Operazione Rif. PA 2022-17295/RER approvata con DGR 1379/2022 del 01/08/2022 finanziata con risorse del Programma Fondo sociale europeo Plus 2021-2027 della Regione Emilia –Romagna.

Progetto n. **1** - Edizione n. **1**

MODULO: N. 6

Titolo: SICUREZZA DEI SISTEMI INFORMATICI

DOCENTE: MARCO PRANDINI

Parte 4 – Sicurezza delle reti

Attacchi passivi

- Gli attacchi passivi non modificano i dati in transito
- Possono essere utili per l'aggressore e comunque dannosi per la vittima:
  - la **scansione** è uno dei primi passi della ricognizione
  - lo **sniffing** può compromettere la riservatezza dei dati
  - il **recupero di una chiave** consente di impersonare la vittima
- Utilizzati contro se stessi possono far parte di un vulnerability assessment (dettagli in seguito)

Scanning - esempi

- Scansione di una rete
  - indirizzi raggiungibili
- Scansione di un host
  - porte TCP / UDP aperte
  - consente di dedurre le versioni del sistema operativo e dei servizi in esecuzione
- "Loudness"
  - per scopi VA, la scansione può essere aggressiva
  - Gli strumenti implementano molti modelli di scansione silenziosa per eludere il rilevamento

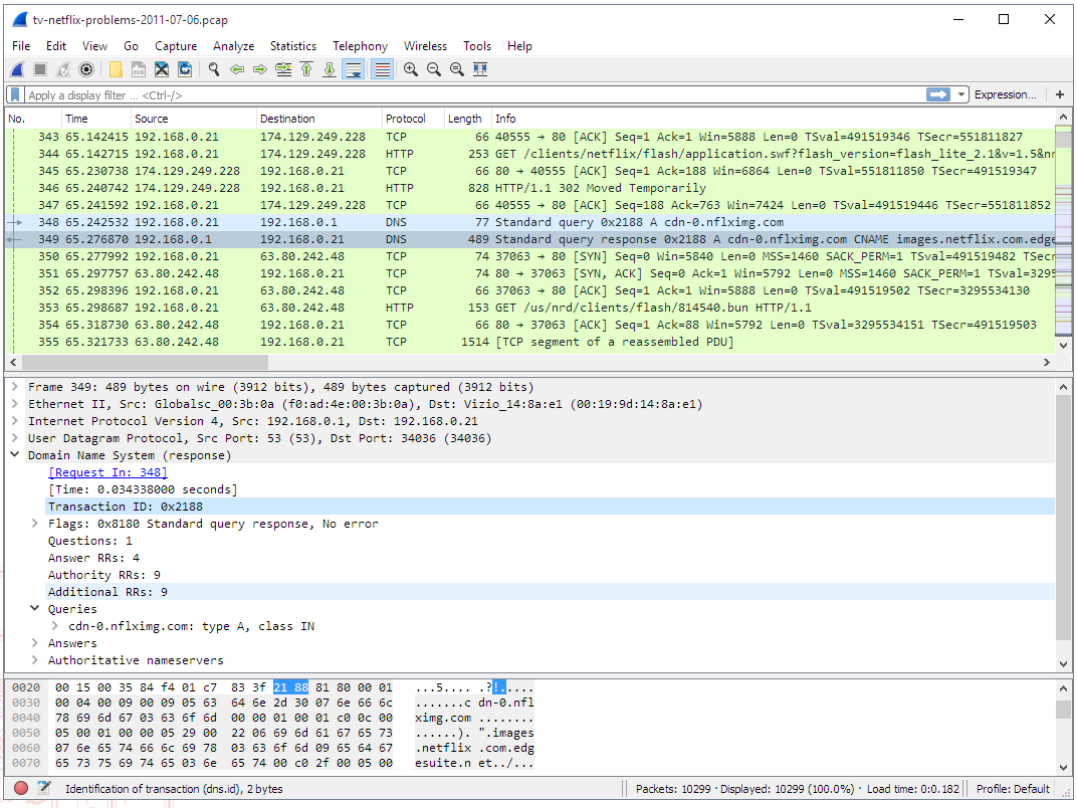
```
prandini@disi057118:~$ nmap -sP 137.204.57.200-205

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-05 13:23 CEST
Nmap scan report for disi057204.ing.unibo.it (137.204.57.204)
Host is up (0.00064s latency).
Nmap scan report for dei057205.dei.unibo.it (137.204.57.205)
Host is up (0.00058s latency).

Nmap done: 6 IP addresses (2 hosts up) scanned in 0.21 seconds
```

```
prandini@disi057118:~$ nmap -A 137.204.57.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-05 13:21 CEST
Nmap scan report for sia057104.ing.unibo.it (137.204.57.104)
Host is up (0.00020s latency).
Not shown: 992 closed ports
PORT    STATE SERVICE   VERSION
21/tcp  open  ftp       vsftpd 3.0.2
22/tcp  open  ssh       OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   1024 47:17:ab:76:24:e2:6b:d6:25:cf:bf:c5:2b:30:e9:84 (DSA)
|   2048 69:a0:58:25:09:06:a6:9d:36:d6:56:b3:55:0e:4e:88 (RSA)
|   256 85:d9:53:e0:dd:ce:46:61:a8:cc:29:7f:a1:50:8d:3c (ECDSA)
|_  256 cf:a5:51:fa:f5:84:63:f8:d4:cf:00:90:bf:d5:9f:68 (EdDSA)
80/tcp  open  http      Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)

Service Info: Host: darma.ing.unibo.it; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel
```

Sniffing

- Lo sniffing richiede l'accesso fisico ai dati in transito
  - essendo già sulla rete locale
  - a seguito di un attacco di dirottamento
- Su reti locali
  - wireless: tutto dovrebbe essere criptato, ma molti protocolli sono difettosi! (vedi seguito)
  - cablate: la crittografia esiste (802.1x per l'autenticazione delle porte, 802.1AE per la cifratura del traffico) ma non la usa quasi nessuno

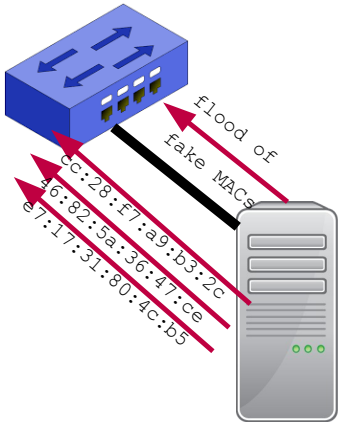
Sniffing – un esempio



MAC flooding

- Gli switch offrono una protezione limitata
  - idealmente, il traffico viene inviato solo sulla porta del destinatario
  - Se lo switch non trova un MAC nella CAM manda i pacchetti in broadcast
- Es. switch con CAM di dimensione 6 righe

Porta	MAC raggiungibile
1	eb:a6:99:de:1c:b0
1	2c:65:1e:b1:9f:44
3	0c:2e:22:b0:8e:16
4	5b:06:72:1b:3c:03
4	e4:b0:56:d5:2d:0f
4	92:ff:9e:6c:b0:8e



Porta	MAC raggiungibile
1	46:82:5a:36:47:ce
1	cc:28:f7:a9:b3:2c
1	e7:17:31:80:4c:b5
1	...
1	...other fake MACs
1	...

- Il MAC flooding costringe lo switch a comportarsi come un hub

Wireless key recovery

Ci sono quattro principali generazioni di protezione delle reti WiFi: WEP, WPA, WPA2, WPA3

- WEP (Wired Equivalent Privacy)
  - chiave simmetrica precondivisa
  - stream cipher RC4, falla di progettazione: è possibile recuperare la chiave se viene raccolto sufficiente testo cifrato prodotto dalla stessa chiave
  - la chiave è "randomizzata" da XOR con un IV piccolo (24 bit)
  - generate abbastanza traffico e l'IV si ripeterà
- WPA (WiFi Protected Access)
  - una patch intermedia durante il lancio di WPA2
    - sostituisce IV con TKIP (128 bit)
  - modalità personale con chiave precondivisa
    - nessuna segretezza in avanti: qualsiasi utente che conosce la chiave potrebbe decrittografare tutti i pacchetti
  - modalità aziendale con autenticazione utente su canale protetto

Wireless key recovery

- WPA2
  - a lungo considerato essenzialmente sicuro
  - grave vuln scoperta nel 2017: attacchi di reinstallazione chiave (KRACK)
    - Android e Linux possono essere indotti a (ri) installare una chiave di crittografia completamente zero
    - In altri dispositivi è comunque possibile decrittografare un gran numero di pacchetti
    - i pacchetti possono contenere credenziali utente con validità a livello aziendale!
  - Pre-shared key (PSK) corta se si usa WPS
- WPA3
  - vari miglioramenti a garanzia della scelta di cifrari robusti
  - sostituisce PSK con Simultaneous Authentication of Equals (SAE)
    - usa un sistema di handshake detto Dragonfly
  - vulnerabile ad attacchi Dragonblood
    - tipo 1: sfrutta la retrocompatibilità con WPA2 – attacco MITM per forzare downgrade
    - tipo 2: sfrutta implementazione non corretta di alcuni passaggi crittografici – consente password partitioning
  - dispositivi aggiornabili

Attacchi attivi

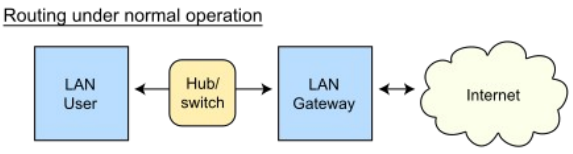
- Gli attacchi attivi minacciano l'integrità, l'autenticità o la disponibilità di reti e sistemi
- Spoofing e hijacking sono spesso un passaggio preliminare per un attacco più impattante, ad es.
  - rubare una rete per originare spam e scomparire
  - fingere un'identità di rete per rubare le credenziali
  - dirottare il traffico per fare sniffing
- Denial of Service (DoS) rende inaccessibile un servizio
  - ancora una volta come passaggio intermedio
  - ma anche come obiettivo principale

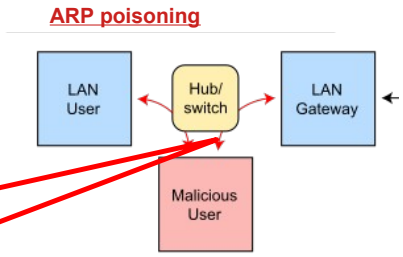
Link layer

- Spoofing MAC
  - assumere l'identità di un dispositivo a livello di indirizzo fisico
  - molto efficace
    - per bypassare ACL
    - per ottenere tutto il traffico destinato alla vittima
  - Limitato alla LAN
  - tecnicamente facile da mitigare: 802.1x
    (ma organizzativamente complesso → raro che lo si faccia!)

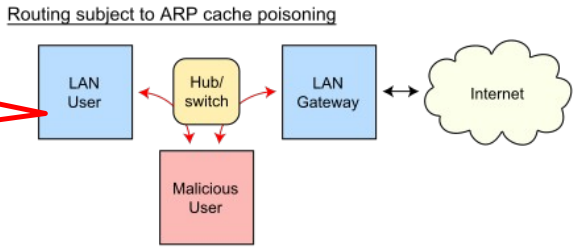
Link layer

- ARP poisoning
  - convincere un host (specialmente il gateway) che l'IP di una vittima è associato al MAC dell'attaccante





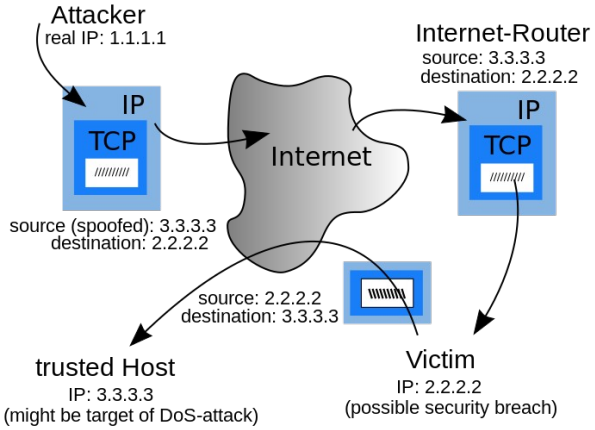
gratuitous ARP replies
"IP of gateway"
is at
"MAC of attacker"



Gli host usano la cache "avvelenata" e mandano sul cavo all'attaccante i pacchetti per l'IP del gateway

Network layer

- IP spoofing
  - assumere l'indirizzo IP di una vittima
  - efficace per dirottare il traffico solo su LAN
    - su Internet, il routing invierà le risposte agli indirizzi mimati
      - l'attaccante non può ottenerli
      - attacchi di *backscatter*! → →
- IP hijacking
  - i router si scambiano informazioni su come raggiungere le destinazioni
  - BGP non è autenticato!
  - Vedi alcuni esempi su http://completewhois.com
  - estende la portata dello spoofing IP su scala globale
- Entrambi utili per bypassare ACL e per dirottare le connessioni dopo l'autenticazione (vedere più avanti)



By original by Nuno Tavares, svg-convertion by Loilo92, this version:GGShinobi - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=27991853

Un caso famoso: Youtube & Pakistan Telecom

Dalla presentazione di Pilosov e Kapela a DEFCON16 (Las Vegas 2008)

- YouTube announces 5 prefixes:
- A /19, /20, /22, and two /24s
- The /22 is 208.65.152.0/22
- Pakistan's government decides to block YouTube
- Pakistan Telecom internally nails up a more specific route (208.65.153.0/24) out of YouTube's /22 to null0 (the routers discard interface)
- Somehow redists from static → bgp, then to PCCW
- Upstream provider sends routes to everyone else…
- Most of the net now goes to Pakistan for YouTube, gets nothing!
- YouTube responds by announcing both the /24 and two more specific /25s, with partial success
- PCCW turns off Pakistan Telecom peering two hours later
- 3 to 5 minutes afterward, global bgp table is clean again

https://virtuale.unibo.it/mod/unibores/view.php?id=538071
http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

Layer di trasporto e applicazione

- Se il dirottamento IP viene utilizzato per impossessarsi di una connessione dopo un'autenticazione, devono essere coinvolti i livelli superiori
  - UDP è privo di connessione: molto facile

    invece

  - TCP perderà la connessione se l'attaccante non utilizza i numeri di sequenza corretti per la finestra scorrevole
  - Spesso i protocolli a livello di applicazione utilizzano identificatori di sessione come i cookie HTTP
- In entrambi i casi l'attaccante ha due opzioni
  - indovinare (forza bruta, spesso molto difficile)
  - sfruttando lo sniffing (se già sul percorso dei dati)

(D)Dos

- Qualsiasi attacco dirottamento può causare un errore mirato
  - livello di trasporto: l'invio di un SN errato o un reset esplicito su connessioni TCP li interrompe
- Distributed Denial of Service
  - molti host coordinano i loro sforzi per saturare la capacità di rete o le risorse di calcolo della vittima
  - Le botnet sono insiemi di computer zombie che possono lanciare attacchi DDoS quando istruiti da comando e controllo (C&C)
    - Botnet IoT: Mirai, Bashlite, ...
- un controllo degli accessi impreciso sull'infrastruttura può peggiorare le cose
  - in termini di effetto
  - nascondendo l'origine
  - per esempio: attacchi di amplificazione DNS

Un esempio di esfiltrazione: DNS Tunnelling

- Query e risposte possono contenere dati
- Utilizzabile per esfiltrare dati da un computer infettato o per mettere in contatto un bot con il C&C

Protocolli ausiliari: DNS hijacking

- Un server DNS malevolo può fornire in risposta l'IP dell'attaccante quando viene richiesto dalla vittima di risolvere un nome legittimo
- DNS
  - non è autenticato
  - è distribuito
  - ha molti livelli di memorizzazione nella cache
- La falsificazione arbitraria è difficile ma ...
  - vedere più avanti per un attacco combinato
  - i server legittimi possono essere attaccati e portati ad agire in modo malevolo

DNS spoofing

- Query e risposta normali

www.amazon.com?

207.171.166.48

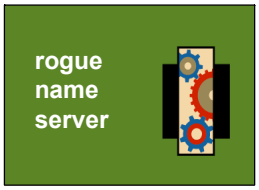
DNS spoofing

- Risposta falsificata

www.amazon.com?

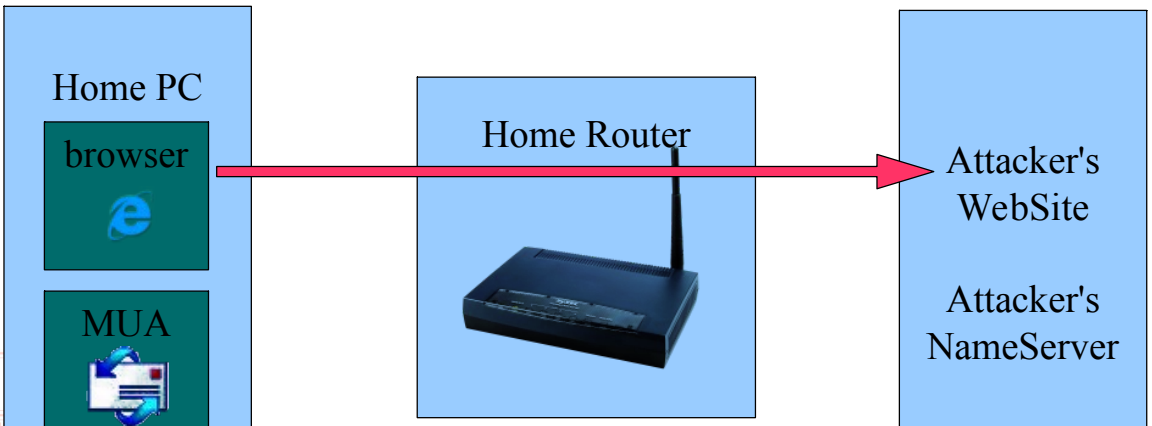
207.171.166.48 X

cracker address



DNS spoofing (pharming)

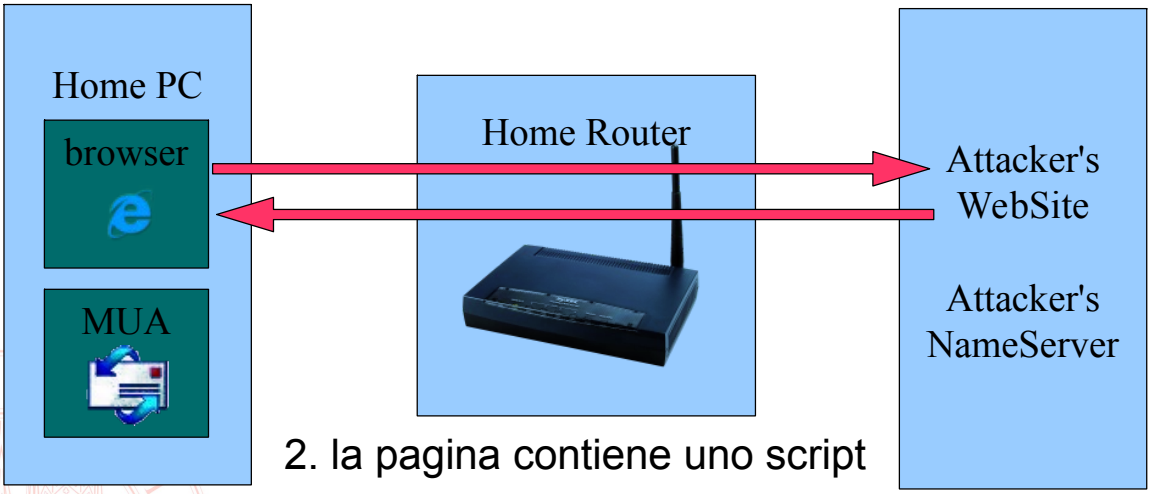
- Sembra difficile falsificare una risposta DNS?



1. L'utente visita una pagina HTML, consapevolmente o no

DNS spoofing (pharming)

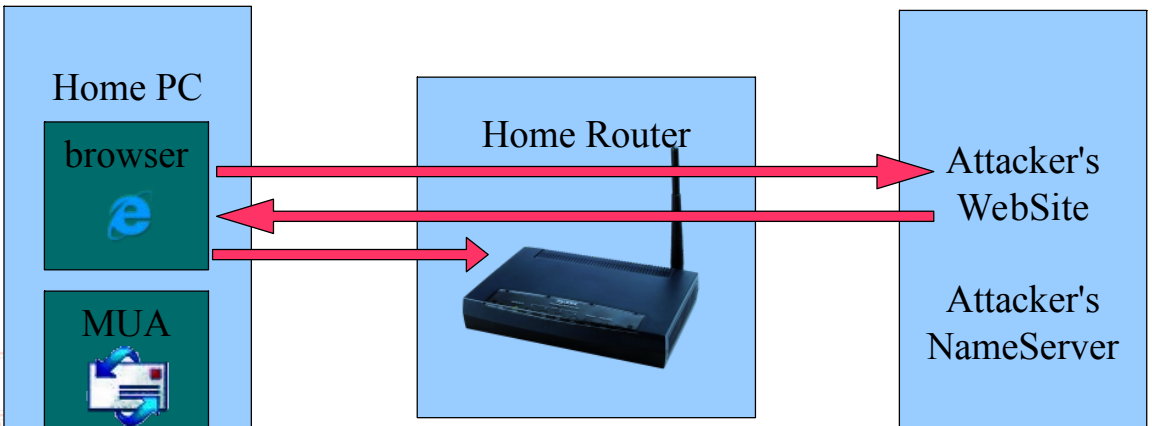
- Sembra difficile falsificare una risposta DNS?



2. la pagina contiene uno script

DNS spoofing (pharming)

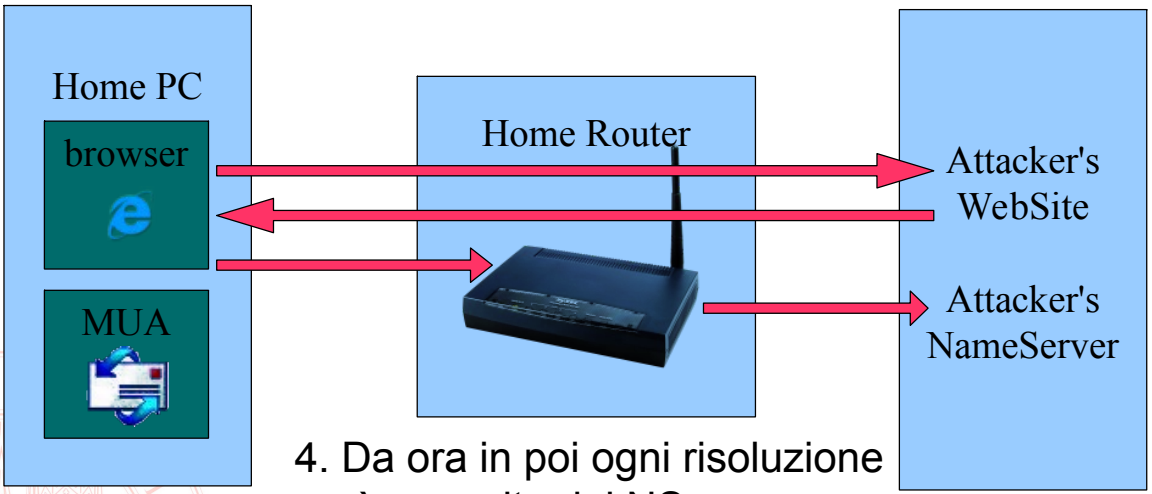
- Sembra difficile falsificare una risposta DNS?



3. lo script, usando la password di default del router, riprogramma il DNS

DNS spoofing (pharming)

- Sembra difficile falsificare una risposta DNS?

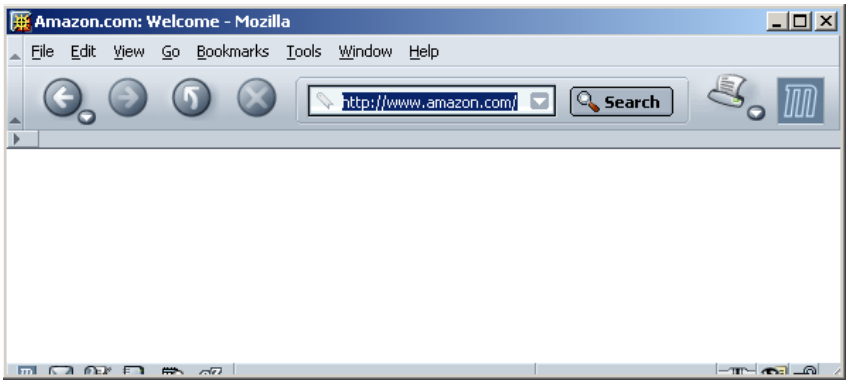


4. Da ora in poi ogni risoluzione sarà eseguita dal NS dell'attaccante

Contromisure e contro-contromisure

- HTTPS permette di bloccare questi attacchi
- … ma esistono modi
  - per evitare che venga visualizzata l'URL effettivamente visitata
  - o per far accettare al browser qualsiasi certificato

HTTPS

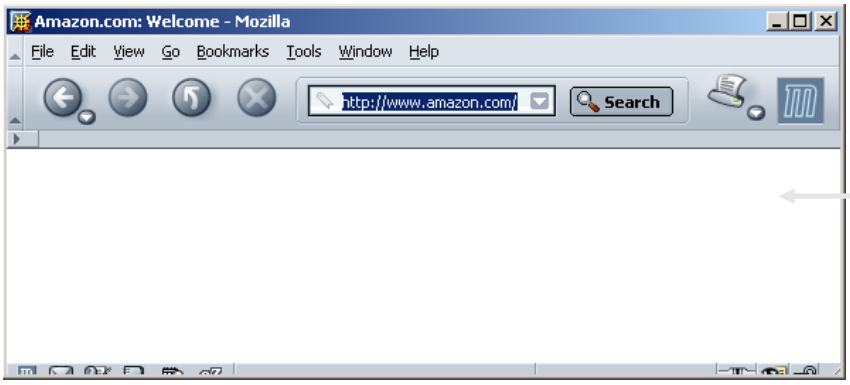


"Provami che hai la chiave privata di amazon"

amazon.com.

Web server @ crackeraddress

HTTPS



"Provami che hai la chiave privata di amazon"

amazon.com.

Web server @ crackeraddress

HTTPS

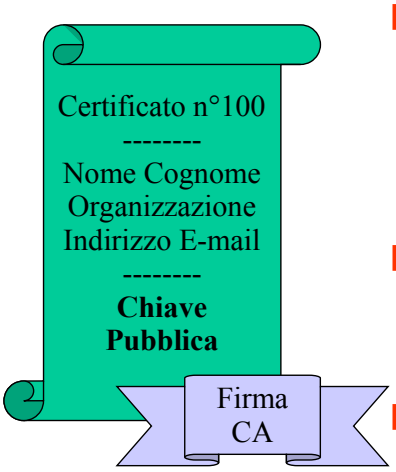
"Provami che hai la chiave privata di amazon"

amazon.com.

Web server @ crackeraddress

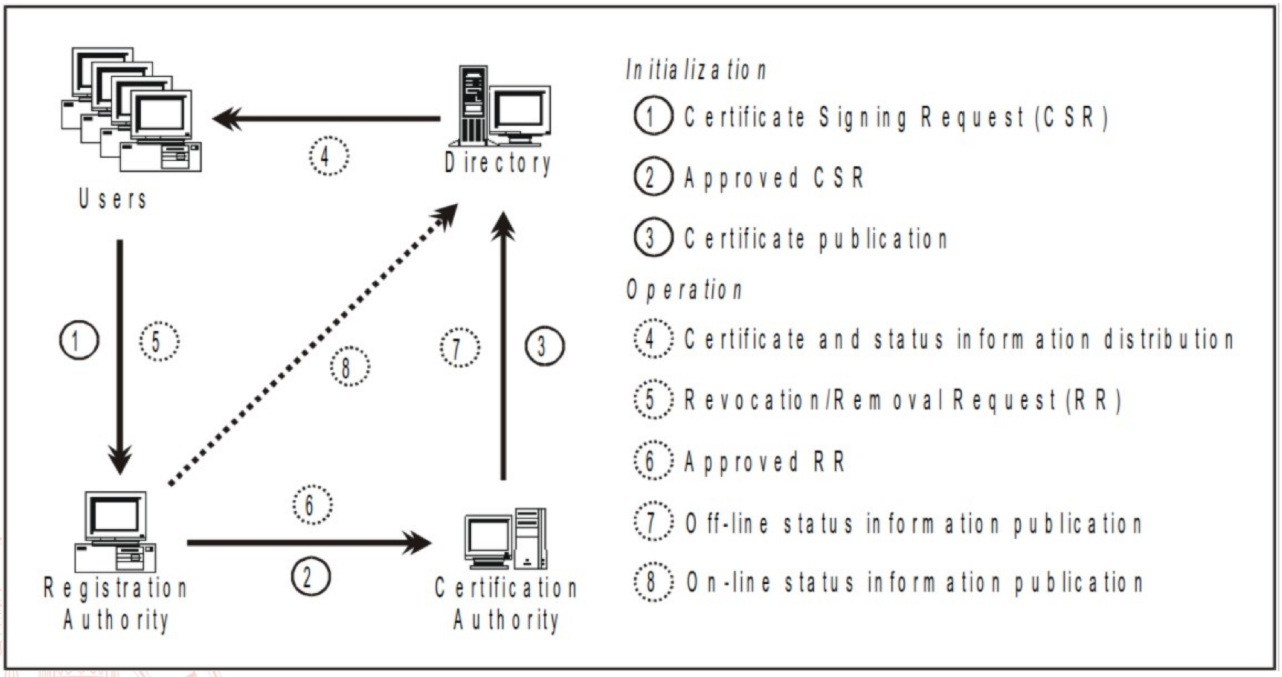
- **Come fa il browser a verificare la prova fornita dal web server?**
  - **Certificate store**
  - **Trusted CAs**

Certificazione della chiave pubblica

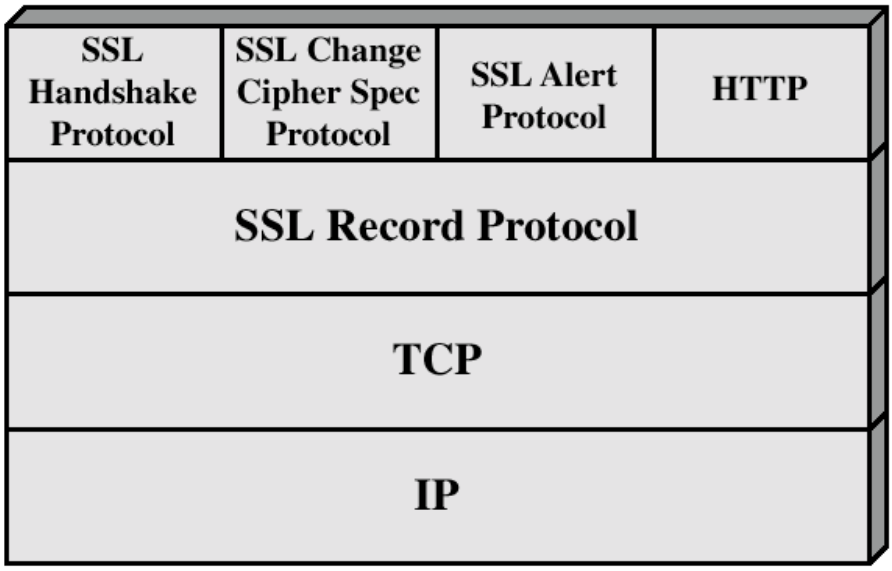


- Certificato X.509
  - Associa chiave e titolare
  - Autenticità e integrità garantite dalla firma digitale di una terza parte fidata (Certification Authority)
- Per verificare la firma serve la chiave pubblica della CA
  - Chi ci garantisce che questa sia autentica?
- Serve una Root of Trust

PKI – ciclo di vita dei certificati

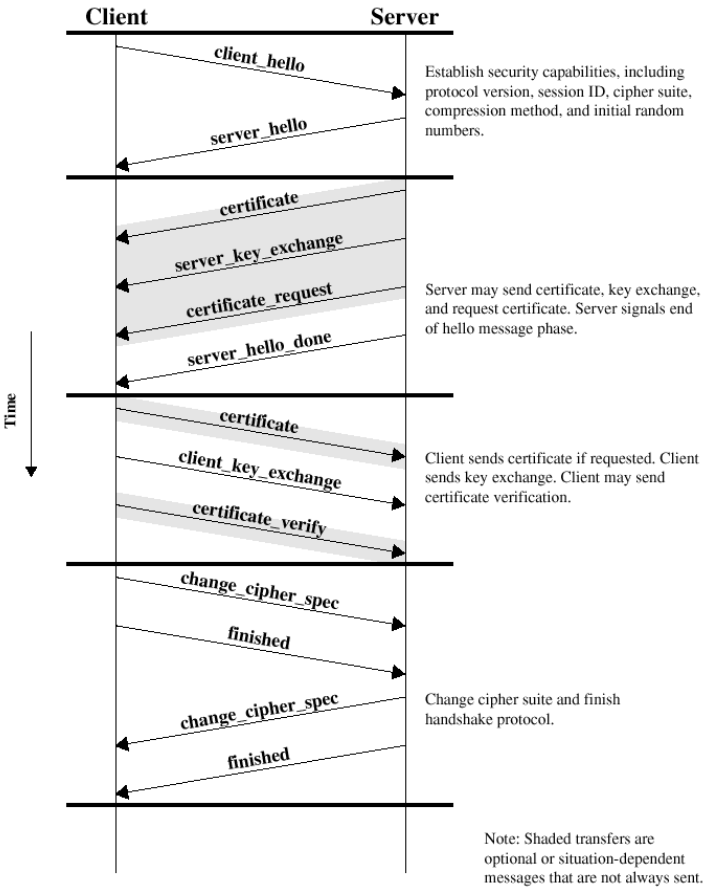


Architettura di SSL



Handshake Protocol

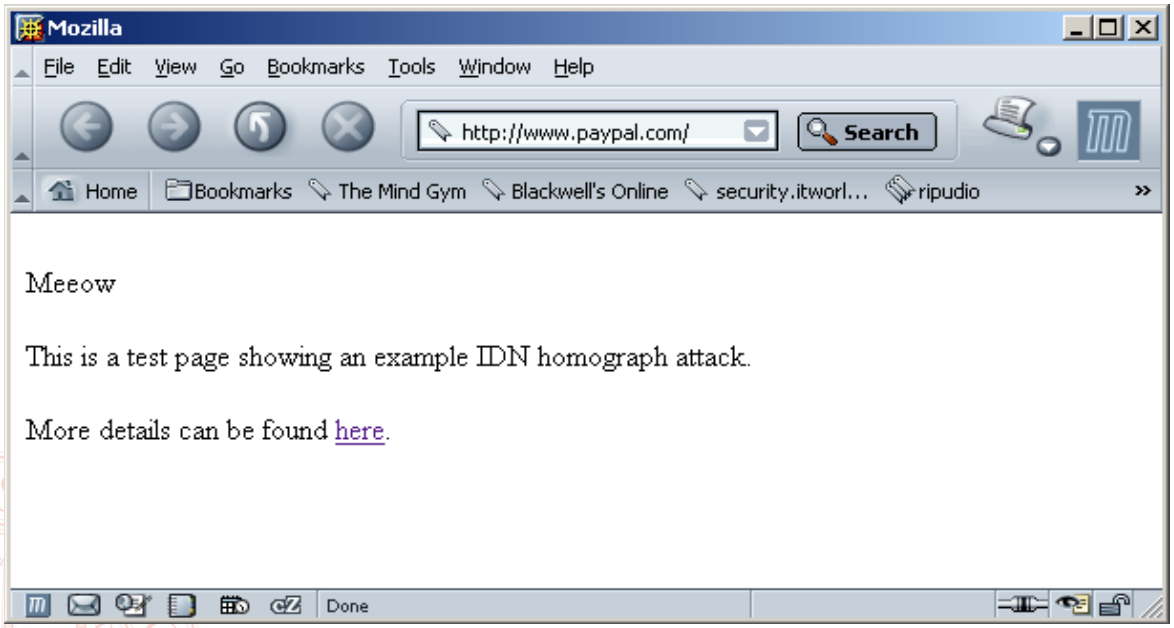
- La parte più complessa di SSL.
- Consente al server ed al client di autenticarsi reciprocamente
  - nelle applicazioni web è comune che il server provi la sua autenticità edntre il client no
- Negozia gli algoritmi e le chiavi per la cifratura ed i controlli di integrità
- Interviene prima che qualsiasi dato sia trasmesso



Occultamento dell'URL

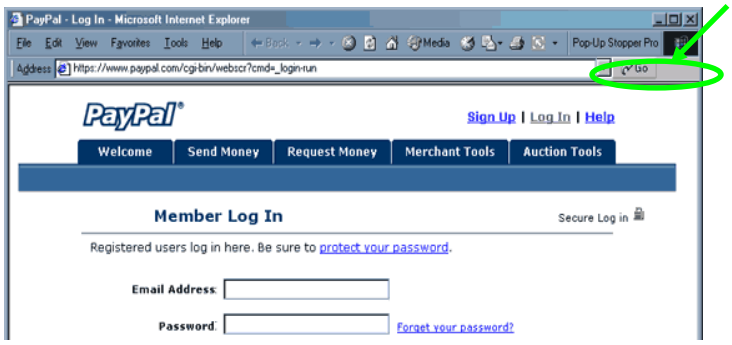
RFC3490/1/2: International Domain Names

ad esempio: http://www.pаypal.com/



Occultamento della barra degli indirizzi

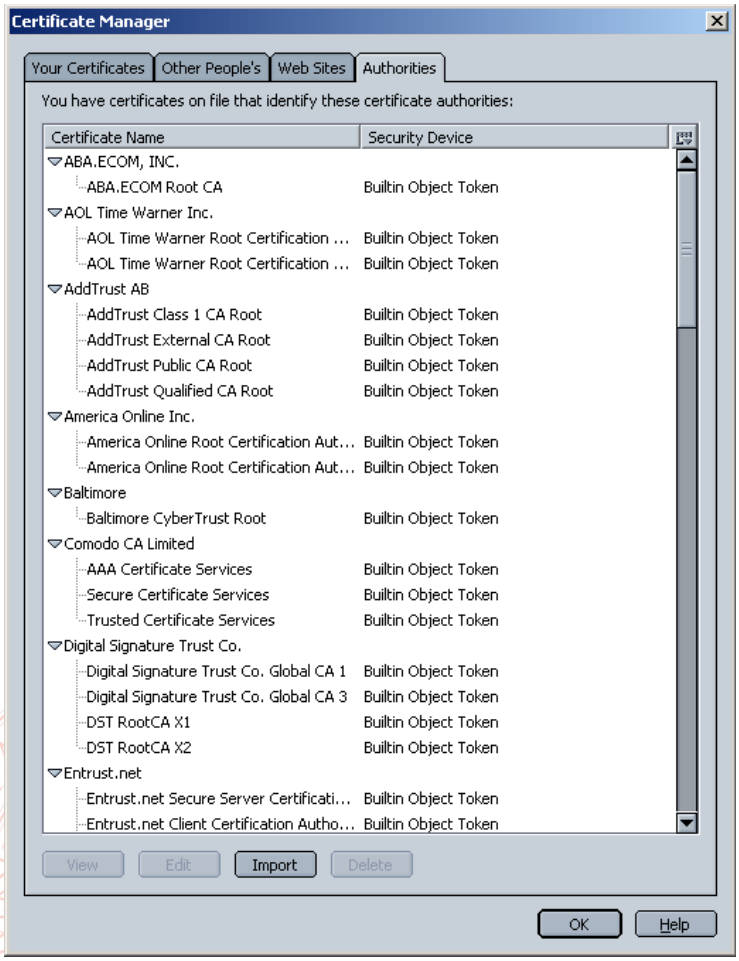
Il vecchio: qualche riga di codice js o activeX

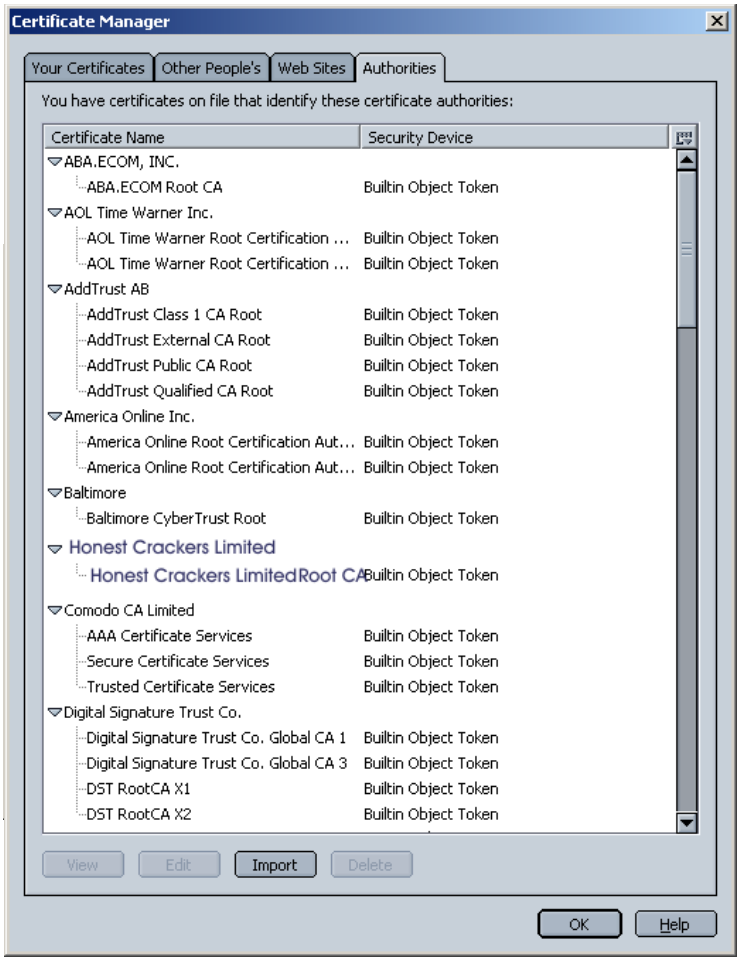


Il nuovo: auto-hiding della barra nei browser mobili

https://jameshfisher.com/2019/04/27/the-inception-bar-a-new-phishing-method/

Iniezione di CA nel certificate store





Vulnerabilità di SSL – a livello di protocollo

- **DROWN (2016) - https://drownattack.com/**
  - Gravi vulnerabilità note nella vecchia versione SSLv2, originata dalle restrizioni imposte dal governo USA all'esportazione di crittografia forte
    - Possibile inviare probe che limitano lo spazio di ricerca delle chiavi a 40 bit
  - Se tale versione è supportata su un server con una certa chiave privata, tutti i server che usano tale chiave sono vulnerabili
  - Impatto: controllo completo, impersonamento del server

- **POODLE (2014)**
  - Un attaccante in grado di posizionarsi *in the middle* (ad esempio contro gli utenti di un hotspot pubblico) può forzare il downgrade delle connessioni verso SSLv3
  - SSLv3 ha varie vulnerabilità sfruttabili
  - Impatto: controllo completo della connessione

Vulnerabilità di SSL – a livello di implementazione

- Heartbleed (2014) - http://heartbleed.com/
  - Implementazione errata della rinegoziazione delle chiavi
  - Consente di leggere pezzi di memoria del sistema target
  - Impatto: possibile leak di materiale sensibile, come le chiavi

Attacchi a livello IP

- IP non può garantire nessuna proprietà di sicurezza ...
  - autenticità
  - integrità
  - riservatezza
- … di nessuna parte del pacchetto
  - header
  - payload

- Esistono varianti che conferiscono queste proprietà, ma richiedono uno stack modificato

IP Hijacking

- Vari modi di *informare internet che la rotta verso una data subnet passa dal proprio AS*, attraverso il protocollo BGP
  - Autorità apparente di annunciare
  - Annuncio spontaneo (nessuno filtra!)
- Usi differenti:
  - Non malevolo: più veloce che chiedere IP al RIR :-)
  - Spamma e fuggi
  - DoS attivo o passivo
  - Impersonare un bersaglio
  - Man In The Middle
- Dirottamenti accidentali avvengono spesso: quindi basse probabilità di essere notati
- Qualche esempio storico disponibile su completewhois.com

Un esempio recente: Youtube & Pakistan Telecom

Dalla presentazione di Pilosov e Kapela a DEFCON16 (Las Vegas 2008)

- YouTube announces 5 prefixes:
- A /19, /20, /22, and two /24s
- The /22 is 208.65.152.0/22
- Pakistan's government decides to block YouTube
- Pakistan Telecom internally nails up a more specific route (208.65.153.0/24) out of YouTube's /22 to null0 (the routers discard interface)
- Somehow redists from static ✉ bgp, then to PCCW
- Upstream provider sends routes to everyone else…
- Most of the net now goes to Pakistan for YouTube, gets nothing!
- YouTube responds by announcing both the /24 and two more specific /25s, with partial success
- PCCW turns off Pakistan Telecom peering two hours later
- 3 to 5 minutes afterward, global bgp table is clean again

Link interessanti:

http://news.cnet.com/8301-10784_3-9878655-7.html

http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

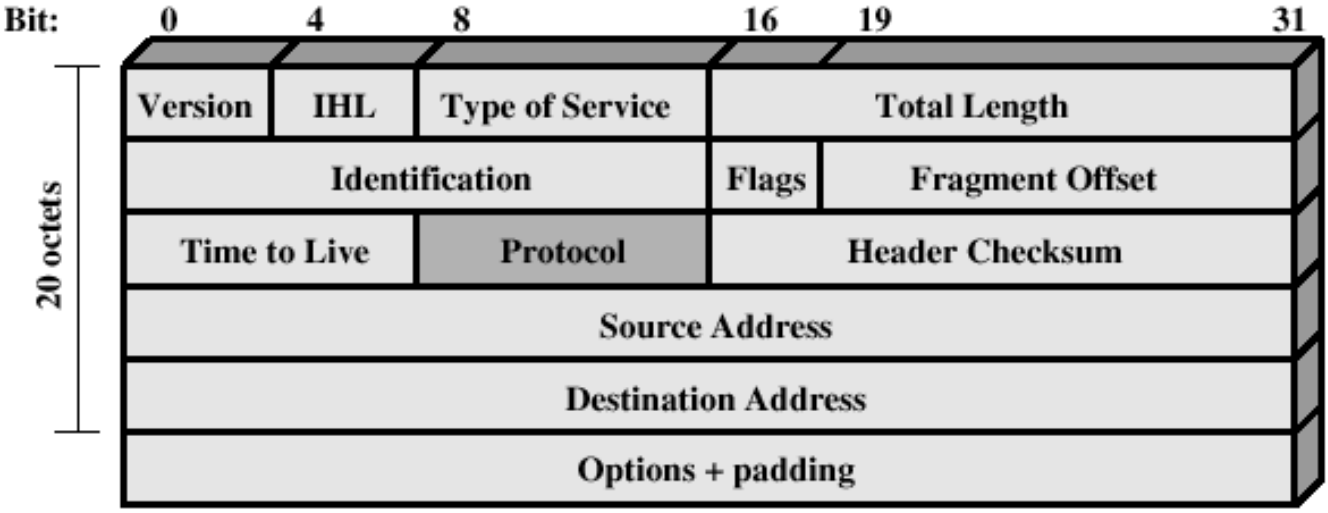
Come risolvere il problema?

- Reagendo:
  - Per avere l'attenzione dei grossi provider upstream possono volerci giorni, se non siete Youtube
- Prevenendo:
  - Filtrando gli annunci sulla base del contenuto (come essere certi della ragionevolezza?)
  - Autenticando i singoli pacchetti: ad esempio con IPSec

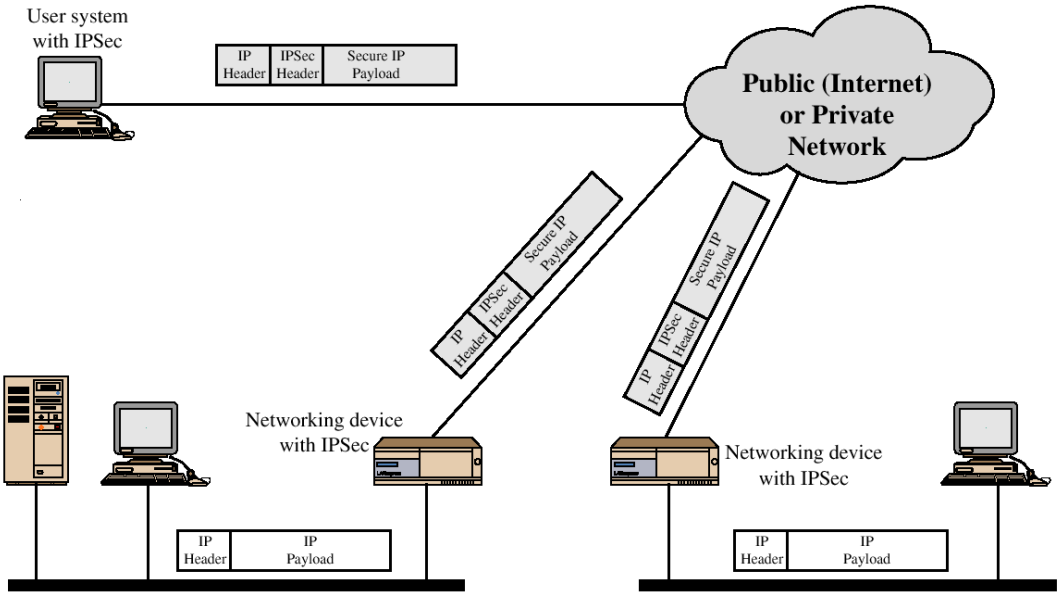
IP Security Overview

- IPSec non è un protocollo singolo
  - set di algoritmi di sicurezza
  - framework per la negoziazione degli algoritmi
  - specifiche per la gestione delle chiavi
- Applicazioni di IPSec
  - Interconnessione di sedi remote attraverso Internet
  - Accesso di client alla rete aziendale attraverso Internet
  - Creazione di reti complesse con criteri di protezione differenziati
- Vantaggi di IPSec
  - Trasparente alle applicazioni
  - Applicabile al traffico infrastrutturale di Internet, come i messaggi che i router si scambiano per aggiornare le tabelle di instradamento

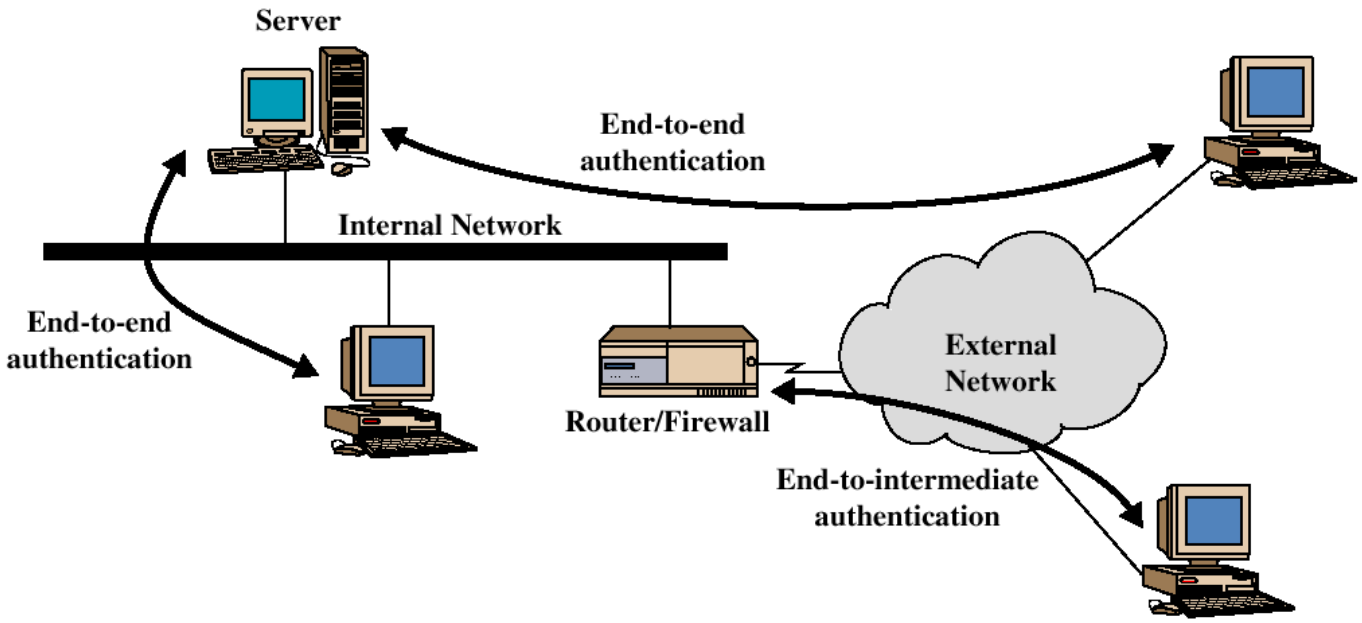
IPv4 Header



IPSec Scenario

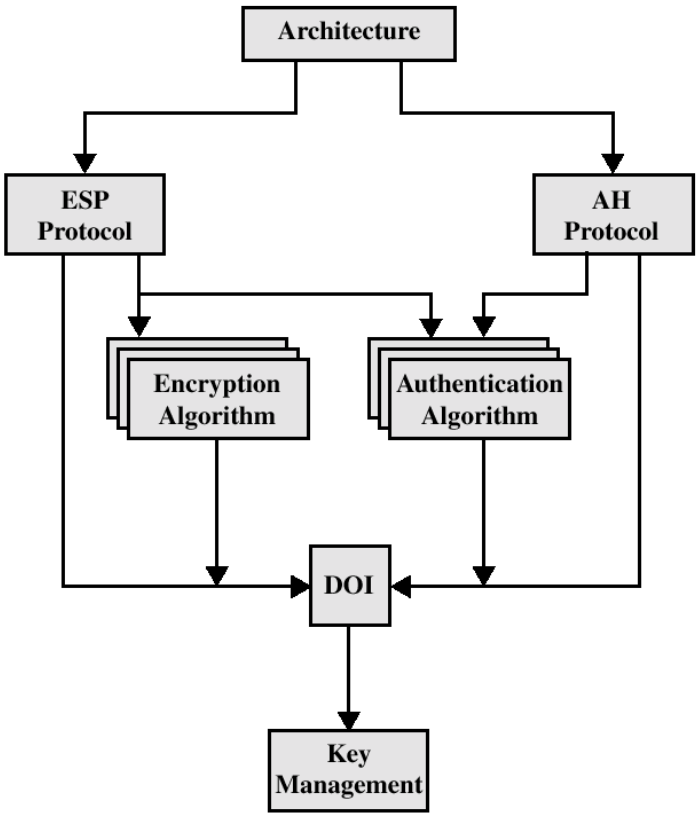


Utilizzo End-to-end / End-to-Intermediate



Gli standard di IPSec

- IPSec documents:
  - RFC 2401: An overview of security architecture
  - RFC 2402: Description of a packet encryption extension to IPv4/IPv6
  - RFC 2406: Description of a packet emcryption extension to IPv4/IPv6
  - RFC 2408: Specification of key managament capabilities



Servizi offerti ed algoritmi utilizzati

- Controllo dell'accesso
- Integrità anche senza connessione
- Autenticazione dell'origine dei dati
- Rilevazione dei replay
- Riservatezza dei dati
- Parziale riservatezza dei flussi di traffico

- Cifratura:
  - Three-key triple DES
  - RC5
  - IDEA
  - Three-key triple IDEA
  - CAST
  - Blowfish
- Autenticazione:
  - HMAC-MD5-96
  - HMAC-SHA-1-96
- Gestione chiavi:
  - Manuale
  - Automatizzata
    - Oakley Key Determination Protocol
    - Internet Security Association and Key Management Protocol (ISAKMP)

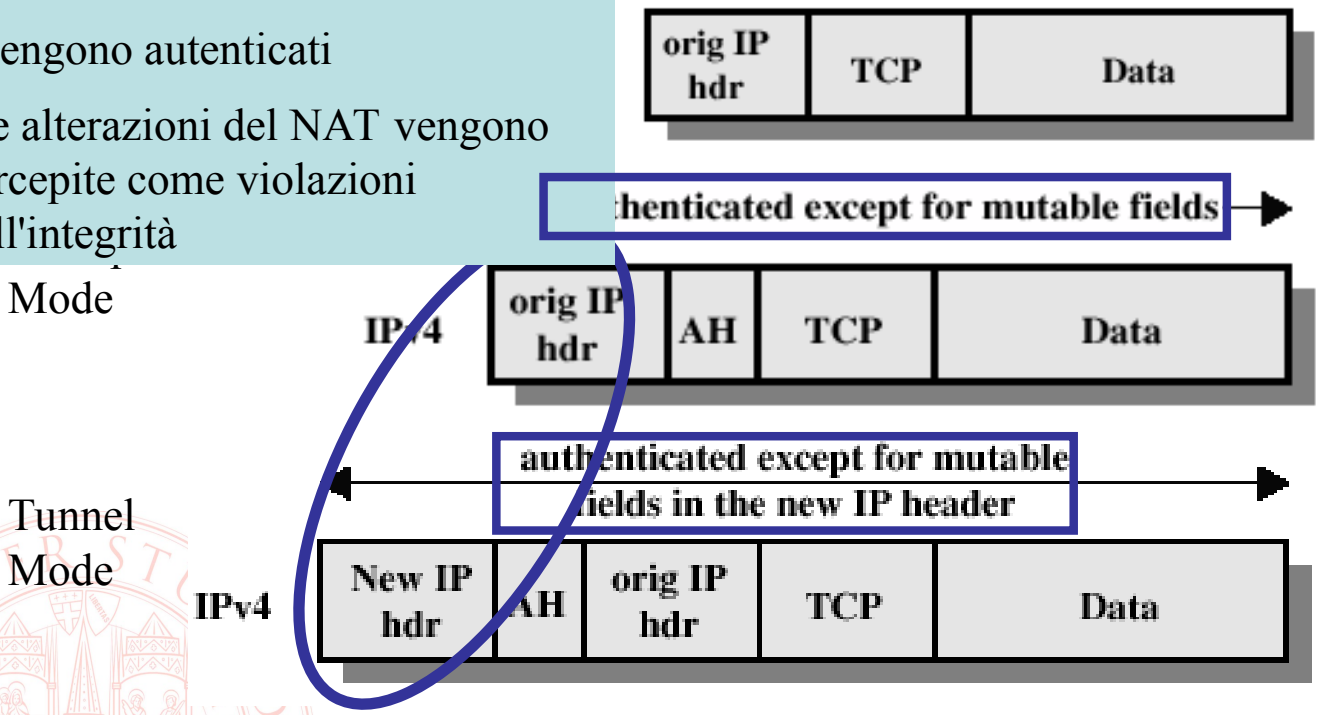
Terminologia di base

- SA (Security Association)
  - relazione unidirezionale tra mittente e destinatario, definita da
    - Security Parameter Index (SPI)
    - IP Destination address
    - Security Protocol Identifier
  - due modalità possibili di SA
    - Transport Mode
    - Tunnel Mode
- Protocolli di sicurezza
  - AH (Authentication Header)
  - ESP (Encapsulating Security Payload)

Autentication Header

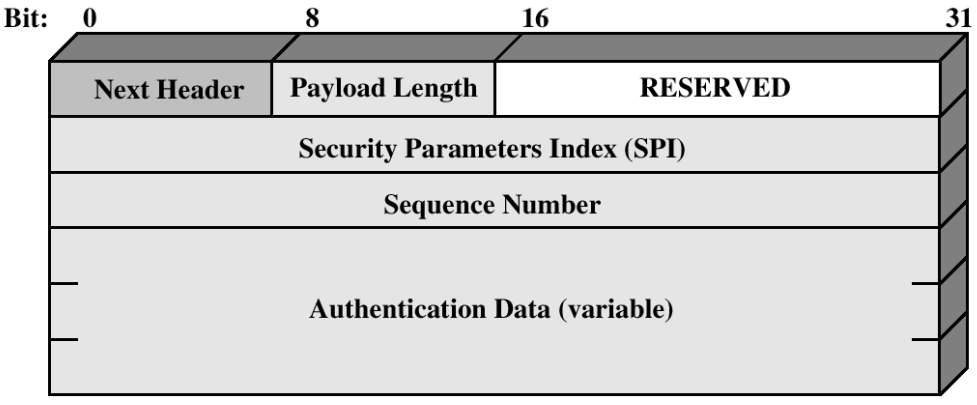
Gli indirizzi, giustamente, non sono considerati campi variabili

- vengono autenticati
- le alterazioni del NAT vengono percepite come violazioni dell'integrità



Authentication Header

- Garantisce l'autenticazione e l'integrità dei pacchetti IP
- Protegge dai replay attacks

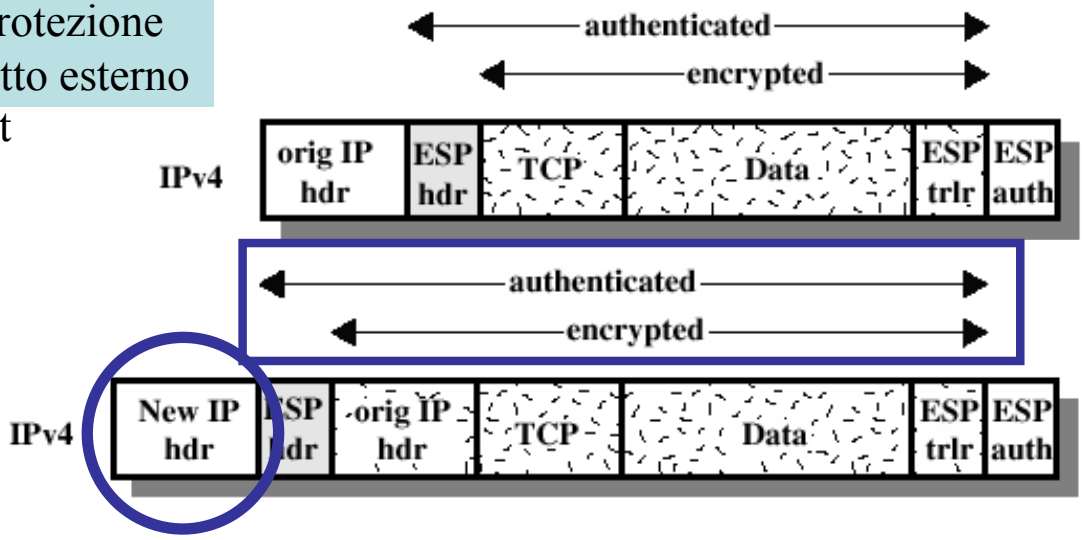


ESP con cifratura ed autenticazione

Nessuna protezione del pacchetto esterno

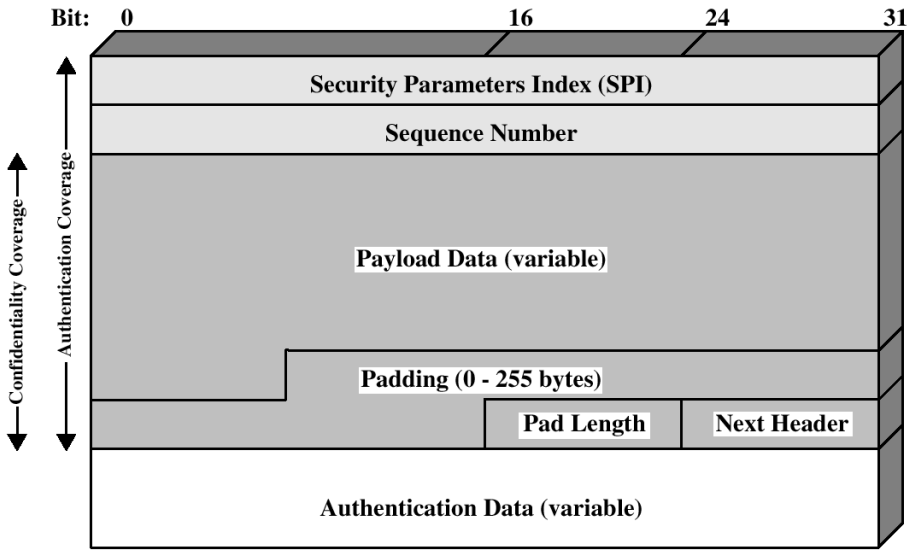
Transport Mode

Tunnel Mode



Encapsulating Security Payload

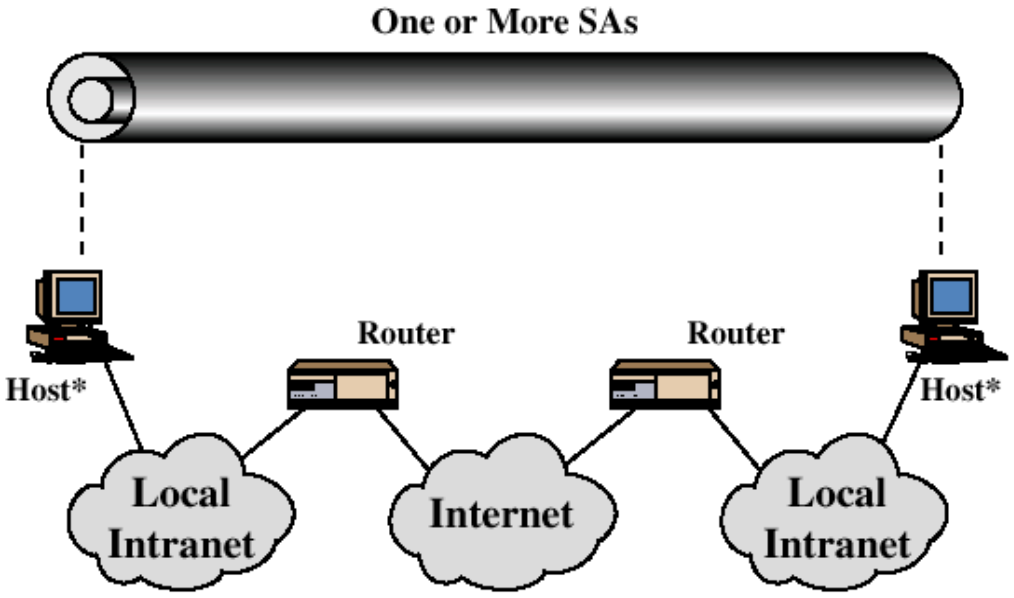
- ESP offre essenzialmente servizi per la riservatezza



Riassunto delle combinazioni dei modi di protezione

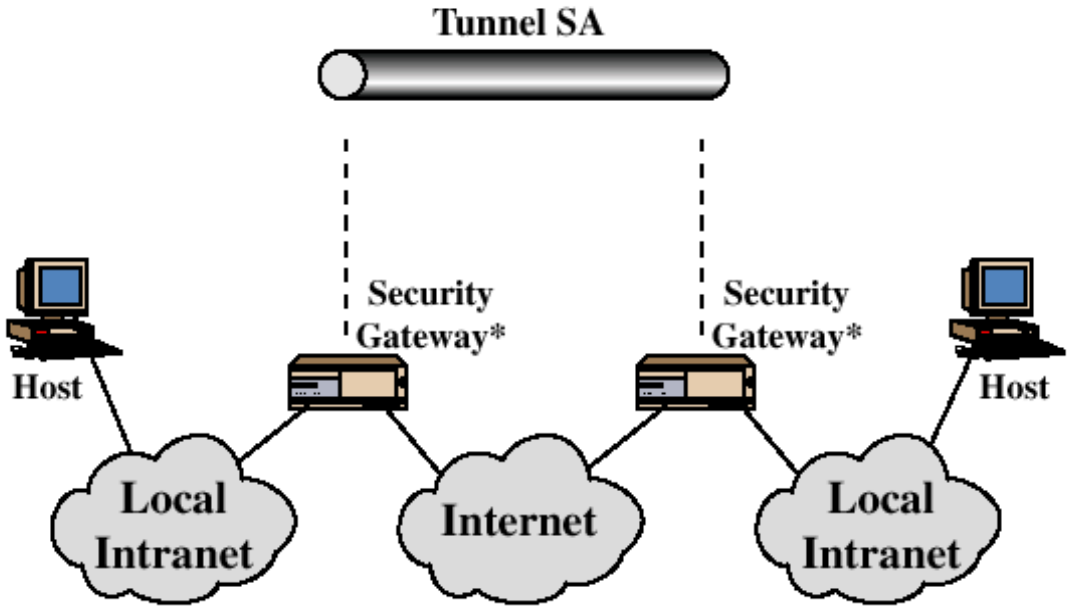
	Transport Mode SA	Tunnel Mode SA
AH	Autentica il payload del pacchetto IP ed alcuni campi dell'header IP	Autentica l'intero pacchetto IP interno ed alcuni campi del pacchetto IP esterno
ESP	Cifra il contenuto del pacchetto	Cifra l'intero pacchetto IP interno
ESP with authentication	Cifra il contenuto del pacchetto. Autentica il payload del pacchetto ma non l'header IP	Cifra ed autentica l'intero pacchetto IP interno.

Combinazione di Security Associations



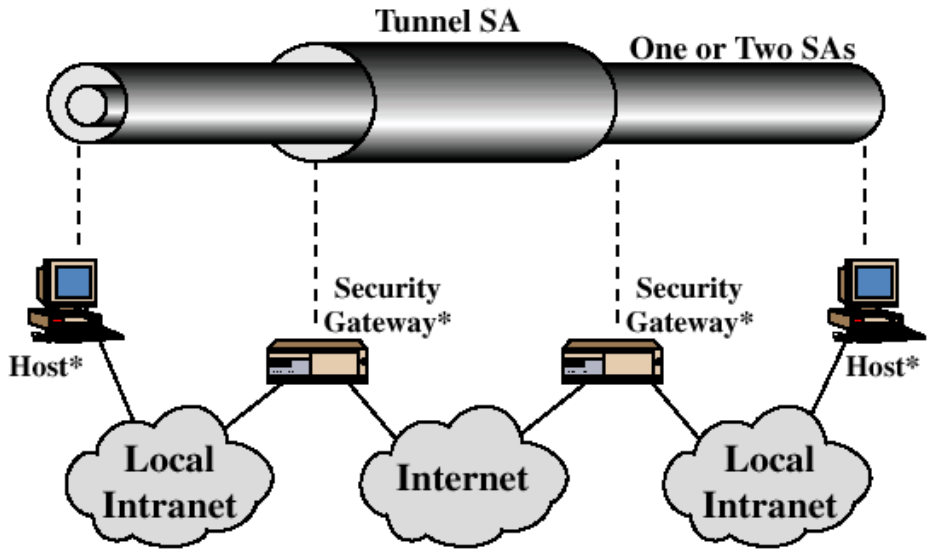
(a) Case 1

Combinazione di Security Associations



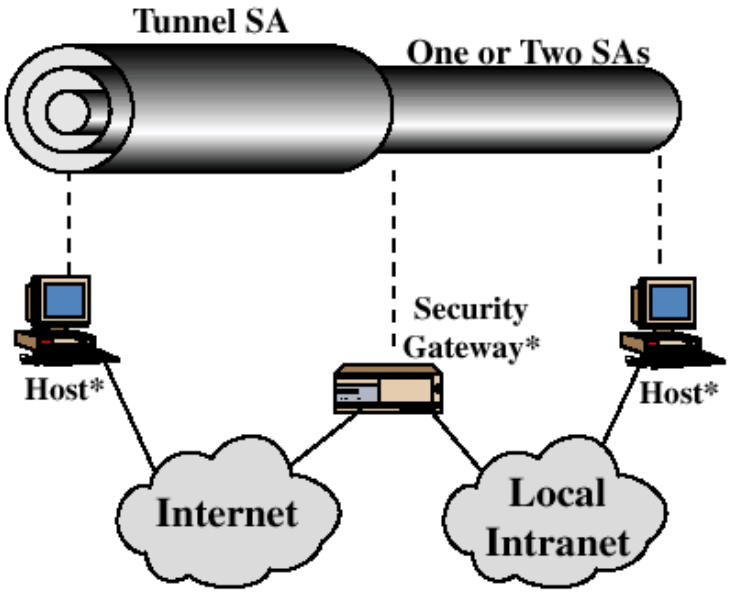
(b) Case 2

Combinazione di Security Associations



(c) Case 3

Combinazione di Security Associations



(d) Case 4

Considerazioni comparative

- SSL/TLS
  - è specifico di un dominio applicativo ☹
  - è semplice e realmente standard ☺
- IPSec
  - è generale e trasparente alle applicazioni ☺
  - è tipicamente implementato nello stack TCP/IP del sistema operativo, con variazioni che rendono difficile l'interoperabilità ☹
- Soluzioni "ibride"
  - utilizzo di varianti di SSL per il trasporto di pacchetti IP analogo al tunnel mode di IPSec
  - implementazione user space, indipendente dal S.O.
    - Es: OpenVPN