Comunicazioni sicure a livello di rete: IPSec e VPN

Indice

- Richiami di rete dei calcolatori
- IPsec
- VPN

Reti di Calcolatori

- Dal punto di vista **fisico**: le reti sono una collezione di segmenti the trasmettono flussi di bit.
  Esempio**:** cavo tra due nodi o canali multiaccesso in una LAN
- Dal punto di vista **logico**: Un mezzo di comunicazione tra *principal* (vedere la parte su protocolli di sicurezza).
  Esempio: un client comunica con un server.

Comunicazione a strati

- Le funzionalità logiche sono costruite a strati:
  - Le comunicazioni a livello applicativo sono costruite su
    - sistemi di trasporto affidabile tra i nodi che sono costruiti su
    - sistemi di trasporti inaffidabili tra link e switch che si basano su
    - canali di trasporto su singoli link.

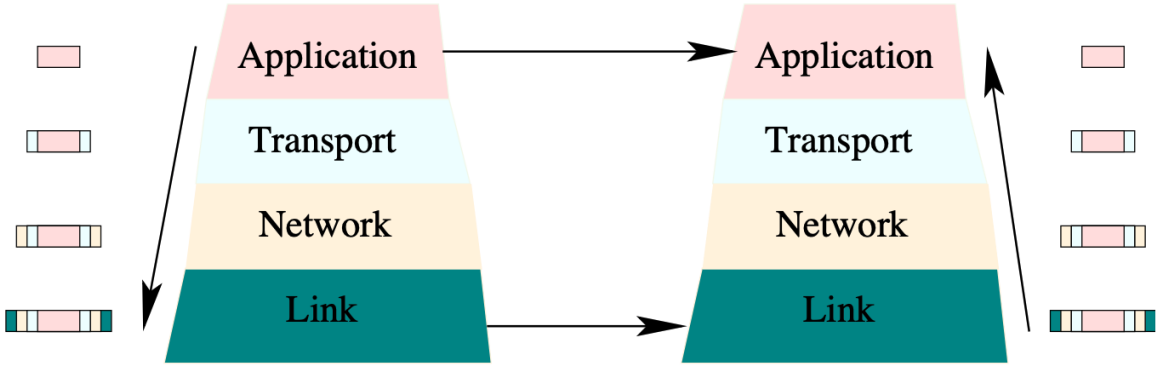
Comunicazione a strati /2

- Il modello di riferimento è il TCP/IP:

Application	Telnet, FTP, HTTP, RPC, SMTP, SET, ...
Transport/session	TCP, UDP
Network (Internet)	IP, ICMP, ...
Link (Interface)	Network interface & device drivers (IEEE 802.x, PPP, SLIP)

Comunicazione a strati /3

- L'i-esimo strato di un nodo comunica con l'i-esimo strato dell'altro nodo, sfruttando i servizi offerti dagli strati inferiori.
- Ogni nodo aggiunge/toglie header del protocollo specifico di uno strato, man mano che il pacchetto attraversa gli strati.
- Gli strati sono una astrazione.



Sicurezza Internet

- Internet: Confederazione di reti che usano lo standard TCP/IP.
- Non c'è un dominio di fiducia (domain of trust) globale.
  - Sottoreti diverse possono essere più o meno fidate/sicure
  - In media un pacchetto attraversa fino a 15 sottoreti per raggiungere la destinazione.

Sicurezza Internet

- Problema: Come rendere sicure le comunicazioni e le applicazioni?
- Una possibilità: rendere sicure lo stato delle applicazioni che usano canali insicuri utilizzando ad esempio:
  - Kerberos un protocollo per cifrare dati trasmessi e garantire autenticità tramite crittografia.
  - PGP per cifrare e garantire autenticità di messaggi inviati via mail.
- È tuttavia possibile anche rendere sicuri gli altri strati.

Quali strati?

- Internet Protocol (IP): invia i dati all'interno di una rete. Gli header del pacchetto IP specificano la sorgente e la destinazione. I protocolli calcolano il cammino e instradano pacchetti attraverso collegamenti multipli dalla sorgente verso la destinazione
- Transmission Control Protocol (TCP): costruisce comunicazioni *affidabili* tra due sistemi su una rete. Per affidabile si intende che tutti i pacchetti siano inviati senza perdita, duplicazione o ricostruiti in modo sbagliato.

Nessuno dei due protocolli garantisce sicurezza, né autenticazione o confidenzialità. Gli indirizzi possono essere finti e il payload (ovvero i dati) possono essere letti o modificati.

Quali strati? /2

- Per molte implementazioni dello stack IP
  - Fino al livello di trasporto, i protocolli sono implementati nel sistema operativo
  - Sopra il livello di trasporto i protocolli sono implementati nello spazio utente.
- Due esempi rappresentativi:
  - **SSL (o TLS/SSH):** il sistema operativo non cambia, cambiano le applicazioni. Le API di SSL sono un soprainsieme di quelle di TCP.
  - **IPsec:** Cambia il sistema operativo, mentre le applicazioni e le API del TCP non cambiano.

TLS

- TLS: Transport Layer Security (TLS) e il suo predecessore Secure Sockets Layer (SSL) sono protocolli crittografici di presentazione che permettono una comunicazione sicura dalla sorgente al destinatario (end-to-end) su reti TCP/IP fornendo autenticazione, integrità dei dati e confidenzialità operando al di sopra del livello di trasporto.
- Diverse versioni sono utilizzate in applicazioni come i browser (HTTPS), l'e-mail, la messaggistica istantanea e il voice over IP.

IPsec

- IPsec, IP Security, è uno standard per reti a pacchetto che si prefigge di ottenere connessioni sicure su reti IP.
- La sicurezza viene raggiunta aggiungendo autenticazione, cifratura e controllo di integrità dei pacchetti IP (datagrammi).
- La protezione viene fornita a livello di rete e il protocollo è trasparente per le applicazioni che quindi non devono essere modificate.

Quali strati? /4

- **Applicativo (o end-to-end):**
  - :-) Non occorre assumere alcuna sicurezza negli strati inferiori.
  - :-) Le decisioni riguardo la sicurezza sono prese direttamente a livello di utenti e dei dati applicativi che si scambiano.
  - :-(Le applicazioni devono essere «sicure».
- **Tra il livello applicativo e di trasporto:** e.g., SSL
  - :-) Non ci sono modifiche sul sistema operativo e sono minime quelle sulle applicazioni
  - :-(Problemi con l'interazione con il livello TCP. L'SSL potrebbe non accettare pacchetti che il TCP accetta, pertanto l'SSL dovrebbe chiudere la connessione TCP → sono possibili facili attacchi di Denial of Service .
- **IPsec:**
  - :-) Garantisce sicurezza a livello di trasporto senza richiedere modifiche delle applicazioni.
  - :-(Autentica solo i pacchetti IP, non gli utenti.
  - :-| E' possibile in linea di principio fare di più ma richiede di modificare le API

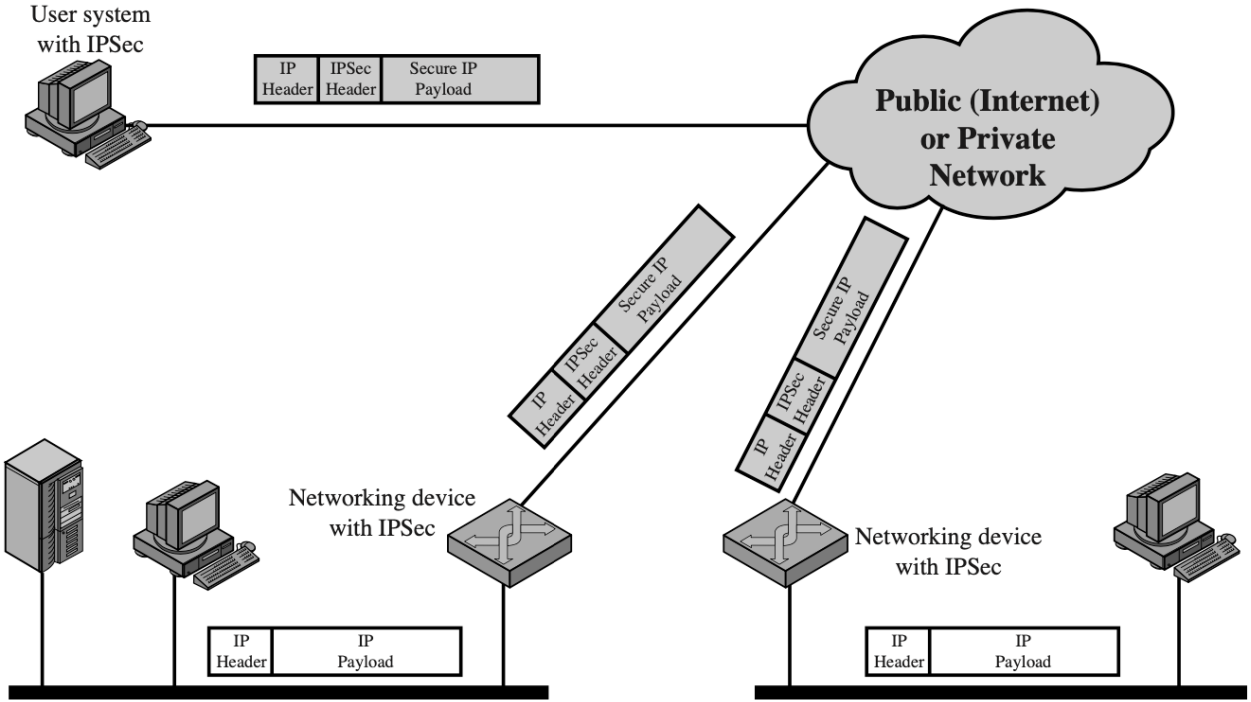
Sicurezza IP: IPsec

- Garantisce un canale sicuro per tutte le applicazioni, cifratura e autenticazione del traffico.
- Garantisce la possibilità di filtrare i pacchetti in accordo con un database di politiche di sicurezza, esattamente come se ci fosse un firewall tra le parti.
- È installato in
  - **Sistemi Operativi:** per garantire sicurezza end-to-end;
  - **Security gateway:** Come firewall o router, è usata per implementare Virtual Private Network (VPN).

Applicazioni di IPSec

- Rendere sicura la connessione dell'ufficio su Internet
- Garantire accessi remoti sicuri su Internet
- Stabilire connessione intranet o extranet con i partner
- Migliorare la sicurezza dell'e-commerce

Uno scenario per IPsec

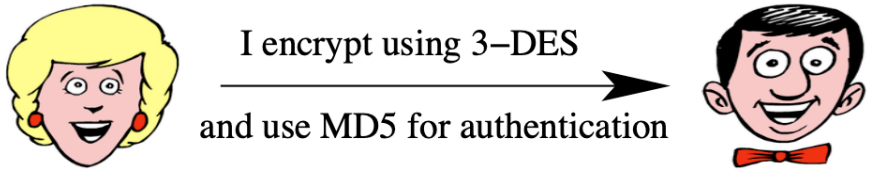


Lo standard IPsec

- IPsec è uno standard IETF, come TLS. La specifica contiene diversi protocolli che svolgono diverse attività e hanno finalità diverse in termini di sicurezza:
  - **Authentication Header (AH):** protegge *l'integrità* e *l'autenticità* dei pacchetti IP (ma non la loro *confidenzialità*).
  - **Encapsulating Security Payload (ESP):** protegge la *confidenzialità* ed, opzionalmente, anche *l'integrità* dei pacchetti dei pacchetti IP.
  - **Key Management (IKE):** Internet Key Exchange Protocol, permette lo scambio di chiavi di cifratura.

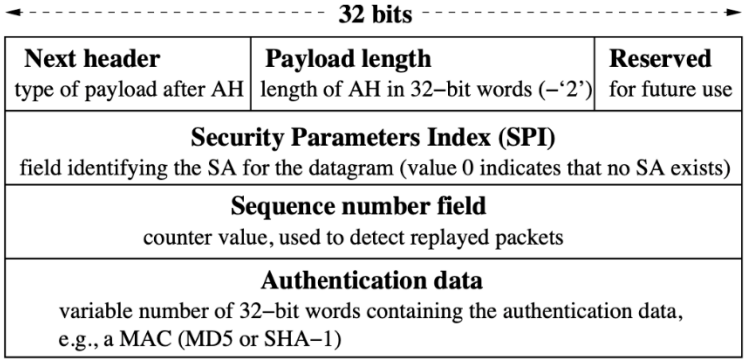
IPsec: Security Associations (SA)

- Una security association (SA) è una relazione one-way tra mittente e destinatario che definisce dei servizi di sicurezza.



- Specifica le modalità del protocollo (tunnel o trasporto), l'algoritmo di autenticazione (AH), l'algoritmo di cifratura (ESP), le chiavi e la durata della validità delle chiavi e della SA stessa, ...
- È identificata da campi negli header AH ed ESP.
- È definita usando il protocollo IKE, o altri.
- Viene normalmente mantenuta in un database.

IPsec: Authentication Header (AH)

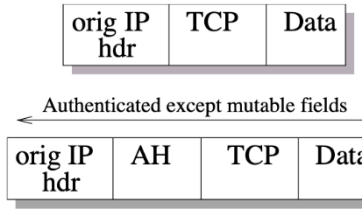


L'AH è uno header extra tra gli strati IP e TCP che fornisce informazioni per identificare univocamente una SA; garantisce integrità ma protegge soltanto l'header IP.

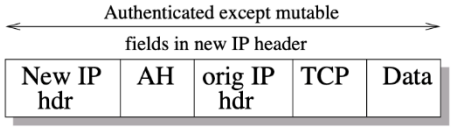
Il Sequence number è inizializzato a zero ed incrementato dal mittente ad ogni pacchetto. Il ricevente salva i pacchetti in ingresso in una finestra scorrevole (sliding window), di dimensione 64 per default, per ordinare i pacchetti e scartare i duplicati, in quanto IP non garantisce ordine nei pacchetti.

IPsec: Authentication Header (AH) /2

Due modalità:

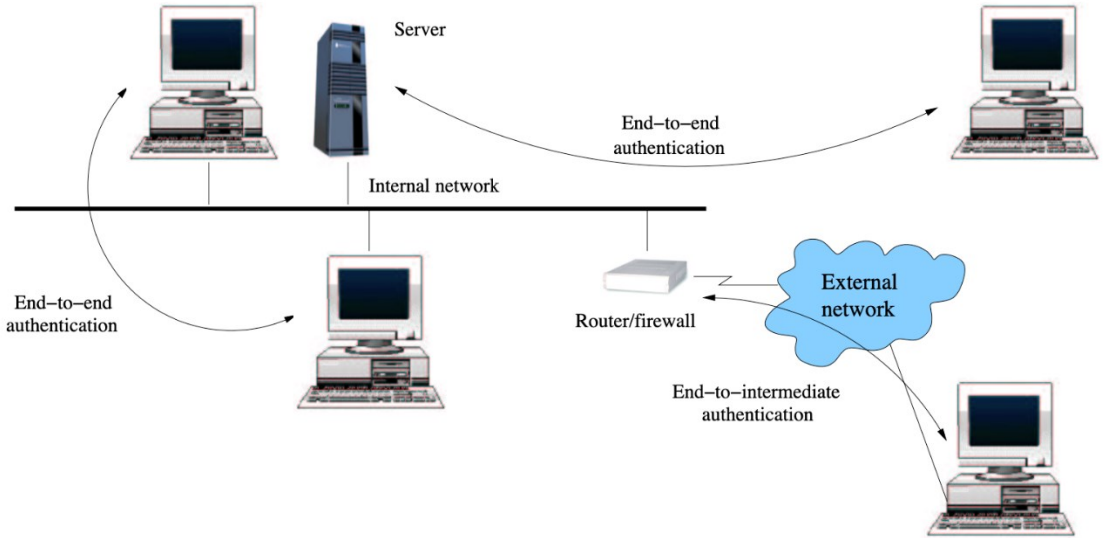


- Modalità trasporto:
  - AH inserito dopo l'header IP, prima del payload IP
  - MAC calcolato sull'intero pacchetto, ad esclusione dei campi che possono subire modifiche
  - Garantisce protezione end-to-end tra sistemi con IPsec.



- Modalità Tunnel:
  - Tutto il pacchetto originale è autenticato, viene creato un nuovo header IP.
  - L'header interno conserva le informazioni sul mittente e destinatario.
  - Anche il nuovo header esterno è protetto (a parte campi mutevoli) e può contenere indirizzi IP diversi (ad esempio dei firewall).

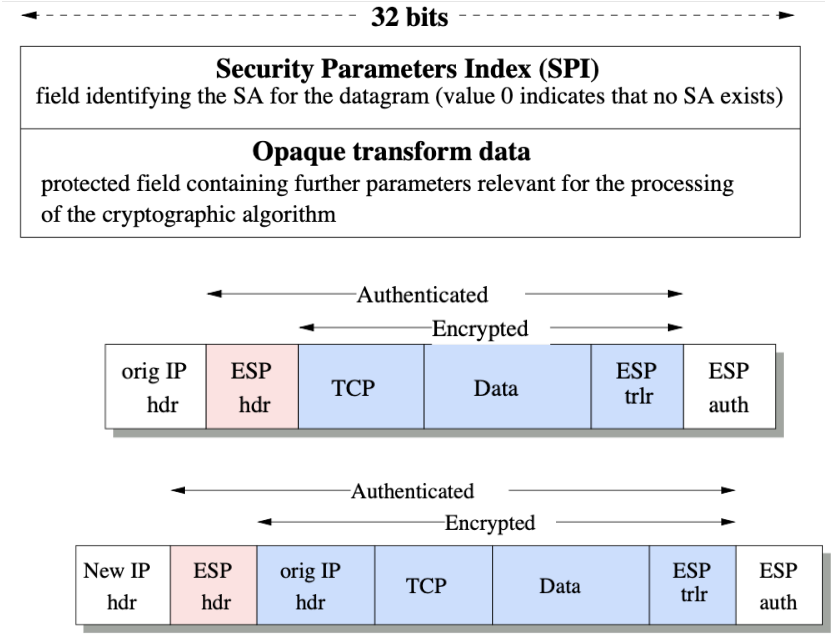
IPsec: una applicazione dell'AH



- L' AH è usato per garantire canali autenticati sia end-to-end (tipico della modalità trasporto) che nella modalità tunnel verso un gateway sicuro.

IPsec: Encapsulating Security Payload (ESP)

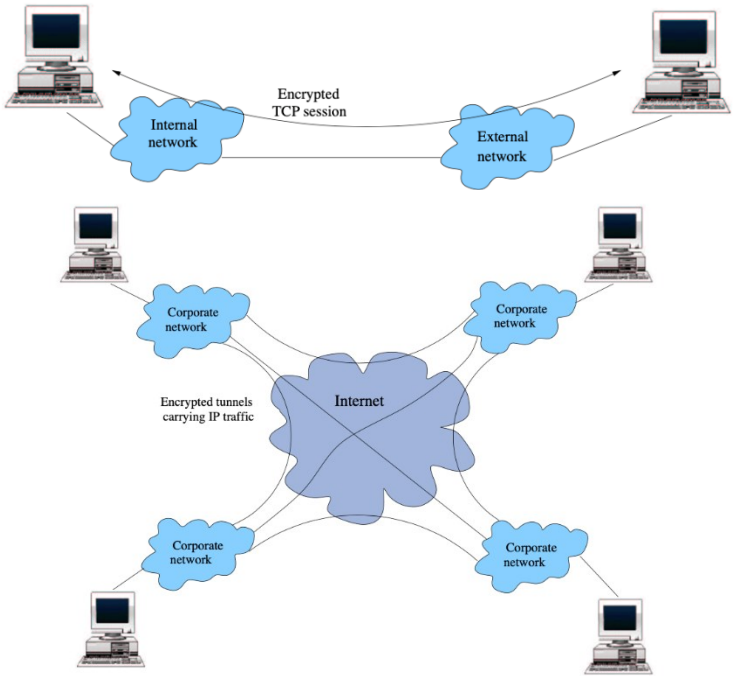
- L'header specifica la cifratura e l'autenticazione.
- Modalità Trasporto:
  - Cifra solo il payload di ogni pacchetto ma lascia l'header nella forma originale.
- Modalità Tunnel:
  - Cifra l'intero pacchetto IP, cifrando sia l'header che il payload.



IPsec: Applicazioni dell'ESP

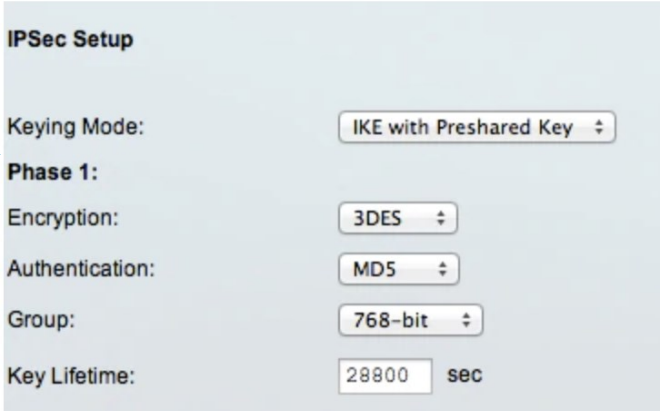
- **La modalità trasporto** fornisce una cifratura end-to-end tra host che supportano IPsec.

- **La modalità tunnel** può essere usata per implementare una Virtual Private Network (VPN). In una VPN, host che appartengono a reti differenti usano Internet attraverso tunnel IPsec tra security gateway. Gli host non devono implementare alcuna soluzione di sicurezza.



IPsec: IKE

- IKE permette di scambiare chiavi e di definire Security Association in termini di protocolli usati per cifrare e per hashing.
- IKE è molto flessibile, in quanto supporta diversi schemi di cifratura ed autenticazione basati su pre-shared keys.
- Tuttavia, è molto complessa da configurare perché ha molte opzioni e supporta molti sub-protocolli.



Esempio di setup di IKE

IPsec: IKE /2

- IKE è evoluta in un numero di differenti protocolli che includono:
  - ISAKMP (Internet Security Association and Key Management Protocol): che fornisce un framework ed un protocollo generico di negoziazione per stabilire SA e chiavi crittografiche, ma non fornisce alcun meccanismo di autenticazione.
  - OAKLEY: una suite di protocolli per lo scambio delle chiavi in cui 2 parti generano una chiave assieme.
- In pratica, IKE combina formati di pacchetti di ISAKMP e li scambia con OAKLEY, che si basa sul Diffie-Hellman.

Esempio di una VPN con IPsec