1 Lezione del 28-11-25

1.0.1 Funzionamento dell'IP Sec

Riassumiamo il comportamento dell'IP Sec con protocollo **ESP** (*Encapsulation Security Protocol*), come introdotto nella scorsa lezione.

Abbiamo detto che una qualsiasi connessione criptata fra router avviene mantenendo un identificatore da entrambi i lati, detto **SPI** (*Security Parameter Index*). Questo indicizza un database locale ad entrambi i router che mantiene le informazioni relative alla connessione sicura.

Quello che fa il router trasmettitore quando vuole inviare un datagramma è quindi:

1. Prendere il datagramma originale e aggiungere una certa quantità di *padding*. Questo è necessario in quanto si utilizzano algoritmi di cifratura a blocchi, e la dimensione del datagramma da criptare deve quindi essere multiplo della dimensione del blocco;

2. Il datagramma così esteso viene quindi criptato secondo la chiave contenuta nella SA della connessione;

3. Al datagramma criptato sono aggiunti due campi: il *SPI*, per indicizzare i parametri della connessione sicura nel router di arrivo, e il **numero di sequenza**. Quest'ultimo è necessario per evitare attacchi di replay;

4. Perché il numero di sequenza sia utile, dobbiamo autenticare l'intero messaggio, sfruttando il classico algoritmo *MAC* e concatenando il codice di autenticazione ottenuto al datagramma criptato.

   Abbiamo quindi a questo punto che header e payload del datagramma originale sono *criptati*, mentre lo stesso datagramma criptato, SPI, numero di sequenza e codice MAC sono solo *autenticati*;

5. Quest'intera stringa autenticata viene quindi incapsulata in un nuovo datagramma IP (*tunneling*), con il suo header che sarà in chiaro. Questo non ci preoccupa in quanto il numero di sequenza ESP è autenticato, e quindi siamo al sicuro da attacchi replay.

Il router ricevitore potrà quindi ricevere il pacchetto, vedere ed autenticare SPI e numero di sequenza (che sono autenticati ma in chiaro), rilevare le corrispondenti informazioni nell'SA e provvedere a decifrare il datagramma.

1.0.2 Database IP Sec

Vediamo nel dettaglio i database di cui i router equipaggiati per l'ESP hanno bisogno.

- **SPD** (*Security Policy Database*): per ogni datagramma, permette di determinare se IP Sec deve essere usato, e in tal caso quale SA usare. In sostanza, contiene informazioni riguardo a *cosa* fare coi datagrammi;

- **SAD** (*Security Association Database*): mantiene informazioni riguardo alle SA, cioè riguardo allo stato della connessione sicura. In questo, contiene informazioni riguardo a *come* elaborare i datagrammi.

1.1 Firewall

Introduciamo il concetto di **firewall**. Questo è un particolare software che si occupa di isolare la rete locale di un'organizzazione dal resto di internet, permettendo l'accesso selettivo solo ad alcuni pacchetti, e bloccando gli altri.

La motivazione del firewall è quella di:

- Prevenire attacchi di tipo **DoS** (*Denial of Service*), dove si mira a sovraccaricare i server con richieste SYN fasulle che non lasciano spazio a connessioni TCP effettive;
- Prevenire **modifiche/accessi illegali** ai dati sulla rete interne: ad esempio un attaccante potrebbe mirare a sostituire pagine web, o arrivare a fare attacchi *ransomware*, ecc...
- Permettere solo **accessi autorizzati** alla rete interna, cioè prmettere solo ad alcuni utenti/host autentcati di accedere alla rete locale dall'esterno.

Esistono 3 tipi fondamentali di firewall:

- Filtri pacchetti **stateless**;
- Filtri pacchetti **stateful**;
- **Gateway** applicazione.

1.1.1 Filtraggio stateless

Il filtraggio **stateless** dei pacchetti consiste nel controllare gli accessi su base *pacchetto per pacchetto*, controllando i campi all'interno del pacchetto come ad esempio:

- Indirizzi IP sorgente e destinazione;
- Numeri di porta TCP/UDP sorgente e destinazione;
- Tipo di messaggio ICMP;
- Bit SYN e ACK TCP (abbiamo detto per gli attacchi DoS questo è particolarmente importante).

Per implementare questo approccio si sfruttano le cosiddette **ACL** (*Access Control Lists*), cioè tabelle di regole applicate *dal basso verso l'alto* ai pacchetti in entrata.

Abbiamo che il funzionamento di queste tabelle ricorda molto l'OpenFlow, già discusso in 19.3.1 (si hanno coppie match/action dove l'unica action è scartare i pacchetti).

L'ultima regola dell'ACL determina il tipo di firewall. In particolare si ha:

- Se l'ultima regola blocca tutte le connessioni, il firewall si dice **inclusivo**, cioè si devono *includere* tutte le connessioni che vogliamo mantenere, mentre le altre vengono bloccate di default.

  Questo approccio è scomodo in quanto bisogna definire tutte le connessioni che si vogliono mantenere;

- Se l'ultima regola permette tutte le connessioni, il firewall si dice **esclusivo**, cioè si devono *escludere* tutte le connessioni che non vogliamo mantenere, mentre le altre vengono permesse di default.

  Questo approccio è più comodo di quello inclusivo (si definiscono meno regole), ma più pericoloso in quanto si ptorebbero tralasciare connessioni che invece vogliamo bloccare.

1.1.2 Filtraggio stateful

Il filtraggio **stateful** dei pacchetti si pone come un'estensione del filtraggio stateless appena visto.

In questo è uno strumento più pesante, che tiene conto non solo dei campi di ogni pacchetto, ma anche delle connessioni TCP correntemente attive. Deve quindi mantenere stato, con un suo database di connessioni TCP attive.

Può quindi tenere conto dell'ordine dei pacchetti SYN/FIN nel corso di vita delle connessioni TCP, ed effettuare ad esempio chiusure di connessioni dopo un certo timeout.

La tabella **ACL** va quindi complicata con entrate relative allo stato di connessione (nel caso più semplice, un entrata che segnala se la connessione a cui la regola si riferisce deve essere aperta o meno).

1.1.3 Gateway applicazione

Gli **application gateway** (tradotto *gateway applicazione*) permettono il filtraggio sulla base non solo dei campi IP (livello network) o TCP/UDP (livello transport), ma anche dei campi di livello *application*.

Questo permette di imporre regole al livello applicazione, come ad esempio permettere la connessione solo ad alcuni utenti, e negarla ad altri.

Otteniamo questa soluzione imponendo agli utenti di accedere a determinate applicazioni solo attraverso gateway specifici, e poi configurando i router della rete per permettere l'accesso in rete solamente a qui gatewey (negando le altre connessioni). Spesso il gateway coesiste con il router, anche se funzionalmente sono entità separate.

Sia firewall che gateway hanno le loro limitazioni.

- Ad esempio, i gateway applicazione richiedono configurazione specifica delle applicazioni client (ad esempio inserimento manuale dell'indirizzo IP gateway);
- L'*IP spoofing* può sempre essere usato per ingannare il firewall e farlo credere che il pacchetto in entrata provenga da una fonte diversa da quella effettiva;

1.2 IDS

Gli **IDS** (*Intrusion Detection Systems*) rappresentano un evoluzione delle semplici tecniche di filtraggio pacchetti.

Risulta, come abbiamo visto, complicato rilevare attacchi informatici controllando solo i singoli pacchetti, o anche tenendo traccia dello stato delle connessioni. Un'IDS risolve questo problema realizzando la cosiddetta *deep packet inspection*, cioè l'ispezione profonda del contenuto dei pacchetti, in maniera simile ad un antivirus. Questo permette agli IDS di risultare resilienti ad attacchi di natura più sofisticata, come ad esempio:

- Attacchi di **port scanning**, dove si mira a mappare le porte aperte di un host;
- Attacchi di **network mapping**, dove si mira a mappare l'intera rete per gli host attivi (magari seguendo con un attacco di port scanning su ogni host per rilevare le porte aperte);
- Attacchi di **DoS**, in maniera più efficiente che con un semplice firewall.

La dislocazione degli IDS è solitamente fatta in più siti, cioè si mira a distribuire il carico dell'analisi del traffico di rete su più *sensori* IDS posti in diversi punti della rete. La densità di sensori IDS dovrà essere maggiore nelle regioni dove si concentrano gli host utenti.

Quando si dislocano servizi di IDS è utile distinguere fra:

- La *rete interna*, dove abbiamo detto conviene massimizzare la presenza di sensori IDS;
- La *zona demilitarizzata*, dove risiedono server DNS, web server, server di posta, ecc... dell'organizzazione. Per questi vogliamo massimizzare l'efficienza nell'accesso a Internet, e quindi preferiamo minimizzare i controlli.

Abbiamo quindi visto le basi della sicurezza in rete, partendo dalle basi della crittografia, passando ai sistemi di autenticazione e di controllo integrità dei messaggi. Abbiamo poi visto come queste soluzioni vengono effettivamente applicate a livello application (ad esempio PGP), e quindi a livello network (con IP Sec). Infine, abbiamo vsito soluzioni di sicurezza operative come i firewall e gli IDS.

1.3 Reti wireless

Abbiamo finora parlato di soluzioni *wired*, cioè dove gli host erano cablati e stazionari. Al tempo attuale, però, la grande maggioranza di collegamenti ad Internet avvengono attraverso link di tipo *wireless*, cioè senza fili, dove gli host possono muoversi liberamente e restare connessi alla rete.

Le due problematiche che andiamo ad incontrare sono quindi:

- **Wireless**, cioè l'assenza di mezzi fisici e l'uso di mezzi basati sull'etere;
- **Mobilità**, cioè la capacità degli host di spostarsi nello spazio, anche su lunghe distanze, mantenendo attive le loro connessioni.

1.3.1 Elementi di una rete wireless

Una rete wireless si aggancia ad una preesistente infrastruttura cablata, da cui si fornisce un certo *access point* wireless (sia questo un antenna telefonica o un access point WiFi, ecc...). Gli accesso point vengono detti anche **base station** (*stazioni base*), e fungono da *relay* (o *bridge*) fra le reti cablate e le reti wireless, cioè fra tecnologie e quindi mezzi di accesso diversi fra di loro.

I dispositivi sulla rete wireless sono gli *host wireless*. Notiamo che il fatto che questi si trovino su una rete wireless non significa necessariamente che sono mobili (cioè che si spostano nello spazio). Ad esempio, un portatile in una rete d'istituto è solitamente stazionario, mentre un telefono cellulare può spostarsi nello spazio velocemente e su lunghe distanze, sempre restando collegato alla rete.

1.3.2 Classificazione dei link wireless

Possiamo classificare i link wireless su diverse caratteristiche ortogonali:

- L'**area di copertura**, cioè la dimensione della regione spaziale che il link è capace di coprire e servire. In questo aspetto possiamo distinguere fra più tipi di rete wireless:
  - Reti *short-range*, cioè a corto raggio, per interni (dai 10 m ai 30 m) ed esterni (dai 50 m ai 200 m). Ad esempio, queste sono reti per le abitazioni o per istituzioni, quindi interi edifici, ecc...

    Fanno parte di questa categoria tecnologie come il Bluetooth (standard IEEE 802.15, dal bitrate particolarmente basso e basso consumo energetico) e il WiFi (standard IEEE 802.11);
  - Reti *medium-range*, sempre per esterni, che vanno dai 200 m ai 400 Km.

    Fanno parte di questa categorie tecnologie come quelle appartenenti all'odierna 5G. Esistono anche tecnologie WiFi di tipo medium-range (802.11 af, ah), pensate per applicazioni IoT a basso bitrate ma che richidono grande scalabilità.
  - Reti *long-range*, anche queste sempre per esterni, che vanno dai 4 Km ai 15 Km circa.

    Fanno parte di questa categorie tecnologie come quelle appartenenti al 4G LTE.
- Il **bitrate**, cioè la frequenza di bit che il link è capace di trasmettere (avevamo già ampiamente discusso questo aspetto parlando delle reti wired).

1.3.3 Handoff

Notiamo che le reti mobili devono permettere funzionalità di **handoff**, cioè di transizione degli host da una base station all'altra, in maniera dinamica e coordinata fra host e base station.

1.3.4 Reti ad hoc

Inoltre, notiamo che le reti wireless possono operare in maniera **ad hoc**, dove non esistono stazioni base, e gli host possono parlare fra di loro solamente in maniera P2P. In questo modo i nodi della rete si organizzano autonomamente in una rete, d instradano pacchetti attraverso loro stessi.