

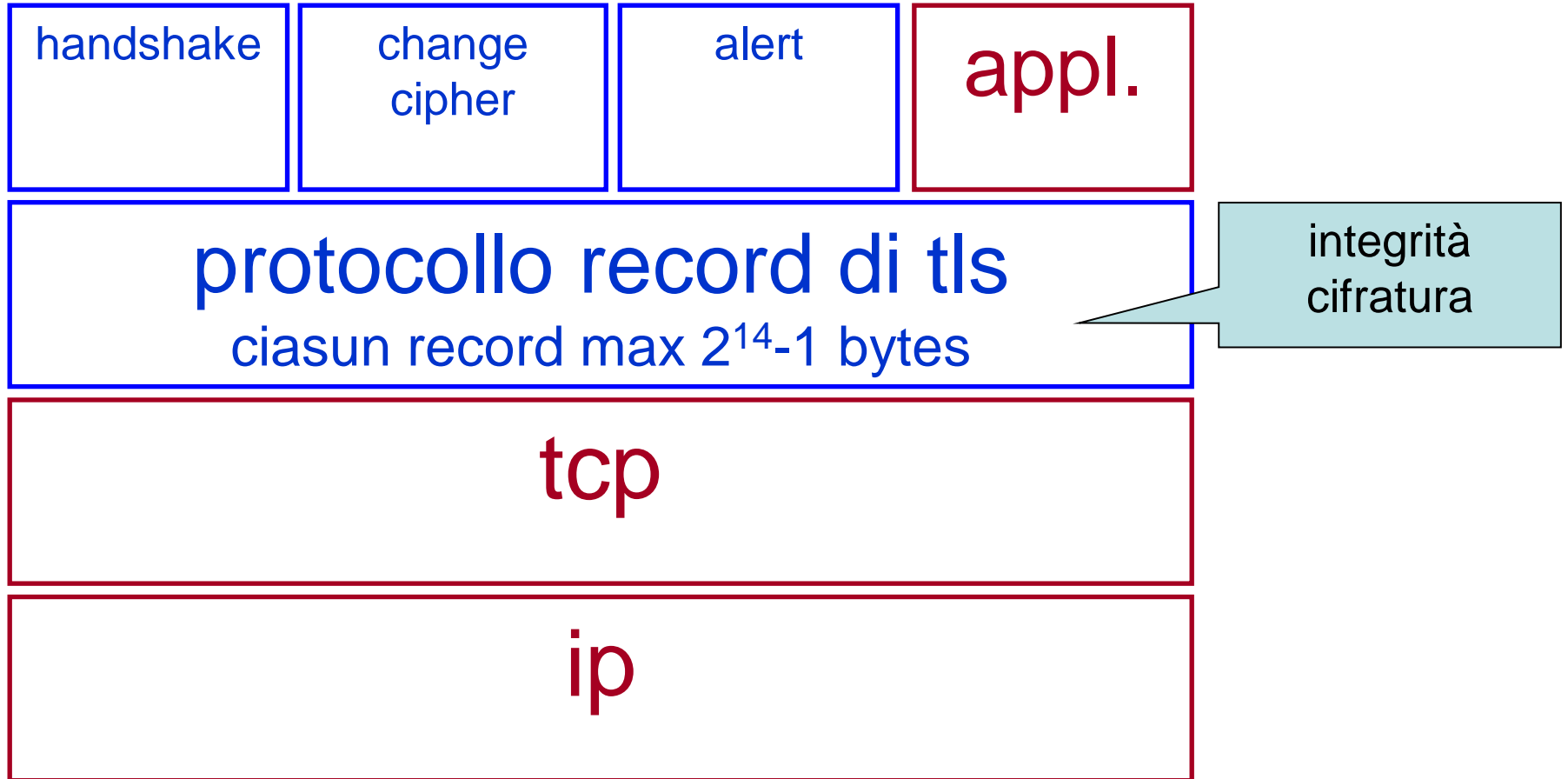
applicazioni della crittografia

protocolli di trasporto ssl, tls e ssh

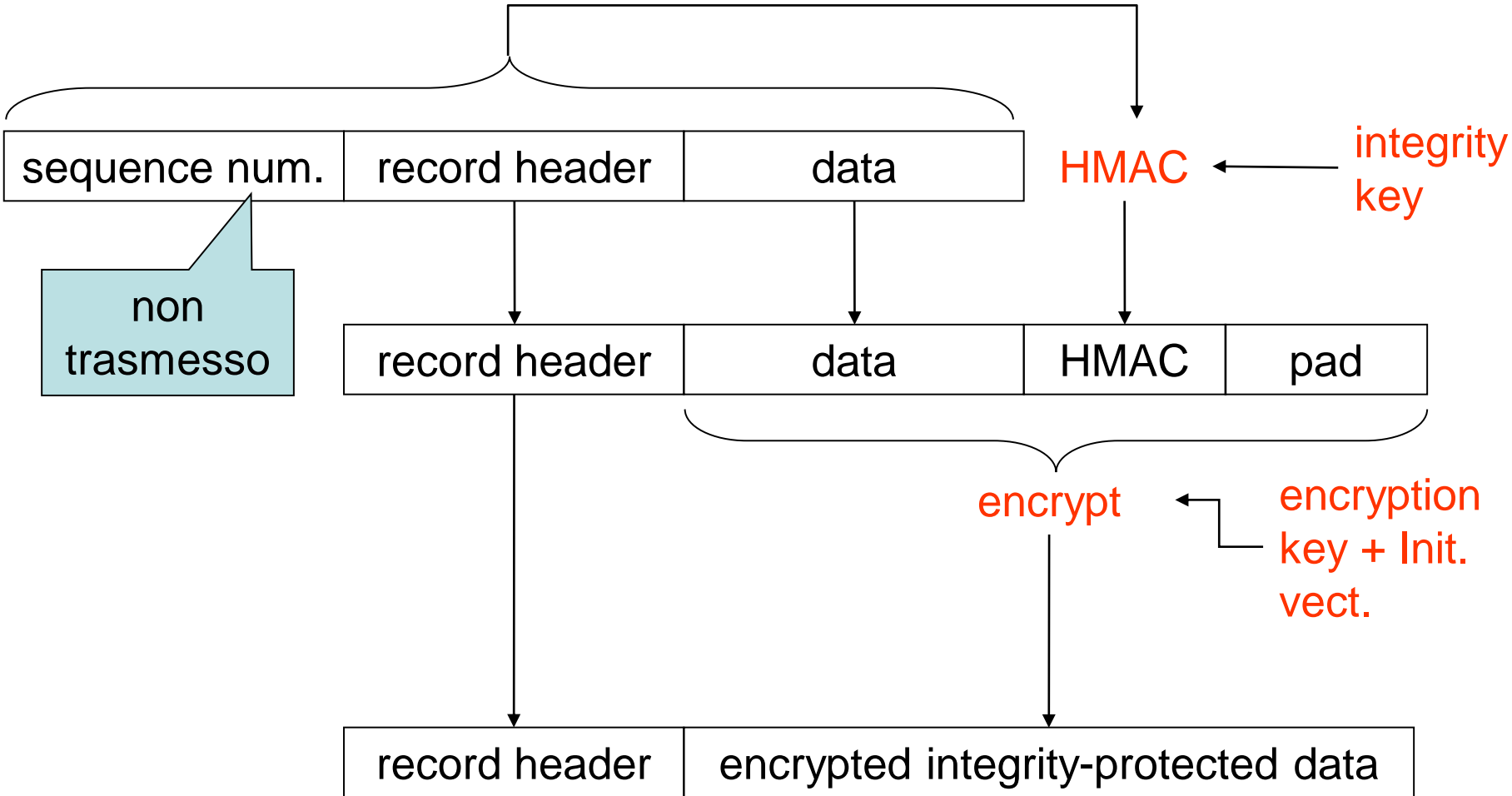
descrizione generale

- Secure Socket Layer (Netscape)
 - versione 2, obsoleta, qualche vulnerabilità
 - versione 3
- Transport Layer Security (IETF, rfc2246)
 - versione 1, molto simile a SSLv3 ma incompatibile
 - v1.1, v1.2, v1.3
- protocolli del tutto generali
 - usati spesso per http (https su porta 443)
 - usati anche per imap, pop, telnet
- supportati dalle applicazioni più diffuse
- sono protocolli piuttosto complessi

il rapporto con la pila osi



cifratura dei record



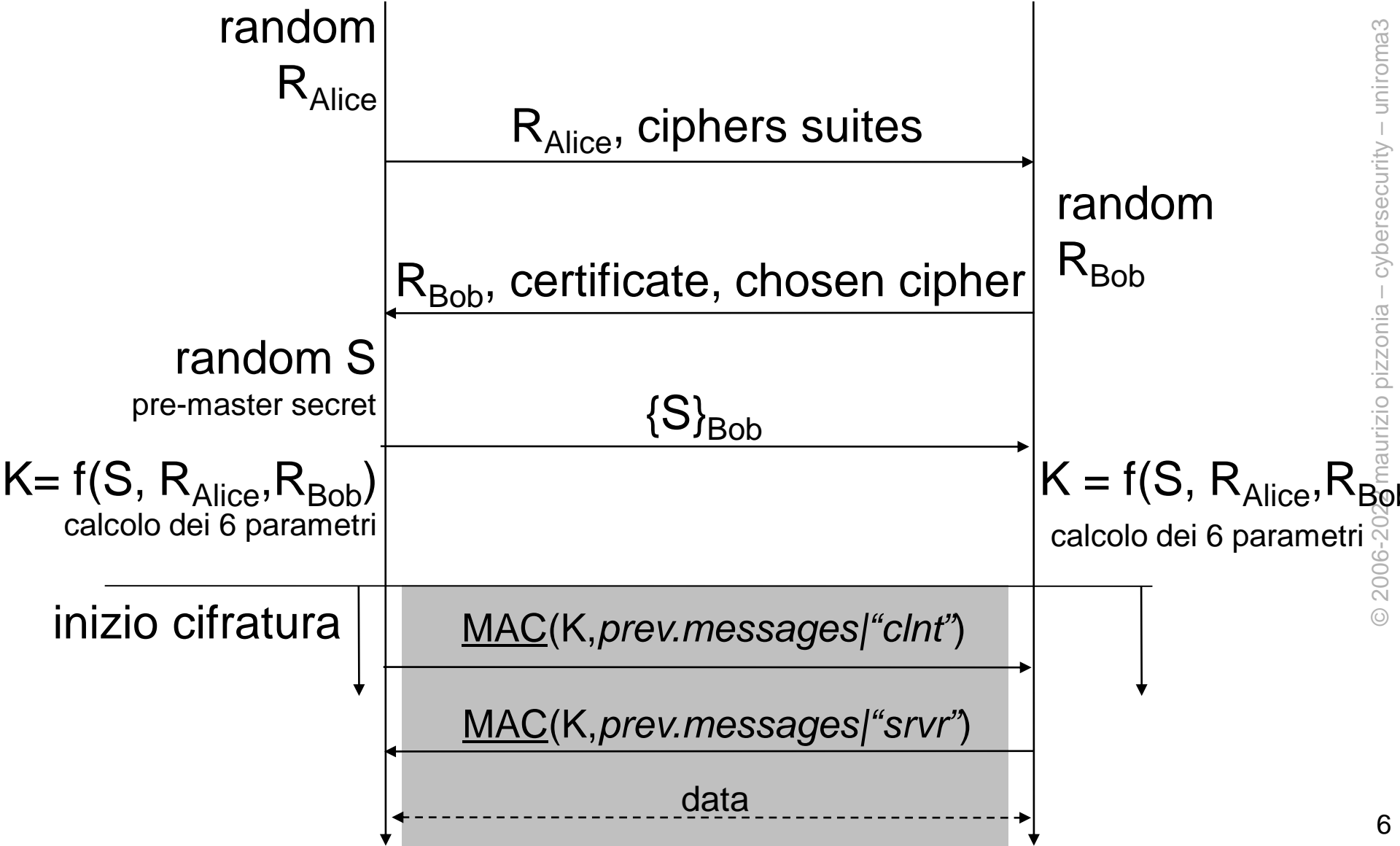
stato della connessione

- per iniziare una connessione cifrata i due devono accordarsi su...
 - algoritmo di cifratura
 - hash function per HMAC
 - come scambiare “la chiave” (pre-master secret)
- ... e su i seguenti 3 segreti per ciascuna direzione (totale 6)
 - integrity protection key
 - encryption key
 - Initialization Vector (necessario per molti algoritmi di cifratura a blocchi, es. DES)
 - sono tutti calcolati a partire dal pre-master secret

scambio rsa

Alice

Bob



esercizio

- perché SSLv3/TLS inseriscono un controllo di integrità per l'handshake?

varianti

- il client può fornire un proprio certificato per essere autenticato
- diffie-hellman
 - il server interviene nella creazione di S
 - autenticato con RSA o DSS
- diffie-hellman ephemeral
 - le chiavi vengono generate per la sessione e poi dimenticate
 - forward secrecy
- session resumption

cipher suites di TLS

- una cipher suite è un insieme di algoritmi da usare per la cifratura, l'integrità, e lo scambio di chiavi
- esempio di stringa identificativa di una cipher suite

TLS_RSA_WITH_3DES_EDE_CBC_SHA

chiavi
scambiate
con RSA

cifratura:
3DES nella
variante EDE
CBC

integrità:
HMAC con
SHA-1

default, usato
solo per
handshake

alcune

cipher suites di TLS

forward
secrecy

TLS_NULL_WITH_NULL_NULL

TLS_RSA_WITH_NULL_MD5

TLS_RSA_WITH_NULL_SHA

TLS_RSA_EXPORT_WITH_RC4_40_MD5

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5

TLS_RSA_WITH_IDEA_CBC_SHA

TLS_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_RSA_WITH_DES_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_DSS_WITH_DES_CBC_SHA

TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA

TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_RSA_WITH_DES_CBC_SHA

TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

TLS_DHE_DSS_WITH_DES_CBC_SHA

TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

TLS_DHE_RSA_WITH_DES_CBC_SHA

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

TLS_DH_anon_WITH_RC4_128_MD5

TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_anon_WITH_DES_CBC_SHA

TLS_DH_anon_WITH_3DES_EDE_CBC_SHA

deprecati perché DH
non autenticato è
vulnerabile a MitM

elliptic curve cryptography (ECC)

- stessi algoritmi nuova definizione di gruppo
- molto più efficiente a parità di sicurezza
- da RFC4492...

Symmetric		ECC		DH/DSA/RSA
80		163		1024
112		233		2048
128		283		3072
192		409		7680
256		571		15360

esempi di cipher suites con ECC

- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA

currently recommended suites in TLS 1.2

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305

adopted to avoid relying only
on AES
(What if a vulnerability is
found in AES? We need a
recommended alternative!)

TLS 1.3

- simpler cypher suites names
- certain algorithms are inferred by other means among limited alternatives
 - key exchange method: DHE or ECDHE
 - authentication: RSA or ECDSA

- shorter suites list

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

TLS_AES_128_CCM_8_SHA256

TLS_AES_128_CCM_SHA256

- also dropped support for some rarely used, or weak, features

- Compression, CBC, Non-AEAD ciphers, Renegotiation of encryption parameters, RC4, DSA, MD5, SHA1, RSA Key Exchange, DH, ECDH

TLS 1.2 vs 1.3

- TLS 1.2 is not deprecated
 - TLS 1.1 and 1.0 are deprecated
- TLS 1.2 is not going to be deprecated soon
- TLS 1.3 is...
 - simpler
 - hard to configure insecurely
 - supported only by recent software

ssh

- ssh è un concorrente di ssl/tls
 - v1 (vulnerabile), v2 attualmente in uso
- del tutto generale
 - usato soprattutto come telnet criptato
 - si può fare tunneling di qualsiasi cosa in ssh (opzioni – L e –R)
 - ma ora si può fare anche con ssl (vedi “stunnel”)
- companion protocols/commands
 - scp, sftp
- diffusione
 - famoso (implementazione open: openssh)
 - ampiamente supportato
 - standardizzato
 - rfc 4250-4256 e seguenti
 - supporta autenticazione RSA ma **non supporta certificati e PKI**

altre applicazioni alle reti (oltre tls)

VPN

- Internet e le reti degli ISP costano poco ma sono non fidate
- le VPN sono reti private “sicure” ricavate da infrastrutture pubbliche
 - gli ISP offrono VPN con dei Service Level Agreement per garantire una certa QoS
- usate per
 - accesso da Internet alla “rete aziendale”
 - Intranet geograficamente distribuite
 - cioè collegamento di sedi distanti della stessa azienda

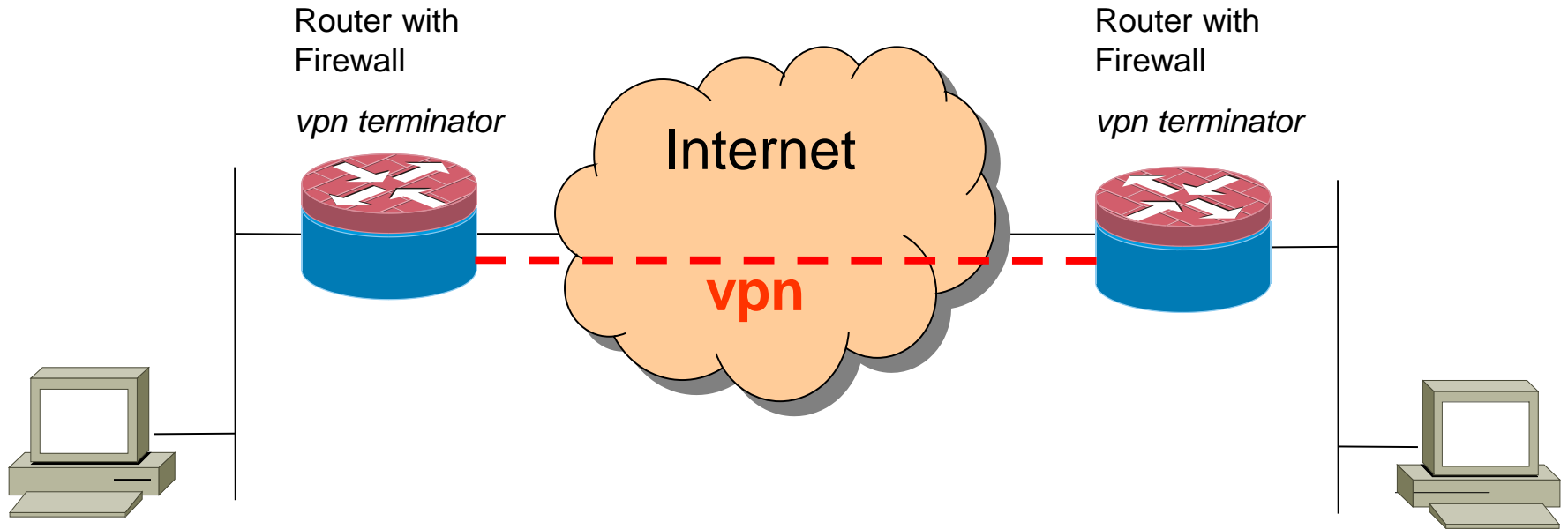
strumenti

- ssl/tls (OpenVpn),
- ssh (opzioni -L -R -W -D ecc.)
- IPsec
- altro (PPTP, L2TP/IPsec)

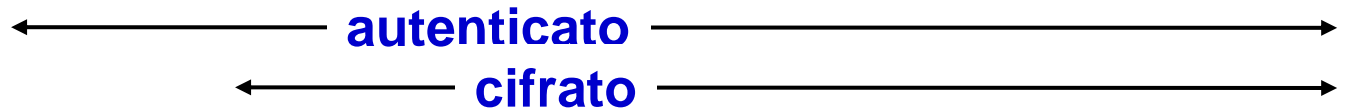
ipsec

- 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)

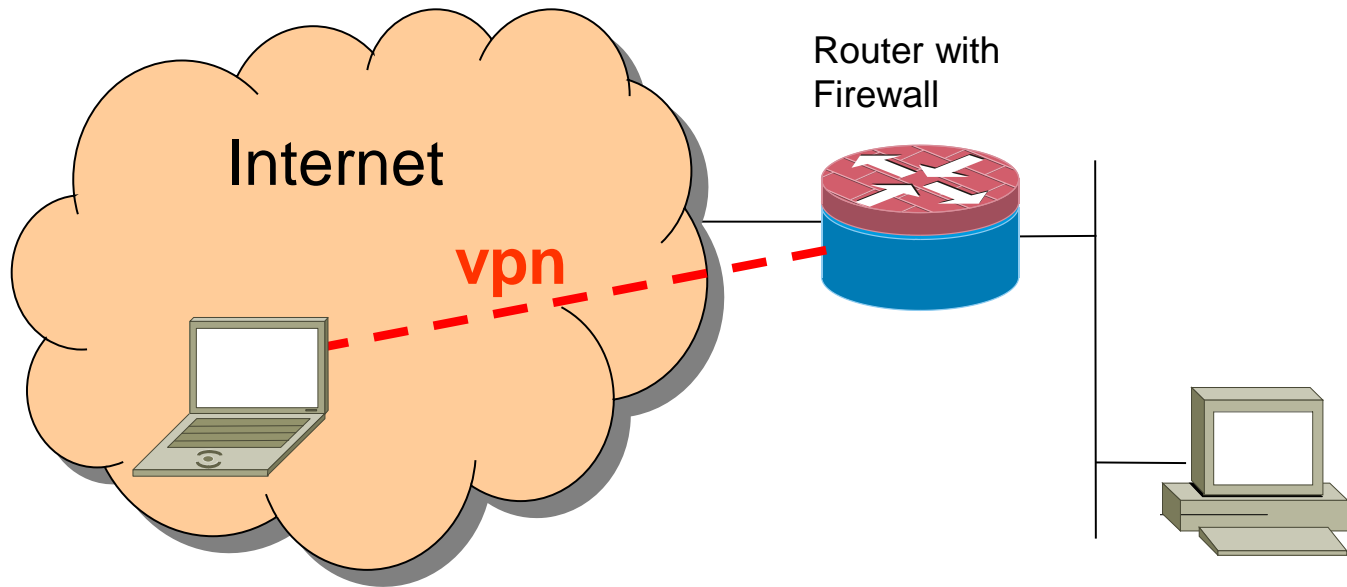
ipsec tunnel mode



pacchetto originale



ipsec transport mode



pacchetto originale



← autentificato →

← cifrato →

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 routing

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 proposto recentemente (rfc 4306, 4307)

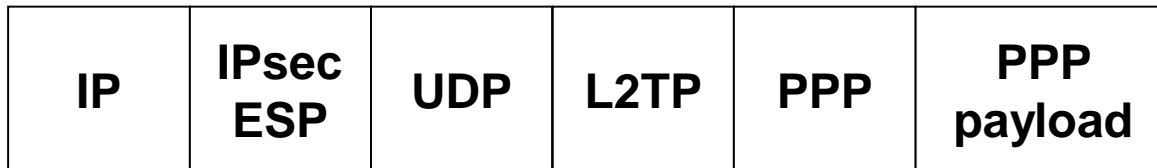
pptp

- 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

IP	GRE	PPP	PPP payload
-----------	------------	------------	------------------------

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



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 ...

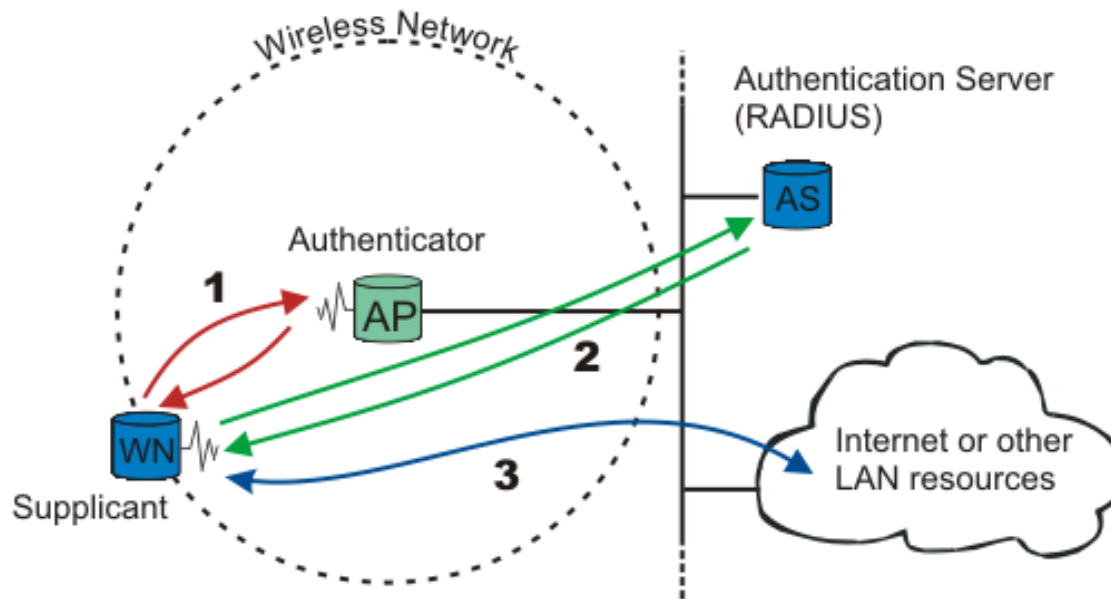
autenticazione a livello 2 per LAN

- 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...

radius

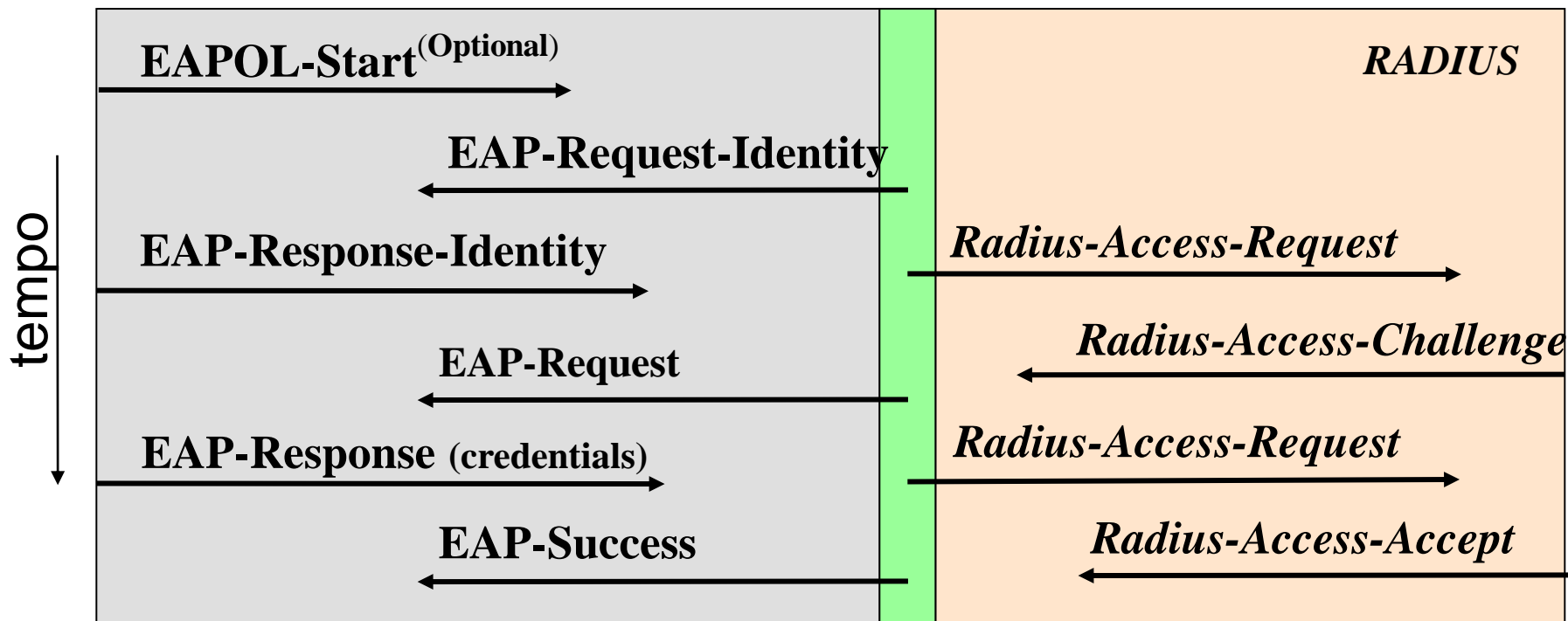
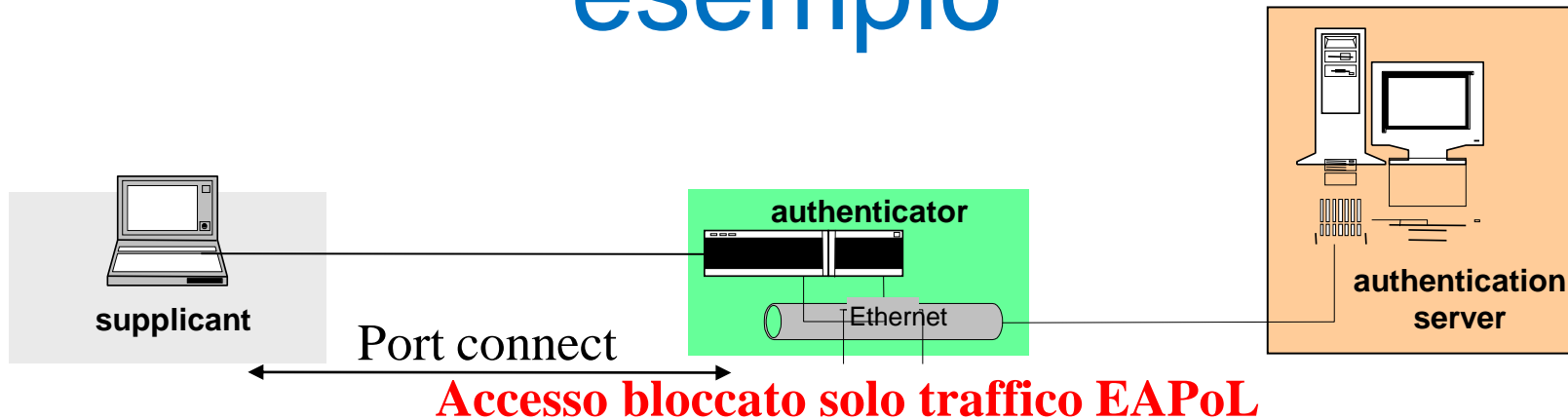
- rfc 2865, rfc 2866
- su udp
- supporto per EAP (rfc 3579)
- elementi
 - User (pc, laptop, telefono, ecc)
 - Radius server
 - autorizza o meno l'accesso alla rete
 - User database
 - ldap, dbms, ecc
 - Network Access Server (NAS, client del radius server)
- protocolli analoghi e concorrenti
 - diameter (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

altre applicazioni non di rete

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

- criptazione a livello di
 - file
 - directory
 - filesystem
 - disco
- windows: encrypted filesystem (EFS)
 - più utenti possono aprire un file criptato
 - encryption/decryption trasparente all'utente durante l'uso del file
 - disponibili servizi commerciali per decrittare senza chiave
- Window Vista: BitLocker
 - a livello di disco
 - basato su TPM
- linux
 - encfs,ecryptfs,fcrypt: directory level
 - raiser4, 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
- generazione di un insieme di passwords
 - Lamport: $h(p)$, $h(h(p))$, $h(h(h(p)))$,
 - le passwords vengono chieste a partire dall'ultima
 - sniffare un telnet o vedere un login non aiuta a entrare nel sistema
 - l'utente deve tenere privato l'insieme di passwords!
 - per ciascun utente si memorizza l'hash dell'ultima password
- time-synchronized OTP
 - dispositivo hardware con clock sincronizzato con il server
 - genera password che dipendono dal tempo