

Crittografia: altre applicazioni, alle reti e non solo

uso della crittografia a livello 2

autenticazione a livello 2 point to point

- gli estremi di una connessione ppp sono tipicamente autenticati
 - vedi connessioni dial-up e adsl
- protocolli famosi:
 - **Password Authentication Protocol (PAP)**
 - richieste di autenticazione con password in chiaro!
 - **Challenge-Response Handshake Protocol (CHAP)**
 - il server invia un challenge, il client risponde con un MAC del challenge (shared secret)
 - richiesta ripetuta durante la sessione (anti hijacking)
 - **MS-CHAP**— versione Microsoft di CHAP
 - lo shared secret è derivato dalla password
 - **Extensible Authentication Protocol (EAP)**

EAP

- RFC 3748
- framework per la negoziazione di meccanismi di autenticazioni arbitrari
- prevede una negoziazione del metodo di autenticazione
 - metodi diversi prevedono protocolli di autenticazione diversi (e quindi una sequenza di messaggi diversa)
- eap methods (sono oltre 40)
 - es. eap-md5: autenticazione one-way,
 - es. eap-tls: usa tecniche simili a tls
- è possibile il supporto per token card, dispositivi biometrici, OneTimePasswords, Smart Card, certificati digitali ...

autenticazione a livello 2 per LAN

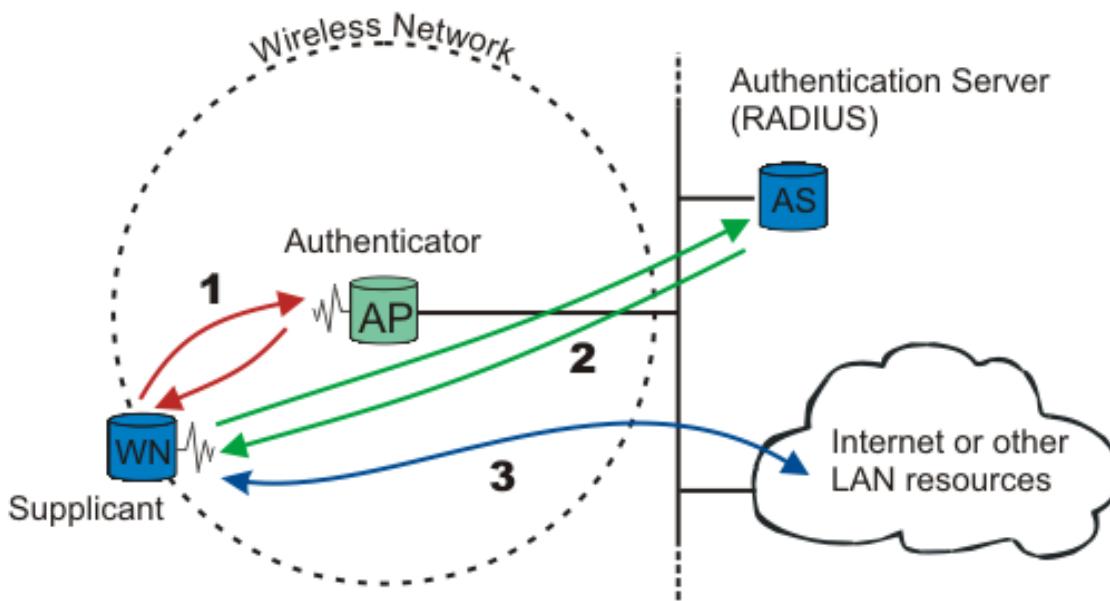
- ieee 802.1X
- è un modo di incapsulare EAP in frame su LAN
 - detto anche EAPoL (EAP over LAN)
- il server è tipicamente un apparato di rete
 - switch
 - access point
 - ...
- scomodo avere uno user db in un apparato di rete si usa un server di autenticazione centralizzato

autenticazione centralizzata

radius

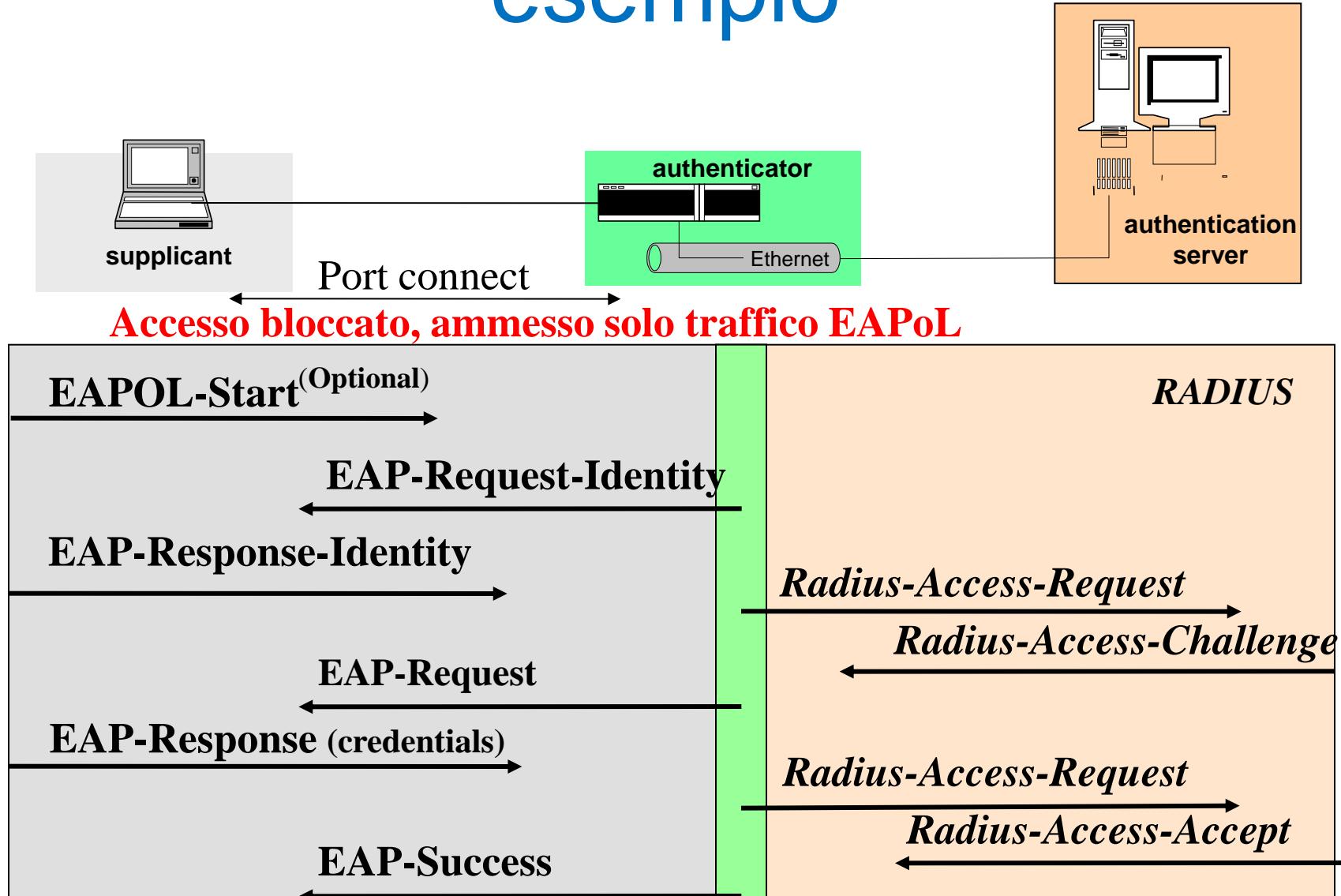
- rfc 2865, rfc 2866
- su udp
- supporto per EAP (rfc 3579)
- elementi
 - User (pc, laptop, telefono, ecc)
 - Radius server
 - autorizza o meno l'accesso alla rete
 - User database
 - ldap, dbms, ecc
 - Network Access Server (NAS, client del radius server)
- protocolli analoghi e concorrenti
 - diameter (rfc 6733), usato in principalmente da operatori di telecomunicazione
 - tacacs, tacacs+ (più vecchi)

802.1X e radius



- supplicant (user) usa EAPoL con l'autenticator (in questo caso un access point che fa da NAS)
- l'autenticator passa i messaggi EAPoL al authentication server usando RADIUS e il supporto per EAP
- quando l'autenticator riceve la conferma dall'authentication server che il supplicant è autenticato allora permette al traffico del supplicant di raggiungere la rete

esempio



Accesso concesso (con eventuali vincoli) dall'autentication server

wireless

- wep (obsoleto e vulnerabile)
 - rc4 (40bit key, 24bit iv), integrity con crc-32
- wpa
 - ha bisogno IEEE 802.1X server
 - distribuisce pre-shared secret diversi a ciascun utente, mutua autenticazione
 - rc4 (128bit key, 40bit iv)
 - key rollover
 - integrity con mac e frame counter (no replay attack)
- 802.11i (wpa2)
 - evoluzione di wpa
 - tra le altre cose usa AES
- wpa3
 - forward secrecy, migliore scambio di chiavi iniziale

Virtual Private Networks (VPN)

Virtual Private Networks

crittografia a livello 3

- Internet e le reti degli ISP costano poco ma sono non fidate
- le VPN sono reti private “sicure” ricavate da infrastrutture pubbliche
- usate per
 - accesso da Internet alla “rete aziendale”
 - Intranet geograficamente distribuite
 - cioè collegamento di sedi distanti della stessa azienda
- attenzione: terminologia sovraccarica
 - Gli ISP offrono servizi che chiamano VPN che offrono dei Service Level Agreement per garantire una certa qualità del servizio e segregazione dal resto del traffico dell'ISP, ma non necessariamente usano tecniche crittografiche.
 - nulla vieta di usare una VPN crittografata assieme ad una VPN per QoS

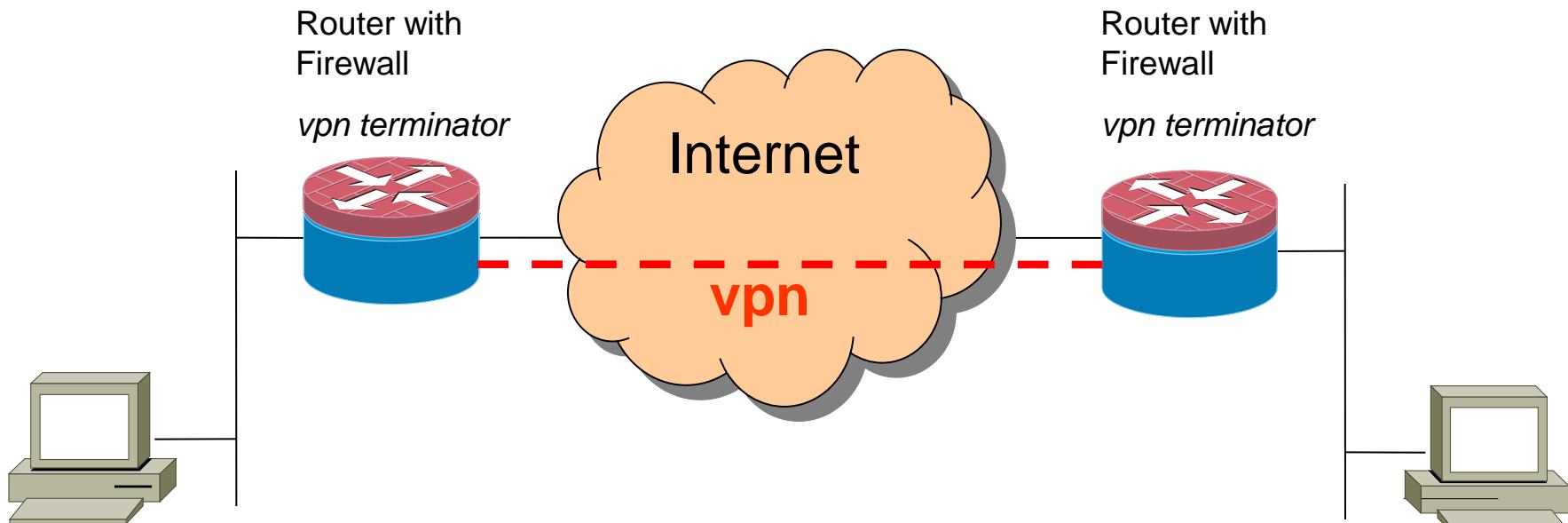
strumenti

- ssl/tls (OpenVpn),
- ssh (opzioni -L -R -W -D ecc.)
- IPsec (OpenSwan)
- altri protocolli e tools: WireGuard, PPTP, L2TP/Ipsec,

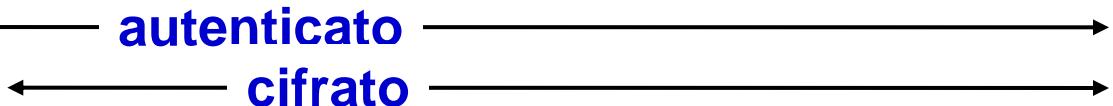
ipsec

- due protocolli crittografici per IP
 - Encapsulating Security Payload (ESP , rfc 4303)
 - confidenzialità (opzionale), integrità e autenticazione dei dati
 - Authentication Header (AH, rfc 4302)
 - integrità dei dati e di parte dell'header IP
 - raramente usato, non c'è motivo di autenticare l'header IP
- due modalità
 - tunnel mode
 - dati in ip(originale) in ipsec in ip(nuovo)
 - transport mode
 - dati in ipsec in ip
 - non strettamente necessario
 - più efficiente perché ha un header in meno (mtu maggiore)

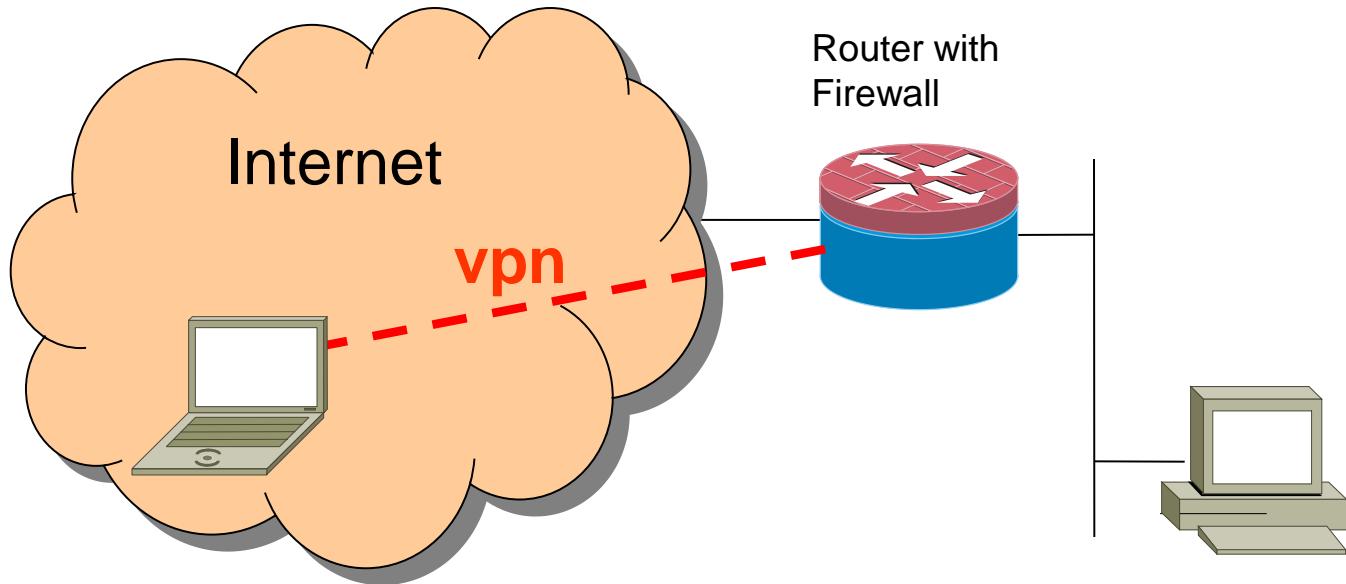
ipsec tunnel mode



**pacchetto
originale**



ipsec transport mode



pacchetto originale



↔ **autenticato** ↔

↔ **cifrato** ↔ 16

concetti IPsec

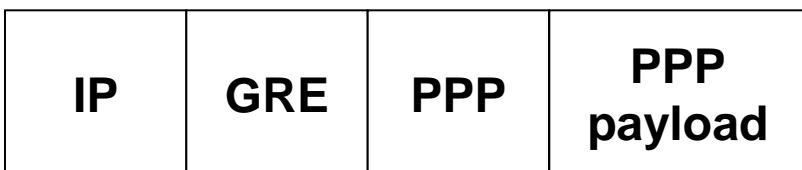
- security association (SA)
 - tra due macchine (addr, addr, modo, algoritmi, chiavi, SPI)
 - spi: security parameter index
 - identifica la SA, non bastano gli indirizzi poiché più security association possono essere instaurate tra le stesse macchine
 - l'spi viene inviato negli header ipsec
- security policy
 - quali pacchetti sono ammessi per essere instradati nel tunnel
 - in pratica è una politica di firewalling

chiavi di sessione

- le chiavi di sessione possono essere configurate manualmente o automaticamente
- Internet Key Exchange (IKE)
 - autenticazione
 - supporta sia chiavi pubbliche che shared secret
 - security association
 - negoziazione degli algoritmi di cifratura e di verifica di integrità
 - scambio chiavi di sessione
 - key rollover
 - protocollo molto complesso (forse troppo)
 - v1 (rfc 2407-2409, qualche problema di sicurezza)
 - v2 (rfc 4306, 4307, 7296)

pptp

- Microsoft
- Generic Routing Encapsulation (GRE, rfc 2784)
 - un protocollo per fare tunnel generici in IP
- protocollo di management del tunnel
 - tcp port 1723
 - problematico per i firewall
- ppp in gre in ip
- autenticazioni MSCHAP (basta una password) o EAP-TLS
 - challenge/response in chiaro
- crittografia opzionale
 - Microsoft Point-to-Point Encryption (MPPE)
 - RC4 chiavi 40-128 bit
- obsoleto



L2TP/IPsec

- Microsoft
- Layer2 Trasport Protocol (L2TP)
 - derivato da ppp incapsulato in udp
 - non prevede autenticazione
- IPsec ESP transport mode
- più sicuro di pptp
 - autenticazione strong tra macchine (IPsec/IKE)
 - autenticazione di utente (su ppp ma criptata)
- poco pratico
 - richiede setup di ipsec (shared secret o certificato)
- poco efficiente
 - mtu ridotto

IP	IPsec ESP	UDP	L2TP	PPP	PPP payload
----	--------------	-----	------	-----	----------------

altre applicazioni

posta elettronica

- pretty good privacy (PGP)
 - obsoleto
- Privacy Enhanced Mail (PEM)
 - IETF, obsoleto
 - usato come formato file (.pem)
- S/MIME (rfc 3850-3851)
 - creato da RSA
 - mime (rfc 2045-2049) + pkcs#7
- Posta Elettronica Certificata
 - in italia ha lo stesso valore legale di una raccomandata con ricevuta di ritorno

documenti crittografati

- criptati con una chiave simmetrica S
- S è cifrata con la chiave pubblica di ciascun soggetto autorizzato alla lettura
 - **S/MIME**
 - più destinatari ciascuno con la sua chiave pubblica
 - **EFS (encrypted filesystem windows XP)**
 - chiave privata e pubblica associata all'utenza
 - chiave privata è persa quando l'utenza viene cancellata
 - più soggetti possono essere autorizzati alla lettura di un file (agente di recupero)

confidenzialità dei files

- cifratura a livello di ...
 - file
 - directory
 - filesystem
 - partizione o disco (blocchi)
- encryption/decryption trasparente all'utente durante l'uso del file
- windows: encrypted filesystem (EFS)
 - encryption di file e directory
 - sharing di file cifrati
- Window BitLocker
 - a livello di disco
 - basato su TPM
- linux
 - Linux Native Filesystem Encryption (fscrypt): directory level
 - Encfs, eCryptFS, considerati obsoleti
 - ZFS: filesystem level
 - dm-crypt: partition level

One Time Passwords (OTP)

- poiché la password può essere rivelata facciamo in modo che si possa usare una sola volta
- HOTP: HMAC-based OTP (RFC 4226)
 - basati su segreto condiviso K e un contatore C che deve essere sincronizzato tra le due parti
 - C monotono crescente
 - idealmente $\text{HMAC}(\text{SHA1}, C, K)$ viene scambiato per autenticare, in realtà si scambia un derivato digitabile di 6-8 cifre
- TOTP: Time-based OTP (RFC 4226)
 - come HOTP ma C è sostituito da un timestamp
 - le parti si devono accordare su K
 - spesso fatto con un qr-code
- ampio supporto, spesso richiesto per 2FA
 - software open source o proprietari su desktop e mobile
 - dispositivi hardware