nome di **Virtual Private Network** (**VPN**), poiché si realizza virtualmente un'unica rete privata (ovvero sulla quale si ha il totale controllo: solo gli host che appartengono alla rete possono inviare e leggere messaggi al suo interno) sfruttando la rete pubblica per creare connessioni sicure tra una o più coppie di reti private fisicamente distinte. Si noti però che IPSec non è l'unico modo di realizzare una VPN: ce ne sono anche altri, basati sull'implementazione della sicurezza a diversi livelli della pila protocollare.