UNIVERSITÀ DI PARMA

DIPARTIMENTO DI SCIENZE MATEMATICHE, FISICHE ED INFORMATICHE
Corso di Laurea in Informatica

Sicurezza delle reti – Parte C

Protocolli

RETI DI CALCOLATORI - a.a. 2022/2023

Roberto Alfieri

La sicurezza delle reti: sommario

PARTE A

- I servizi di sicurezza
- Metodi e strumenti di attacco
- Strumenti di Difesa

PARTE B

- Crittografia applicata e OpenSSL

PARTE C

- Protocolli di Autenticazione
- IPsec
- VPN
- Sicurezza delle reti WiFi

Protocolli di Autenticazione

Riferimenti: *http://it.wikiversity.org/wiki/Protocolli_di_autenticazione*

Autenticazione (Authentication): un servizio di sicurezza che consente di accertare l'identità dichiarata da una entità mediate la verifica di credenziali.

L'autenticazione può avvenire:

- tra una persona fisica e un host o dispositivo (es. bancomat)
- in una comunicazione di rete (l'origine dei dati o i peer di una comunicazione) mediante un opportuno protocollo

L'autenticazione può essere mutua oppure no, dipende dalle situazioni.

Ad esempio è mutua quando consulto la posta elettronica:

- Il server si deve autenticare con me per dimostrarmi di essere il server che gestisce la mia posta.
- Io devo dimostrare al server che sono il titolare della mailbox.

Le tecniche possono basarsi su

- La conoscenza di un segreto (password, PIN, ..)
- tecniche crittografiche
- Caratteristiche biometriche (se l'autenticazione avviene tra una persona ed un host locale): timbro voce, impronta digitale, fondo dell'occhio, ecc

Autenticazione tramite password

La password è un segreto condiviso che l'utente deve presentare per accedere alla risorsa.

E' un metodo largamente utilizzato perché facile da implementare e da usare.

E' insicuro specialmente quando:

- la password non viene modificata regolarmente
- Le password sono individuabili con **attacco al dizionario**

(la generazione e la verifica di un elevato numero di possibili password, prodotte con l'ausilio di un dizionario di parole comuni).

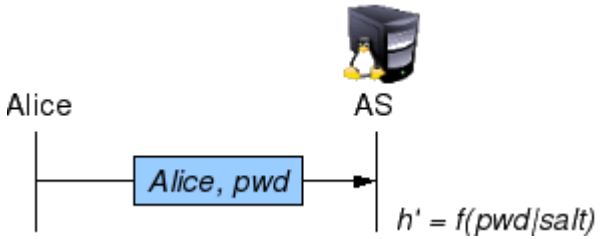
- La password viene utilizzata in diversi protocolli di autenticazione in rete quali PAP e CHAP

Autenticazione tramite password: PAP

PAP (Password Authentication Protocol)

- presume che il canale sia sicuro (non intercettabile)
- A manda al server il proprio Nome e la Password
- Il server cerca in una tabella il nome utente e verifica la correttezza della password applicando una funzione di trasformazione

  (che consente di evitare che il server memorizzi la password in chiaro)
- Ancora in uso in PPP anche se deprecato.



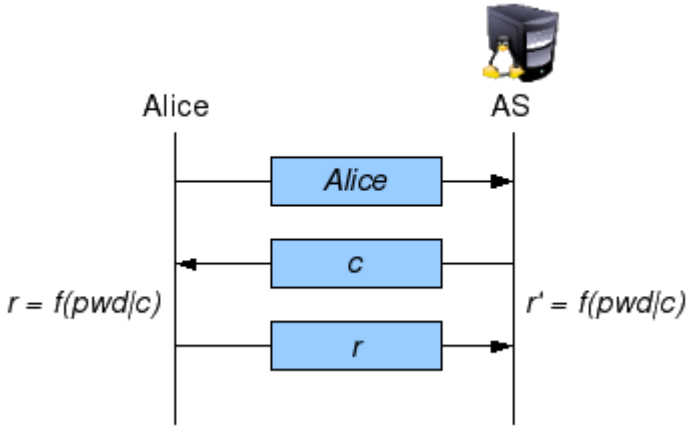
Autenticazione tramite password:CHAP

CHAP (Challenge Handshake Authentication Protocol)

- Usato in PPP
- Windows usa una variante di CHAP detta MS-CHAP
- Il server invia un numero casuale c (challenge) utilizzato dal client come salt
- La funzione di trasformazione r=f(pwd,c) è calcolata sia dal server che dal client
- L'implementazione standard di CHAP usa MD5: r=MD5(pwd, c)

Vantaggi: La password non viene scambiata tra client e server

Problemi: Il DB delle password deve essere salvato in chiaro. Attacco al dizionario



One-Time Password (OTP)

Una One-Time Password (password valida una sola volta) è una password che è valida solo per una singola sessione di accesso o una transazione e non è quindi vulnerabile agli attacchi al dizionario.

Le password sono legate tra loro secondo un determinato algoritmo e devono essere utilizzate in un ordine predefinito.

Gli algoritmi che sono stati realizzati per generare OTP sono abbastanza diversi tra loro. Il più diffuso è TOTP (Time based OTP, RFC 6238) Le password sono generate con un algoritmo funzione di una chiave segreta (k) e il tempo corrente (t). Per TOTP l'algoritmo è HMAC (HOTP) in cui Password = HMAC (t, k)

Metodi di distribuzione dell'OTP:

Una password OTP non può essere memorizzata da una persona. Essa richiede quindi una tecnologia supplementare per poter essere utilizzata.

Alcuni sistemi elettronici prevedono l'uso di speciali token che l'utente porta con sé, che generano le OTP e le mostrano utilizzando un piccolo display.

Altri sistemi sono costituiti da un software che gira sul telefono cellulare dell'utente (vedi Google Authenticator). In alcuni casi le OTP vengono generate dal server e trasmesse all'utente su un canale fuori banda, come ad esempio un canale di messaggistica SMS.

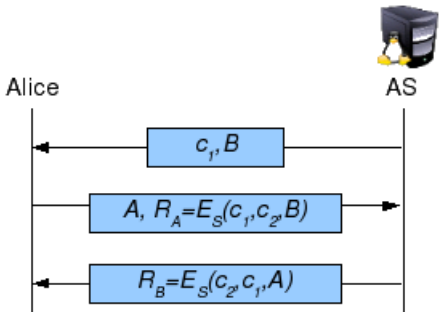
Autenticazione con challenge e chiave simmetrica

Le 2 parti A e B , che condividono una chiave simmetrica S, si inventano ciascuna un numero casuale, detto Challenge (c1 e c2)

Il server invia la propria identità (B) e il proprio Challenge (c1)

Il client risponde inviando la propria identità (A) e la cifratura di c1, c2 e B.

Il server chiude il protocollo inviando la cifratura di c1, c2 e A.



Vantaggi: I messaggi cifrati non sono esposti ad attacco al dizionario.

Problemi:

- Se abbiamo N nodi ogni nodo deve conoscere N-1 chiavi.
- La condivisione di una chiave simmetrica si espone ad intercettazione.

Autenticazione con KDC

Il modello del “Centro di Distribuzione delle Chiavi” (KDC, Key Distribution Center) si applica ad una comunità di N entità (persone/host/servizi) che devono autenticarsi reciprocamente.

In questo schema ogni utente ha una singola chiave condivisa con il KDC.

Esempio: A deve comunicare con B

A condivide con KDC la chiave Ka, B condivide con KDC la chiave Kb

A sceglie una chiave di sessione Ks, invia a KDC la chiave e B, in modo cifrato.

KDC decifra Ks e la invia a B

```
A  ->   A, Ka(B,Ks)   ->  KDC
                          KDC    ->    Kb(A, Ks)   -> B
```

Vantaggi: Singola chiave Ka per comunicare con N entità.

Problemi: A deve inserire la chiave Ka per ogni connessione.

Autenticazione Kerberos

Kerberos è un protocollo di Autenticazione (progettato al MIT) che implementa il modello del “Centro di Distribuzione delle Chiavi”.

E' ampiamente diffuso soprattutto negli USA sia su Linux che Windows

Un sistema Kerberos gestisce una comunità di utenti (REALM) in cui ogni utente ha una singola chiave condivisa Ka con il KDC, ma il KDC si compone di 2 server:

AS (Authentication Server) Gestisce il LOGIN

TGS (Ticket Granting Server) Gestisce la sessione

La password di A (Ka) viene usata una sola volta per tutte le autenticazioni della sessione (Single Sign On - SSO) e rimane sul computer del client solo per pochi millisecondi.

La chiave di sessione che A presenta a B serve solo a dimostrare l'identità di A (autenticazione). B deciderà cosa consentire di fare ad A (autorizzazione)

Autenticazione Kerberos

Innanzitutto A chiede all'AS la chiave di sessione Ks (Login sul REALM):

A -> A -> AS

A <- Ka(Ks), Ktgs(A,Ks) <- AS

Ktgs(A,Ks) contiene A e Ks cifrate con la chiave segreta del TGS

Quando A deve comunicare con B chiede al TGS un Ticket Kab da usare con B:

A -> Ktgs(A,Ks), B, Ks(t1) -> TGS

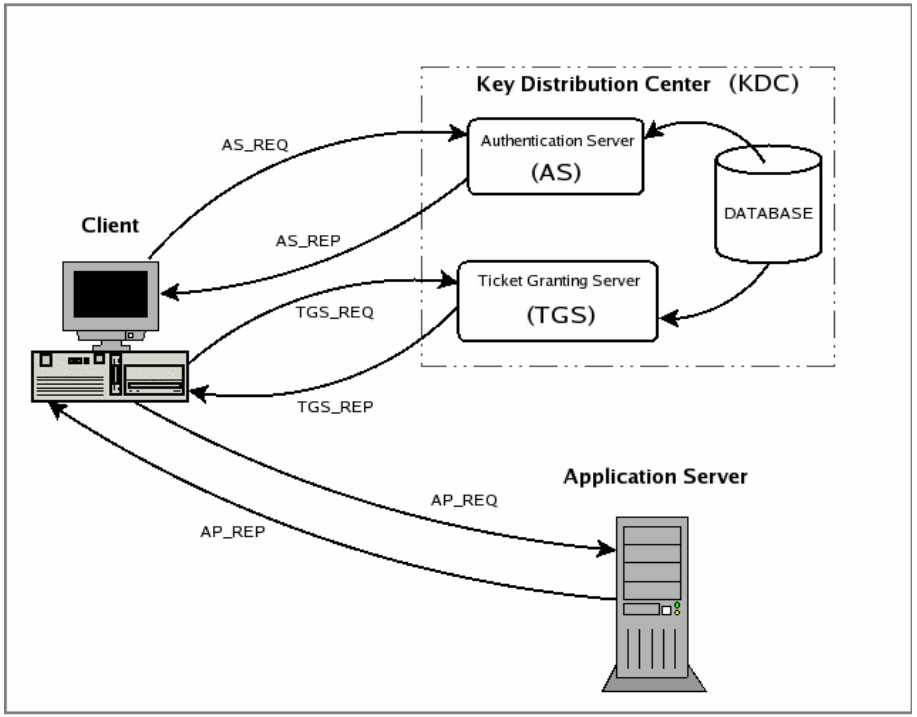
A <- Ks(B, Kab), Kb(A,Kab) <- TGS

Quindi A si rivolge a B comunicandogli la chiave di sessione Kab:

A -> Kb(A,Kab), Kab(t1) -> B

A <- Kab(t2) <- B

I timestamp t1 e t2 impediscono che qualcuno possa intercettare i messaggi e replicarli con un mittente falsificato (spoofed).



Scambio chiavi di Diffie-Hellman

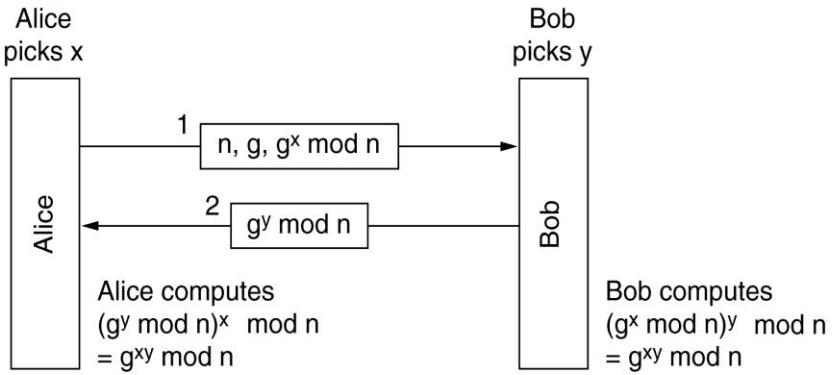
Consente a 2 entità che non hanno avuto contatti in precedenza di stabilire in modo sicuro una chiave simmetrica condivisa.

Servizi di sicurezza: **confidenzialità senza autenticazione.**

A e B devono condividere 2 numeri grandi n e g che possono scambiarsi in chiaro.
(n e (n-1)/2 sono primi, g=f(n) opportunamente calcolato)

1) A sceglie X grande che mantiene segreto
quindi invia A -> n, g, g^x mod n -> B

2) B sceglie Y grande che mantiene segreto
quindi invia A <- g^y mod n <- B



3) B calcola $(g^x \bmod n)^y \bmod n = g^{xy} \bmod n$
A calcola $(g^y \bmod n)^x \bmod n = g^{xy} \bmod n$

g^{xy} mod n
è la chiave condivisa di sessione

Autenticazione con PKI

L'utilizzo di una PKI (Public Key Infrastructure) ha il vantaggio di non richiedere preventivamente chiavi condivise.

I nodi A e B hanno una coppia di chiavi A-> (Ea,Da) B-> (Eb,Db).

Le chiavi Ea ed Eb sono pubbliche.

A invia la propria Identità e un Challenge Ra a B, cifrati con la chiave pubblica di B.

A -> Eb(A,Ra) -> B

B decifra il messaggio, sceglie una chiave di sessione Ks e la invia ad A:

A <- Ea (Ra, Rb, Ks) <- B

A risponde con il Challenge di B cifrato con la chiave di sessione Ks:

A -> Ks(Rb) -> B

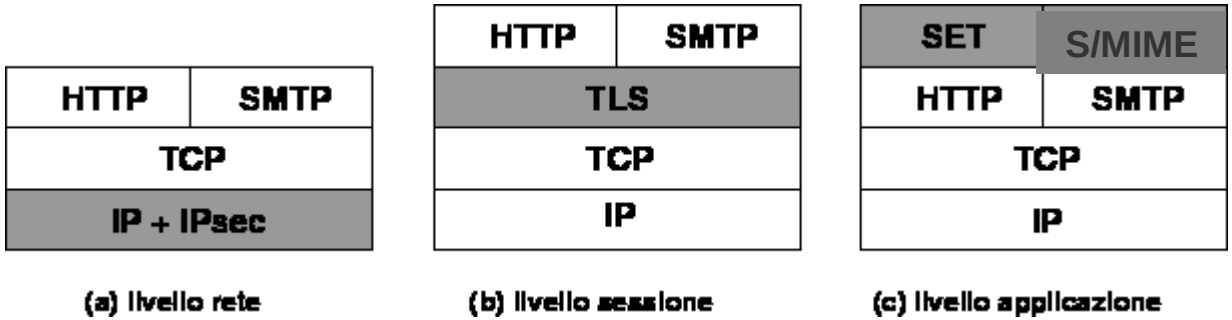
Servizi di sicurezza:

- **la chiave di sessione Ks è condivisa (confidenzialità)**
- **gli host hanno verificato l'identità reciproca (autenticazione).**

Protocolli per la riservatezza

La cifratura di una comunicazione può avvenire a diversi livelli:

- Alcune applicazioni cifrate si appoggiano sull'applicazione in chiaro. Il payload viene cifrato e quindi veicolato da applicativo non cifrato (vedi ad es. S/MIME su SMTP)
- Il protocollo **SSL/TLS** fornisce un Layer intermedio tra TCP e applicazione che consente di cifrare le applicazioni. Questo richiede la riscrittura delle applicazioni che devono interfacciarsi al layer SSL anziché TCP.



- IPsec è un Layer di cifratura che viene posizionato a livello rete, rendendo la cifratura trasparente al livello delle applicazioni, che non devono essere modificate

IPsec è integrato in IPv6 (Extension Header 50 e 51), mentre è opzionale in IP4.

Attualmente l'uso predominante di IPsec è la creazione di Reti Virtuali Private (VPN)

Protocolli IPsec

Una “connessione” IPsec chiamata SA (Security Association), è una connessione Simplex e ha un Identificatore di sicurezza associato.

Per una connessione Duplex è necessario attivare un SA per ciascuna direzione.

Ogni pacchetto Ipsec include nell’intestazione un indice (Security Parameter Index – SPI) che consente al ricevente individuare la SA e quindi di reperire la chiave di decifratura.

IPsec, analogamente a SSL, è formato da

- Un protocollo per lo scambio delle chiavi necessarie per la cifratura del canale:
  - **IKE** (Internet Key Exchange)
- Due protocolli alternativi per la cifratura dei dati sul canale:
  - **AH** (Authentication Header). Gestisce integrità, ma non confidenzialità.
  - **ESP** (Encapsultating Security Payload). Anche confidenzialità (cifratura payload)

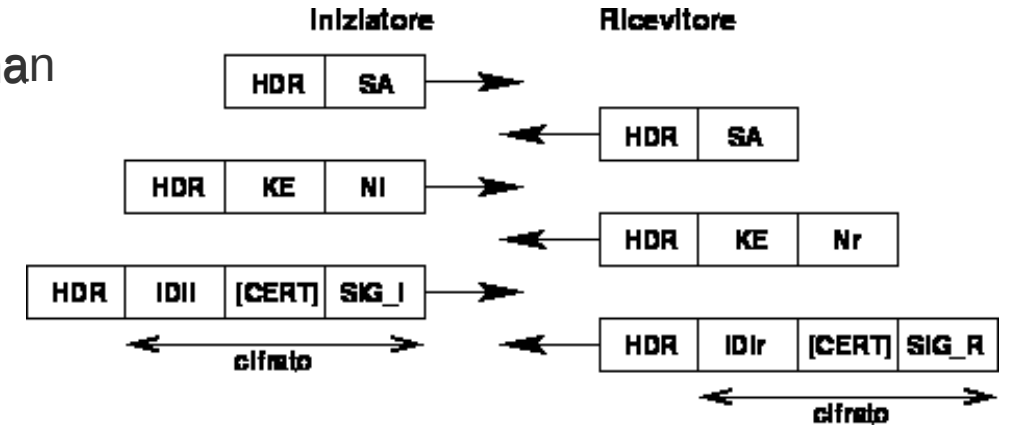
IKE (Internet Key Exchange)

IKE è utilizzato per stabilire una SA.

E' a livello applicazione e usa UDP come trasporto sulla porta 500.

L'obiettivo è stabilire una Shared Session Secret da cui poi derivare la chiave per cifrare la SA.

Viene utilizzato l'algoritmo di Diffie-Hellman



Ogni host IPsec gestisce un Security Association Database che include l'elenco delle SA attive.

Ogni elemento del DB indicizzato dal Security Parameter Index (SPI) include:

- l'indirizzo di destinazione
- servizi di sicurezza (AH, ESP)
- Algoritmi simmetrici usati per cifrare i dati (3DES, AES, ..) e le chiavi associate
- altri parametri quali l'IPsec lifetime

Transport mode e Tunnel mode

Sia AH che ESP possono funzionare il modalità Transport o Tunnel.

Transport mode

- connessione host-to-host
- usato dagli end-point non dai gateway
- viene cifrato solo il payload dei datagrammi IP, non l'header
- computazionalmente leggero
- ogni host deve avere tutto il software necessario ad implementare IPsec
- si aggiunge solo l'header IPsec; mittente e destinazione si vedono

Tunnel mode

- connessione Gateway-to-Gateway
- viene cifrato tutto il pacchetto IP originale
- utilizzato per realizzare le VPN
- computazionalmente oneroso
- solo i Gateway devono avere il software IPsec
- si hanno punti di centralizzazione quindi single point of failure
- si ha un doppio incapsulamento, aggiungendo l'header del gateway e l'header IPsec

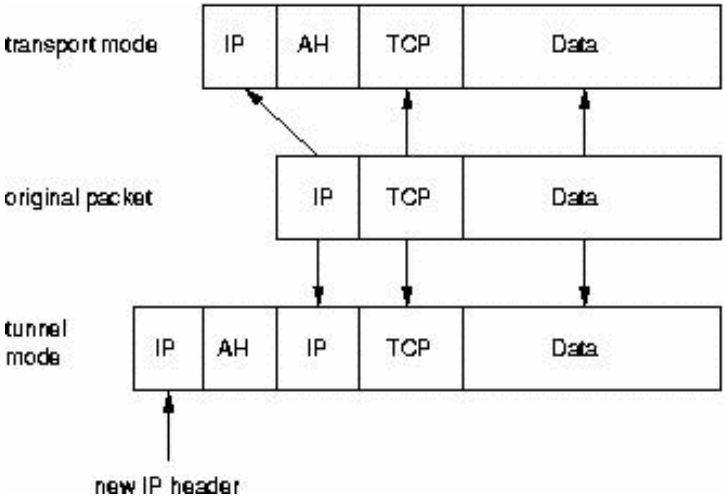
AH (Authentication Header)

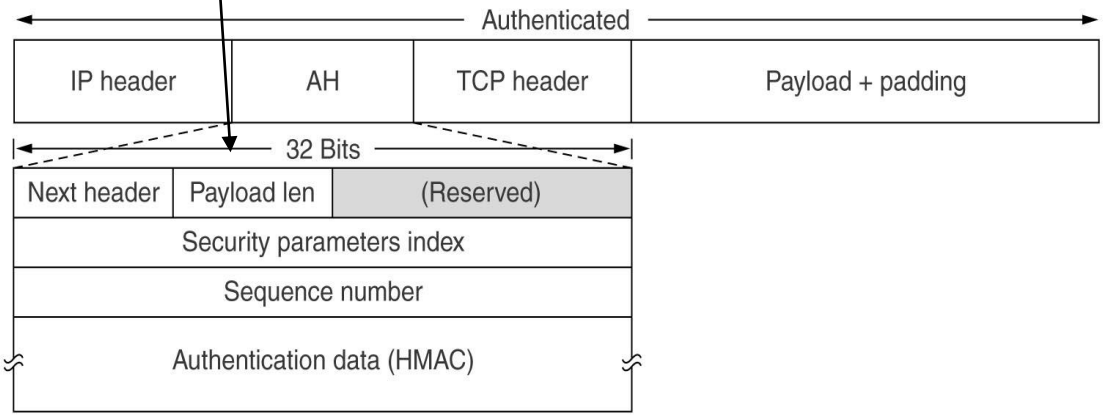
AH gestisce integrità del pacchetto, ma non la confidenzialità: non ha la cifratura.

Il protocollo determina una intestazione di 24 Byte che contiene l'HMAC del Datagramma IP (Header+payload)

L'intestazione che può essere inserita

- nelle estensioni dei protocolli IPv4 e IPv6 (**Transport Mode)**
- nell'estensione di un nuova intestazione IP che come payload incapsula il pacchetto IP originale **(Tunnel Mode)**





ESP (Encapsulating Security Payload)

ESP, rispetto a HA, aggiunge la confidenzialità poiché il payload viene cifrato.

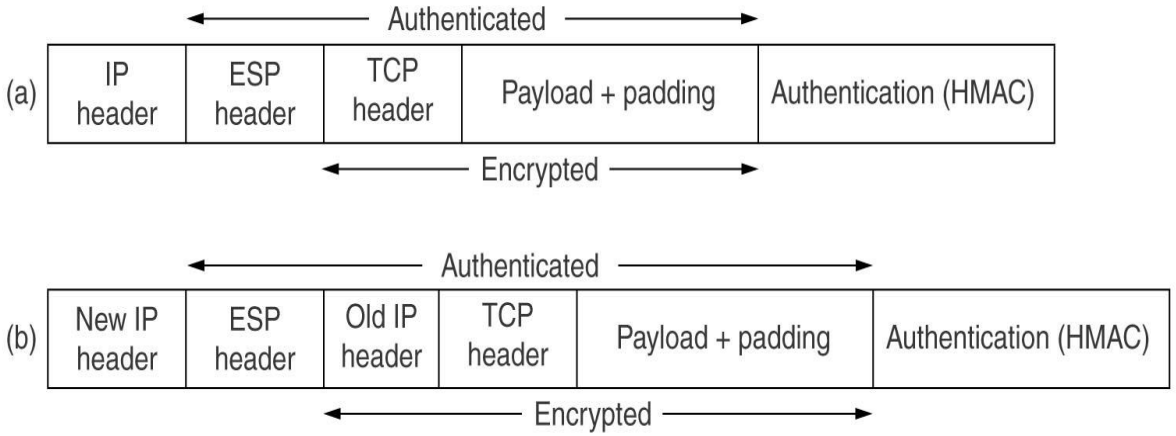
Il campo **HMAC (**diversamente da AH)

- non copre l'Header IP
- è accodato al payload cifrato. Viene calcolato mentre il pacchetto sta uscendo

Cifratura:

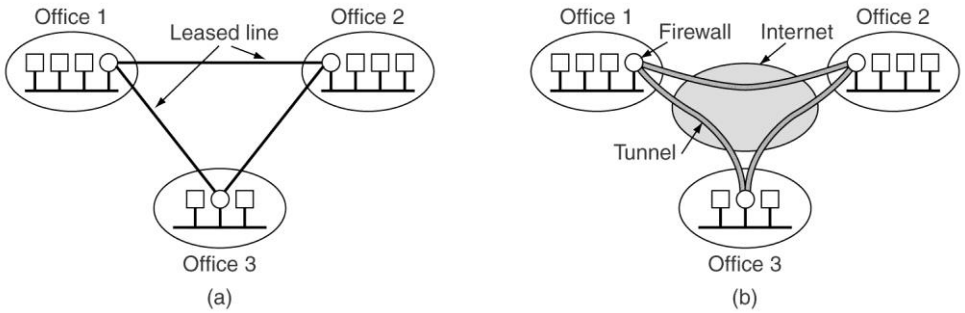
a) **Transport**: viene cifrata la trama di trasporto (TCP Header + Payload)

b) **Tunnel**: viene cifrato il pacchetto IP (old IP header+TCP header+Payload)



VPN (Virtual Private Network)

Una Virtual Private Network o VPN è una rete privata instaurata tra soggetti che utilizzano un mezzo di trasmissione pubblico e condiviso come ATM o, più frequentemente, Internet.



L'utilizzo tipico in Internet è

- tra 2 o più LAN remote
- tra una LAN e un singolo host (e.g. Una persona che si trova all'esterno della propria struttura e vuole connettere il proprio portatile come se fosse all'interno.)

In entrambi i casi viene generato un tunnel protetto tra 2 gateway.

I protocolli più utilizzati per realizzare il tunnel cifrati sono:

- IPsec, SSL/TLS, PPTP (Point-to-Point Tunnelling Protocol di Microsoft)

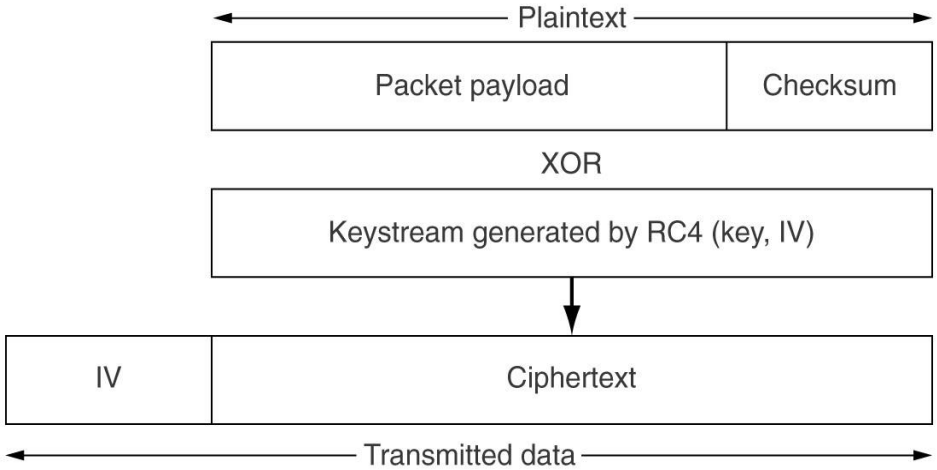
Use Cases: Forticlient (in uso in UNIPR) https://forticlient.com/techspec

Sicurezza WiFi: WEP

I collegamenti Wireless sono particolarmente esposti ad attacchi alla sicurezza per mancanza di barriere fisiche.

WEP (Wired Equivalent Privacy) è stato il primo algoritmo di cifratura (1999) utilizzato per proteggere le comunicazioni Wifi (802.11).

Utilizza RC4 con chiavi a 40 o 104 bit, combinato con un Vettore di Inizializzazione (IV, 24 bit) che viene spedito in chiaro assieme al testo cifrato (simile al salt).



Problemi:

- La chiave è condivisa. L'Algoritmo è violabile (Borisov 2001)
- Il CRC non è sicuro: è possibile modificare il messaggio mantenendo coerente il CRC, anche senza conoscere la chiave.

Sicurezza WiFi: WPA e 802.11i

Storia: Per superare la debolezza della cifratura *WEP*, il Working Group 802.11 ha ratificato nel 2004 un nuovo standard di sicurezza per 802.11 denominato *802.11i,* con l'obiettivo di rafforzare la cifratura e introdurre l'autenticazione.

In attesa di 802.11i la "WiFi Alliance" (il gruppo che gestisce lo standard WiFi) aveva sviluppato il protocollo **WPA** (WiFi Protected Access) che supporta parzialmente 802.11i. WiFi Alliance ha invece denominato WPA2 il nuovo protocollo 802.11i.

Dal 2006 la certificazione WPA2 è obbligatoria per tutti i nuovi dispositivi con marchio Wi-Fi

Cifratura: WPA**,** come WEP, utilizza la cifratura simmetrica RC4 mentre WPA2 utilizza AES. La chiave oltre che Pre-Shared (PSK) può essere cambiata dinamicamente con il protocollo TKIP (Temporal Key Integrity Protocol).

Autenticazione: La modalità WPA-Enterprise utilizza lo standard **IEEE 802.1x** per gestire l'**autenticazione dei client e dei server** e la distribuzione di **differenti chiavi per ogni utente**. In questa modalità è necessaria la presenza di un server di autenticazione Radius.

IEEE-802.1X

E' uno standard per autenticare e autorizzare l'accesso alla rete (LAN, WiFi) stabilendo una connessione punto-punto cifrata tra Supplicant (client) e Authenticator (Access Point Wifi, Switch, ..). Generalmente l'Authenticator si rivolge ad un Authentication Server (es: server Radius).

Quando il Supplicant chiede l'accesso alla rete deve prima autenticarsi all'Authenticator (Access Point) mediante il protocollo EAP (Extensible Authentication Protocol) over LAN (EAPOL). L'autenticatore reincapsula EAP nel protocollo RADIUS utilizzato per la comunicazione tra Access Point e l'Authentication Server (Radius Server).