Corso di Laboratorio di Telematica – AA. 2002-2003

Franco Pirri, Maria Chiara Pettenati, Claudio Bizzarri, Maurizio Masseti

Lezione 9

Principi di Sicurezza nelle Reti di Telecomunicazioni

Sicurezza: cosa si intende

- Sicurezza Fisica: accesso controllato ai locali, conservazione delle chiavi di accesso alle sale dati, riconoscimento fisico degli utenti ammessi
- Sicurezza Logica: gestione oculata delle passwords, dei diritti di accesso agli utenti
- Sicurezza di Rete: garantire sicurezza nelle comunicazioni in rete, in modo da tutelare l'integrità e la riservatezza dei dati critici e sensibili

Approccio alla sicurezza

- Quali risorse proteggere?

Capire quali sono i processi e le informazioni più “sensibili” alla sicurezza. Identificare le risorse critiche.

- Da chi proteggerle?

Cercare di individuare i possibili attori dell’attacco: interno o esterno?

- Da cosa proteggerle?

Cercare di prevenire le più comuni modalità di attacchi

- Sensibilizzazione del personale, a tutti i livelli!

Sicurezza Fisica

- Uso di badge, smart card, dispositivi biometrici

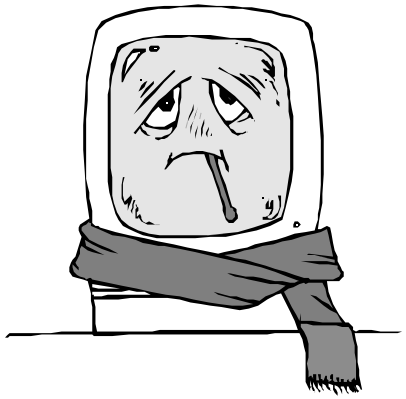
Sicurezza Logica

- Passwords di minimo 6 caratteri
- Almeno 13,14 caratteri, misti con maiuscole e minuscole, NO da dizionario (10 caratteri ~ 1 week con un Pentium)
- Caratteri maiuscoli e minuscoli, con numeri
- Diritti di administrator (root) sui server e sui router ben tutelati
- No passwords con post-it sul monitor!!!!

Sicurezza e pila TCP/IP

- Sicurezza al livello fisico: evitare buchi nel sistema a livello di LAN (modem portato da casa, sniffer su hub!)
- Sicurezza al livello IP: controllare, classificare e filtrare il traffico in base alle informazioni contenute nel pacchetto IP, rendere sicuro lo strato Network
- Sicurezza al livello TCP/UDP: filtrare in base alle applicazioni (port number), rendere sicuro il socket
- Sicurezza al livello Applicativo: content-based filtering, autenticazione degli utenti, e-mail sicure

Principali Attacchi Informatici



- Malicious code: Virus, Worms e Trojan Horse
- Sniffing
- Spoofing IP: sostituzione/mascheramento ind. IP
- Denial of Service, Theft of Service (si ruba QoS!!! Modificando DSCP)
- Smurf: echo ICMP forzati (consumo di banda)
- SYN flooding: sessioni TCP aperte a crescere (consumo risorse server)
- TCP ACK Storm
- Buffer overflow: Ping of Death (Ping di >65KB anziché 64 B), crash del server
- Man in the middle
- TCP sequence number guessing per entrare nella connessione 3-way
- Social engineering (chiamare qualcuno-per telefono!- facendo finta di essere dell'azienda, citando codici, passwords, etc)

Malicious code

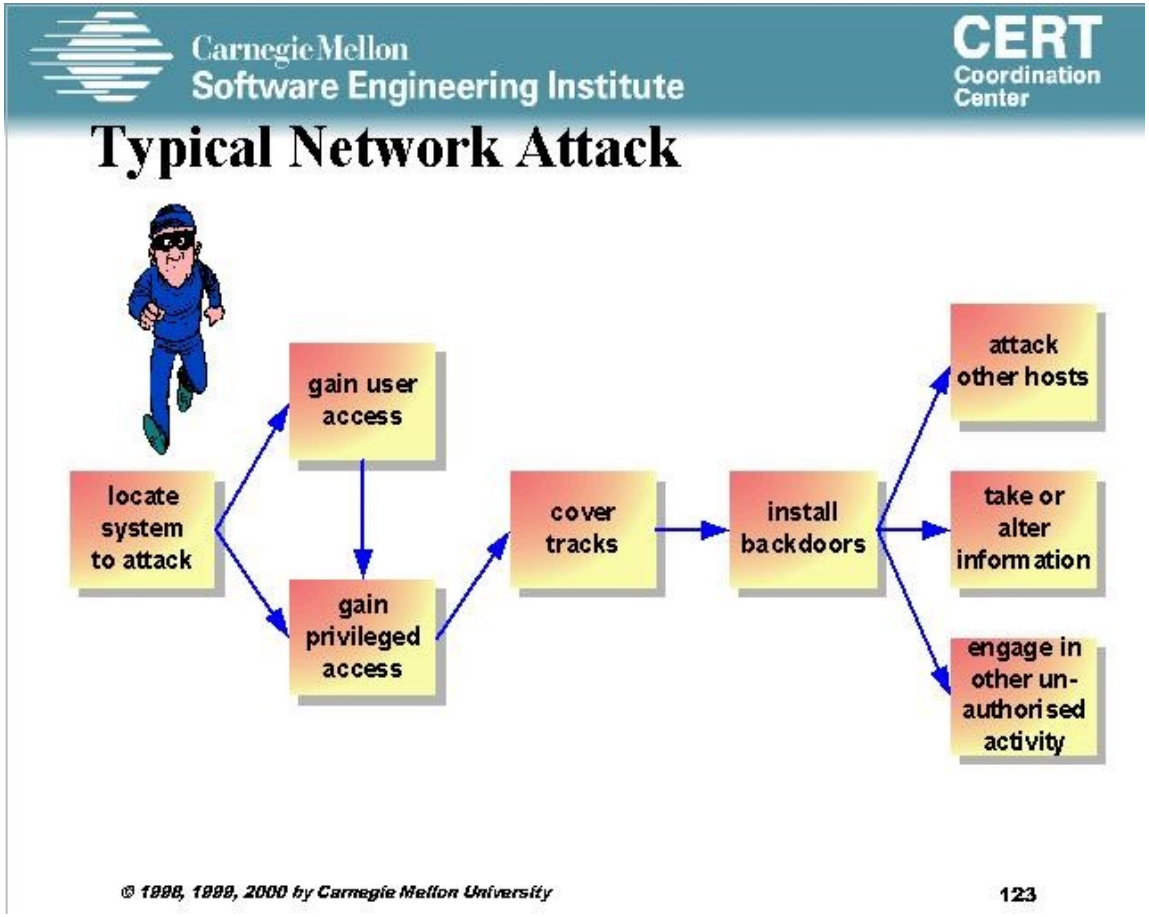
- **Virus**: ha bisogno di un host (es. un file), non si diffonde automaticamente
- **Worm**: arrivato sul pc si diffonde e riproduce da solo, si propaga molto più rapidamente
- **Trojan Horse**: si installa nel PC come software qualunque e poi si esegue in modo indipendente, anche ricollegandosi alla Rete autonomamente.
- Modifica lenta dei file (rovina anche i backup di un anno fa!!!) es. aumenta del 0.001% al giorno previsioni di mercato di un'azienda su foglio excel!!!!
- Back Orifice: Trojan Horse di tipo client/server, è un remote administration tool, dà privilegi "system admin" sull'host attaccato, può arrivare con dei file in vari modi (attivo dal 1998, W95 e 98)

Virus e Sistemi Operativi

- 1986 – 2001: Microsoft: ~60.000 virus
- Linux: 25!
- MAC: 50
- Palm OS: 1
- Windows CE: al 2001 nessun virus!
- Allarme: virus via SMS, su palmari, cellulari UMTS!!!

Dati di F-secure, Roma, Giugno 2001

Attacco di Rete



·**CERT** (COMPUTER EMERGENCY RESPONSE TEAM) : dicembre del 1988 dalla DARPA

Attacco di rete (2)

1. Footprinting: ricerca di informazioni
2. Ricerca di eventuali firewall
3. Ricerca/guessing del Sistema Operativo
4. Sfruttamento dei bugs, per:
    1. Denial of Service
    2. Installazione backdoors
    3. Attaccare altri hosts

Il Footprinting

Raccolta di informazioni sull'host da attaccare:

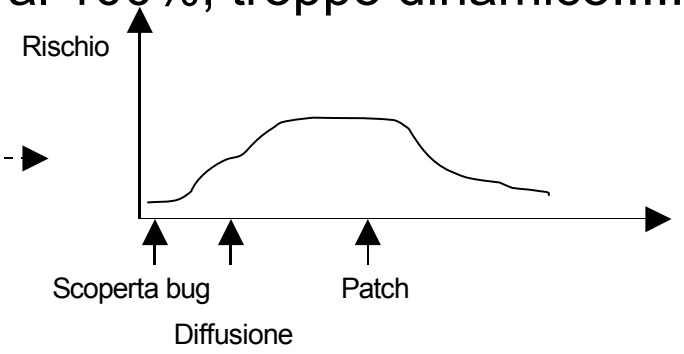
- Range di indirizzi IP
- E-mail dell'amministratore (social engineering!)
- Ping sugli indirizzi IP, per vedere le macchine attive
- Port Scanning per vedere i servizi attivi
- Guessing del sistema operativo

Le patches

Dati di Intrinsic SpA, Giugno 2001

2. Buffer overflow: su server DNS di BIND 4.9.7: rilasciato nel 1999, nel 2001 si è trovato un bug di buffer overflow su 4 linee di codice (4 su 30.000 di programma!), syslog del 1995
3. Gli hacker mandano in overflow il buffer del programma e attaccano il codice
4. 2.5 bug su OS a settimana
5. Applicare le patches 2 volte a settimana!!!!!!!!
6. O non si fa nulla e si reinstalla tutto ogni volta!
7. Nessun sistema è sicuro al 100%, troppo dinamico!!!!! → analisi del rischio e prevenzione

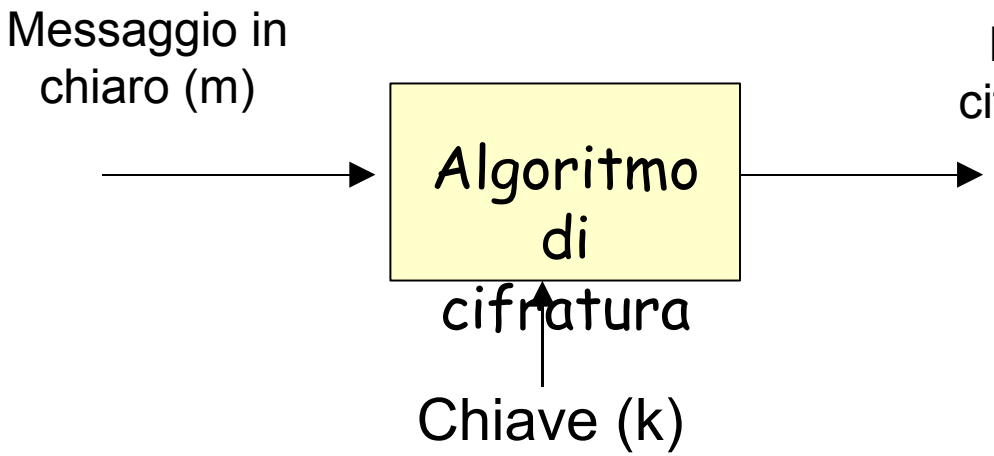
Window of exposure di un bug



Architettura per la Sicurezza

Servizi	**Soluzioni**
• Autenticazione	• Crittografia
• Controllo degli accessi	• Liste di Accesso
• Riservatezza	• Crittografia
• Integrità	• Crittografia
• Non ripudio	• Crittografia

Principi di Crittografia



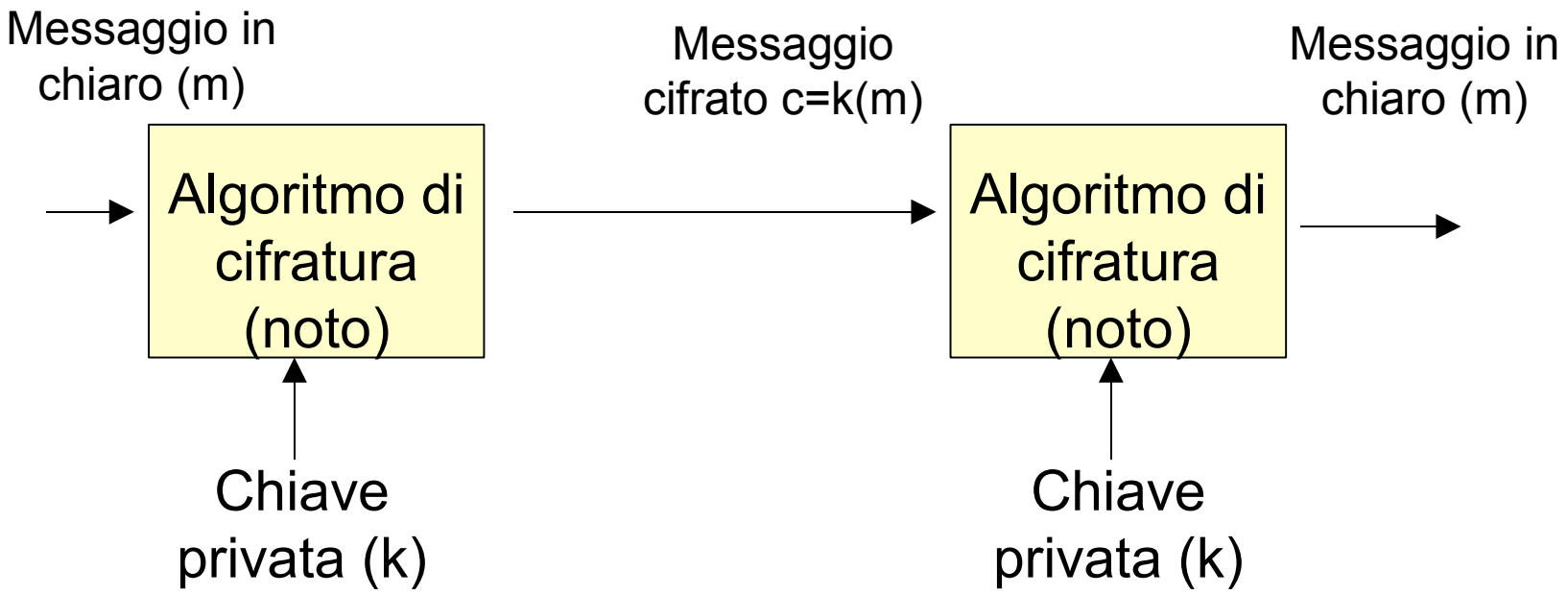
Possibili algoritmi di cifratura:

- elevamento a potenza del messaggio in chiaro, dove la chiave è inclusa nella potenza

- shift ciclico del messaggio in chiaro di un numero di posizioni dipendente dalla chiave

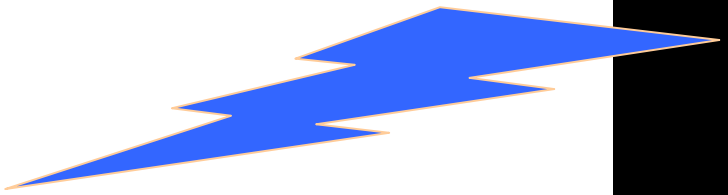
- scrambling del messaggio in chiaro con algoritmi dipendenti dalla chiave

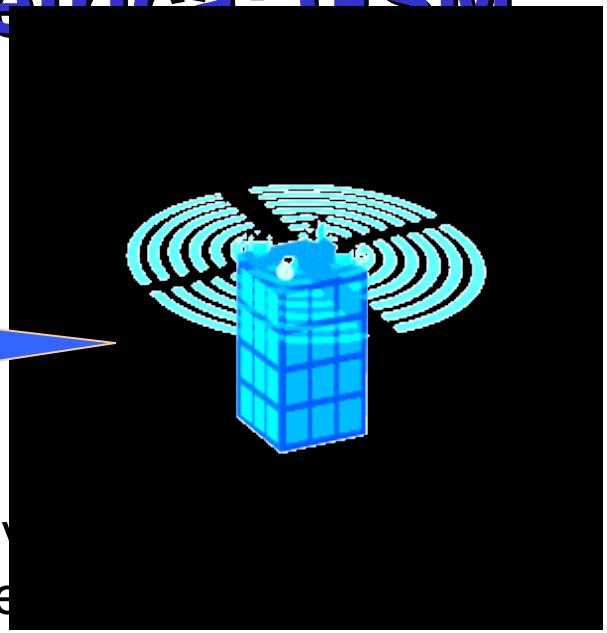
Cifratura a Chiave Simmetrica



- Semplice, veloce
- Tutto si incentra sulla sicurezza e sulla riservatezza della chiave!

Esempio di chiave simmetrica: GSM

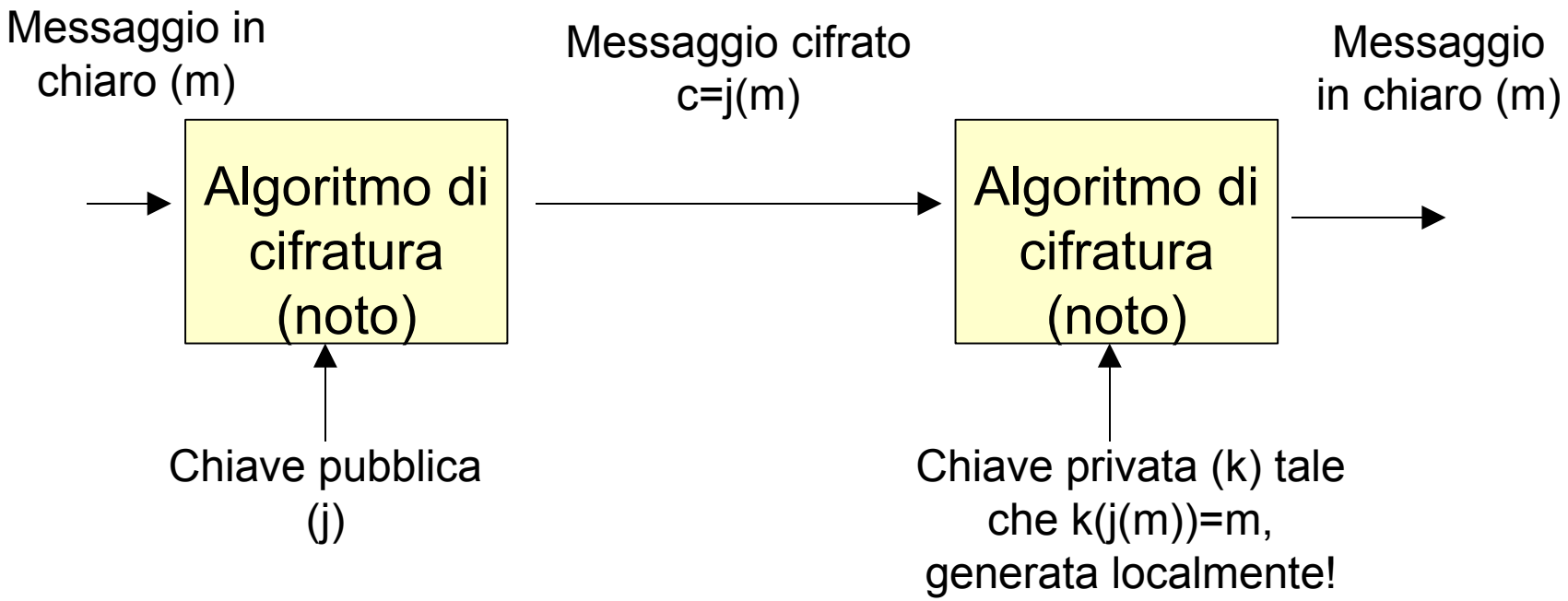




Chiav
conte
Location Register della rete GSM

Chiave simmetrica di 128 bit, contenuta nella SIM card

Cifratura a Chiave Asimmetrica



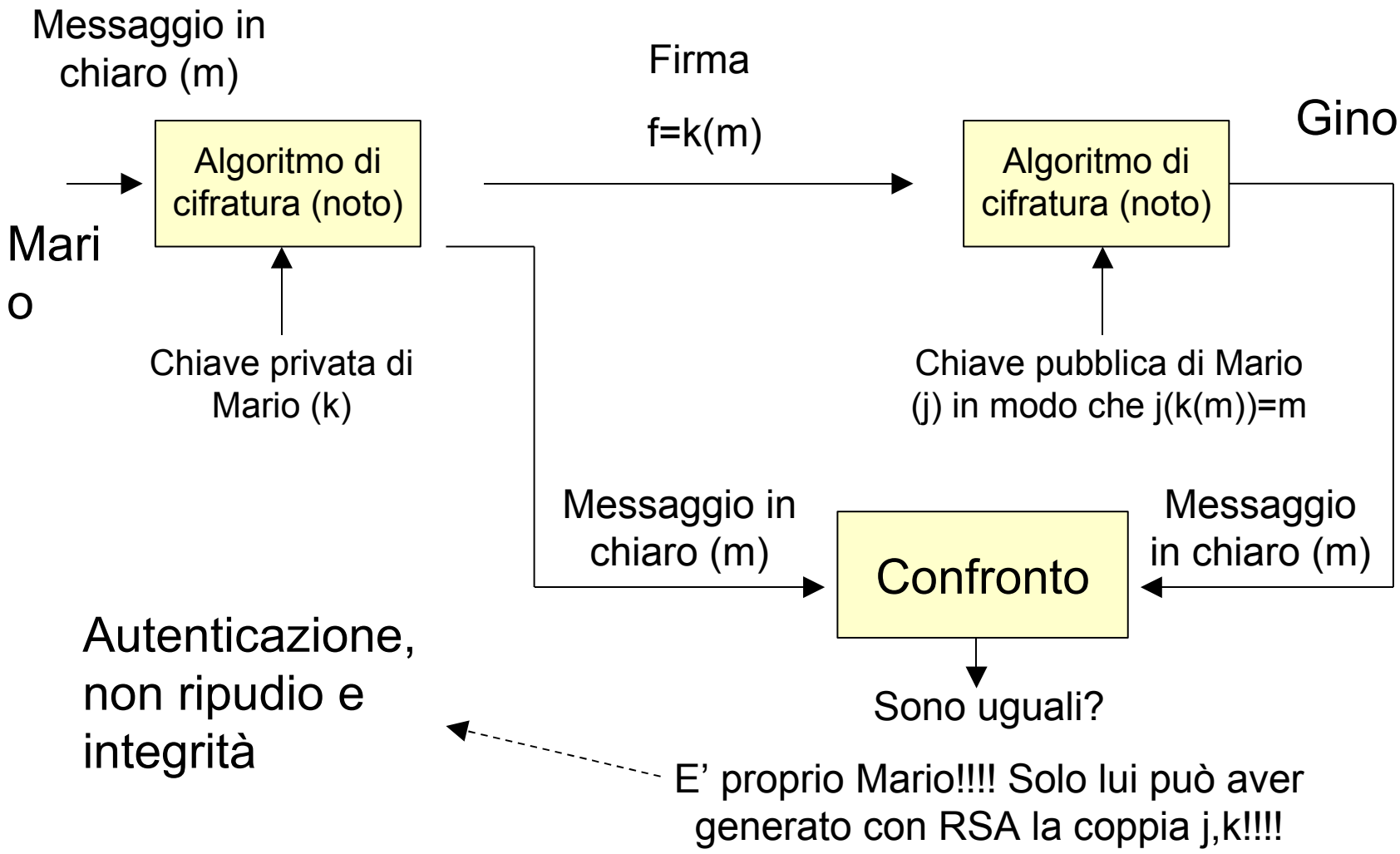
- In realtà vale anche j(k(m))=m!! (firma elettronica!)
- Molto lenta! Elevamento a potenza: 1024 bit →max 7,4 Kbit/s !!!
- Più sicura su reti pubbliche → Internet!
- Sicurezza: non esistono algor conosciuti per la fattorizzazione veloce di un numero

Cifratura Simmetrica/Asimmetrica

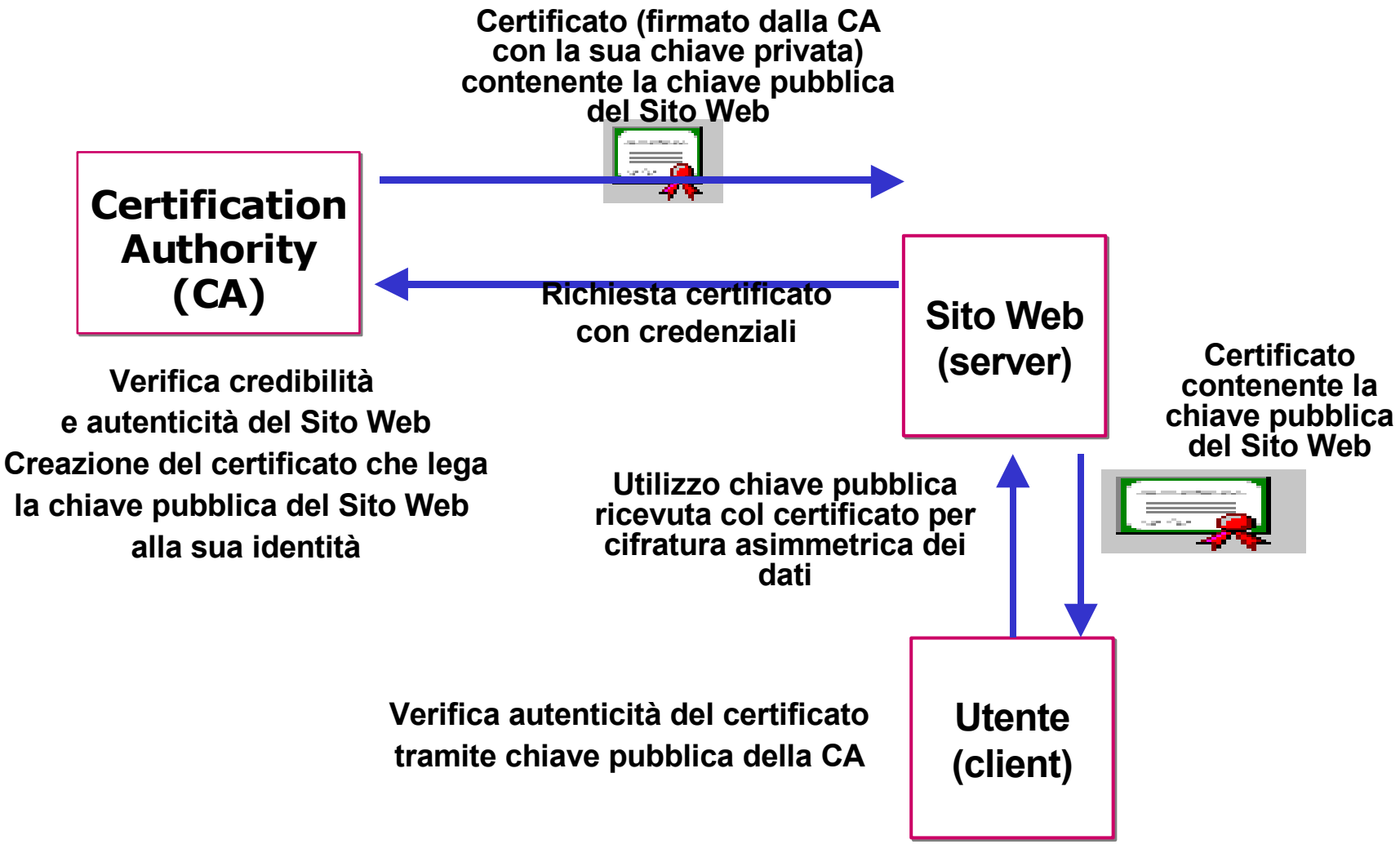
- ✓Cifratura simmetrica: veloce ma poco sicura su reti pubbliche per lo scambio della chiave
- ✓Cifratura asimmetrica: lenta ma sicura su reti pubbliche

- ➢Fase iniziale: scambio della chiave privata (di sessione) con cifratura asimmetrica (RSA)
- ➢Fase operativa di trasmissione dati: la chiave di sessione è stata consegnata con sicurezza, si può cifrare in modo simmetrico (DES) con la chiave di sessione, più veloce!

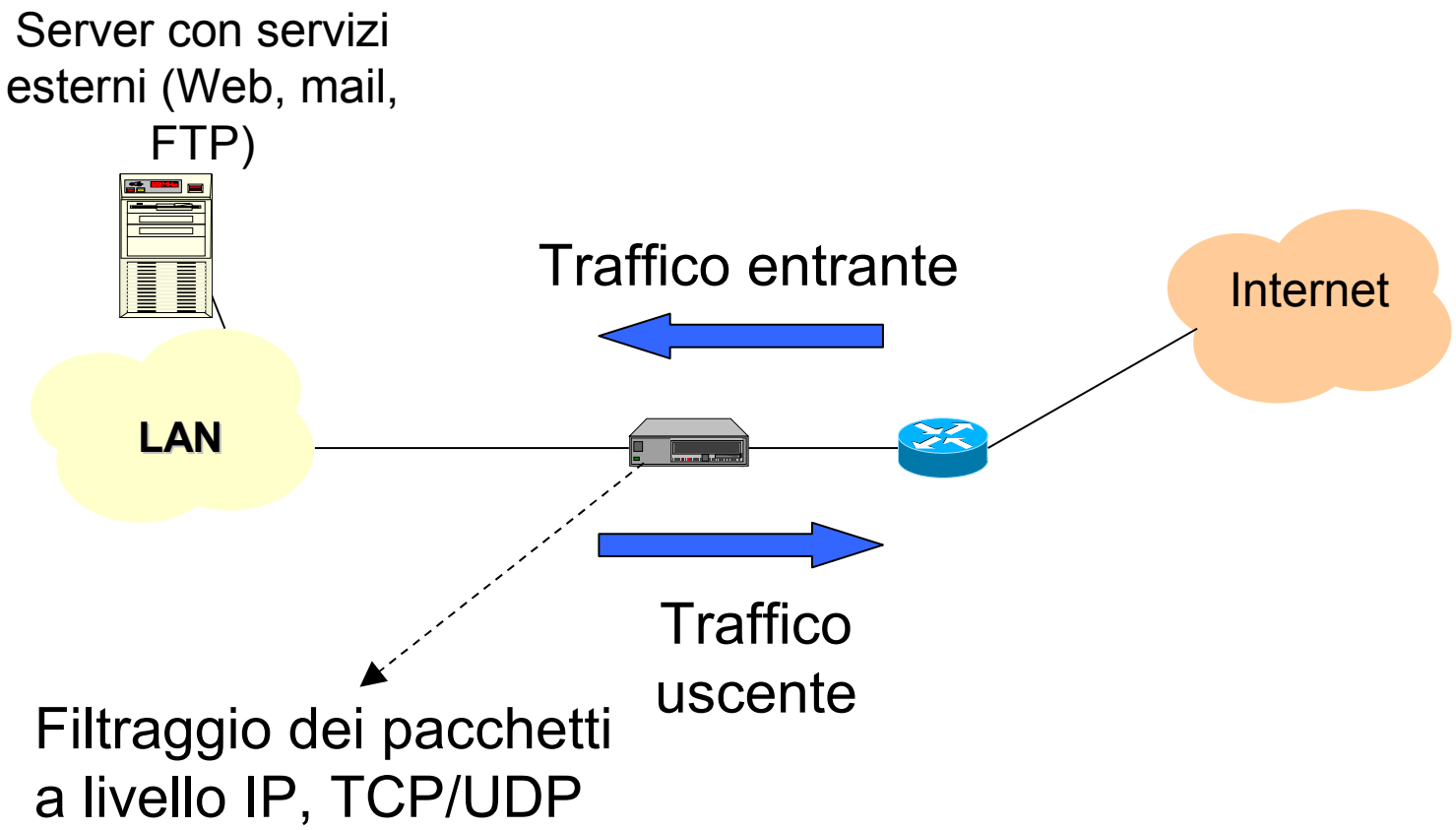
Firma Elettronica



Certificato Digitale - CA



Controllo degli accessi: Packet Filtering



ACL

Liste di Accesso (Access List) sui dispositivi di rete:

Es:voglio far passare SOLO Web da fuori verso il Server Web:

Access-list 101 permit ip 0.0.0.0 241.23.12.1 eq 80

Access-list 101 deny all

Problema: non funziona!!! (ACK del TCP vanno da server verso client!!!)

E' molto difficile capire e decidere cosa far passare e cosa no!

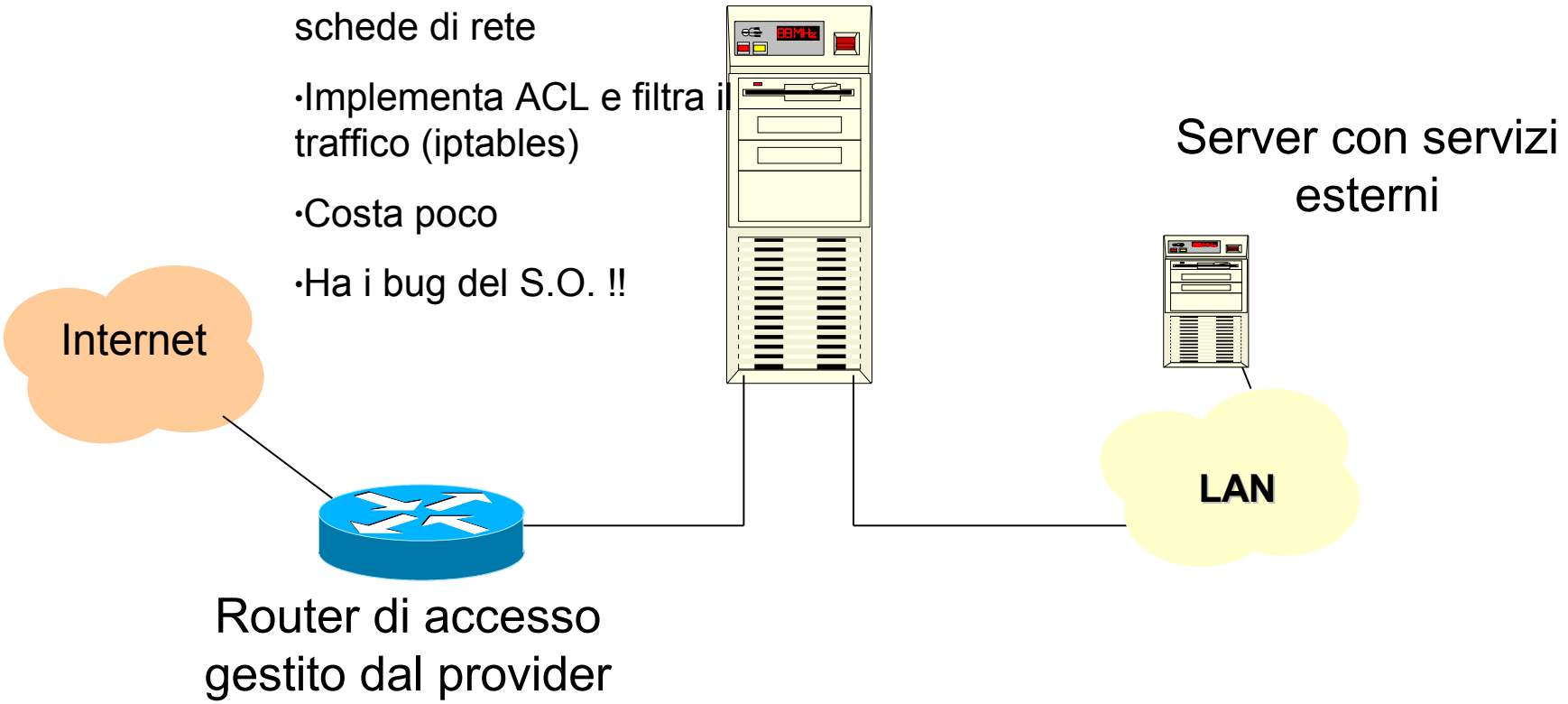
(es: il capo vuol far accedere il figlio a Internet tramite la rete aziendale da casa!!!, il capo vuol accedere al server via FTP (pwd in chiaro!!) da casa!)

Il Firewall

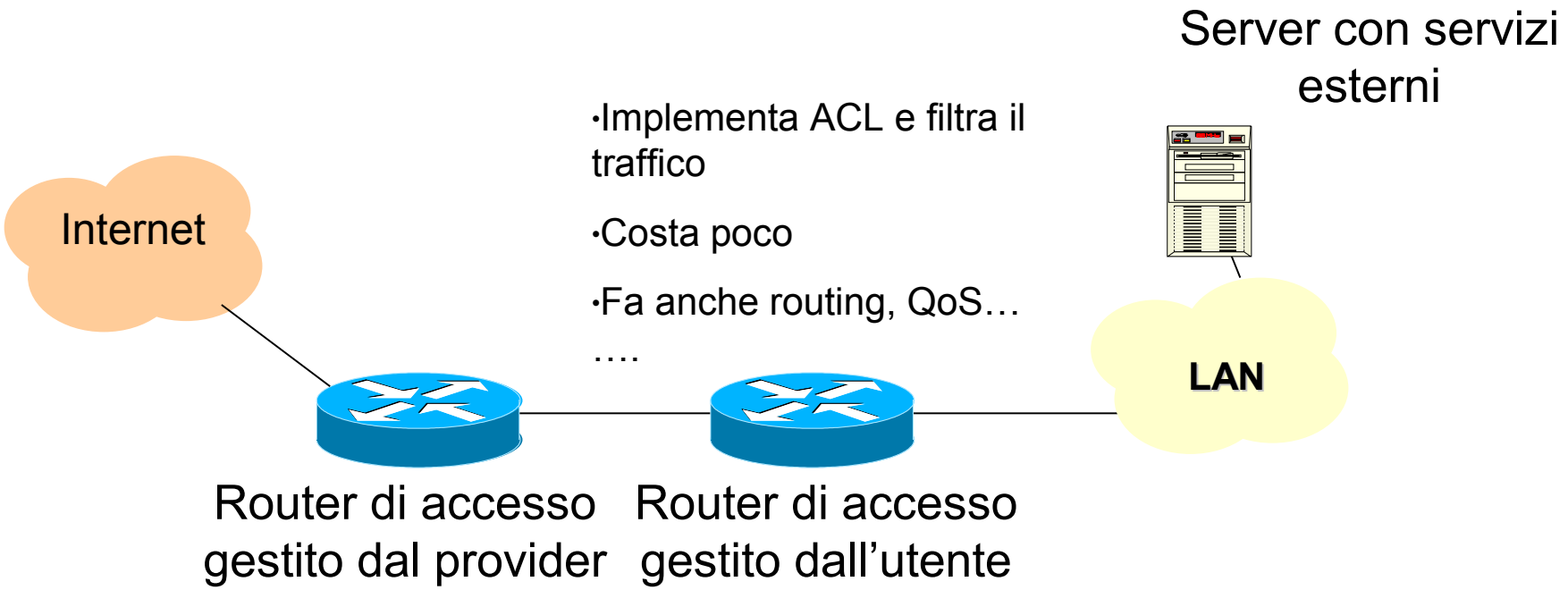
- E’ un dispositivo di rete che filtra i pacchetti entranti e uscenti dalla rete in base a determinate politiche di sicurezza.
- A differenza di un semplice packet filter, un firewall è un gateway che può lavorare fino al livello 7 OSI.
- Lavora con lo stesso principio dei packet filter
- Si basa sulle Liste di Accesso - ACL

Implementazione di Firewall (1)

- Macchina Linux con due schede di rete
- Implementa ACL e filtra il traffico (iptables)
- Costa poco
- Ha i bug del S.O. !!

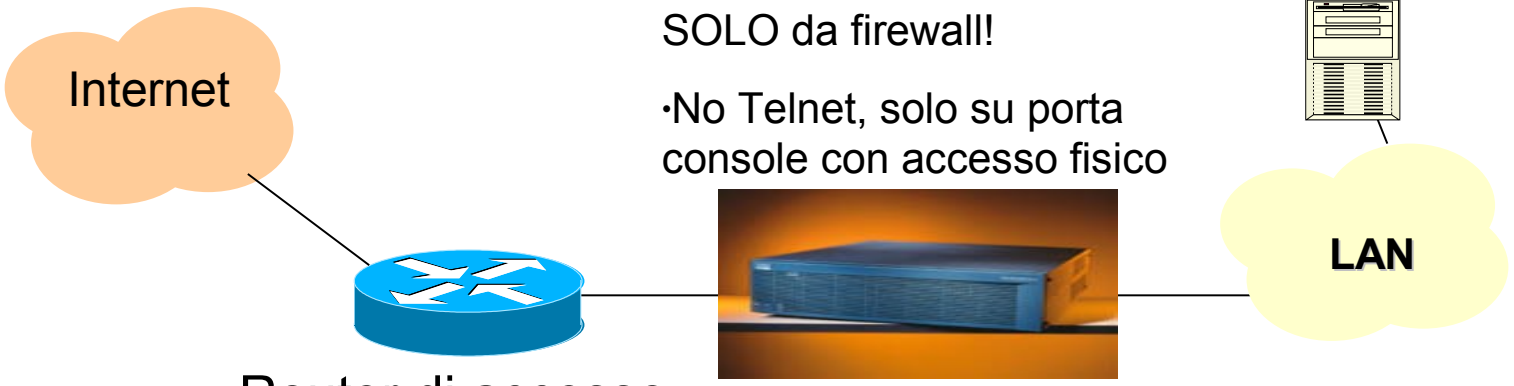


Implementazione di Firewall (2)



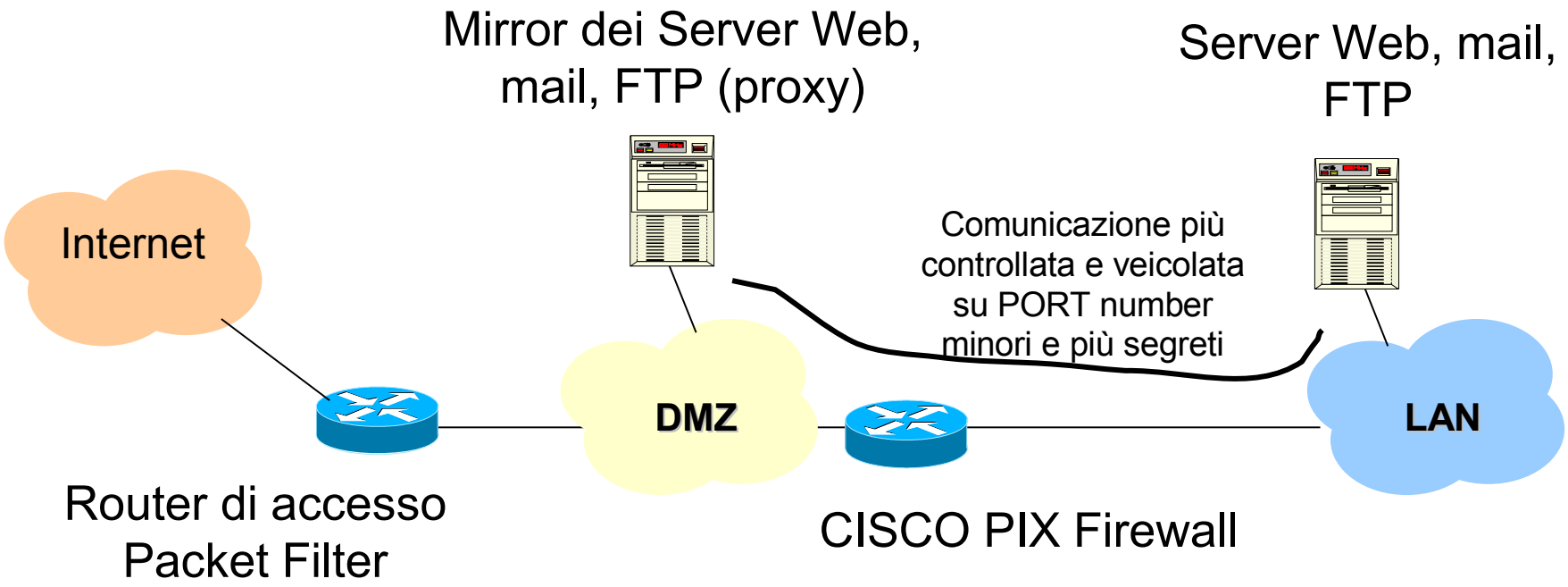
Implementazione di Firewall (3)

- Firewall hardware che implementa ACL e filtra il traffico
- Più costoso
- E' in realtà un router, ma fa SOLO da firewall!
- No Telnet, solo su porta console con accesso fisico



DMZ

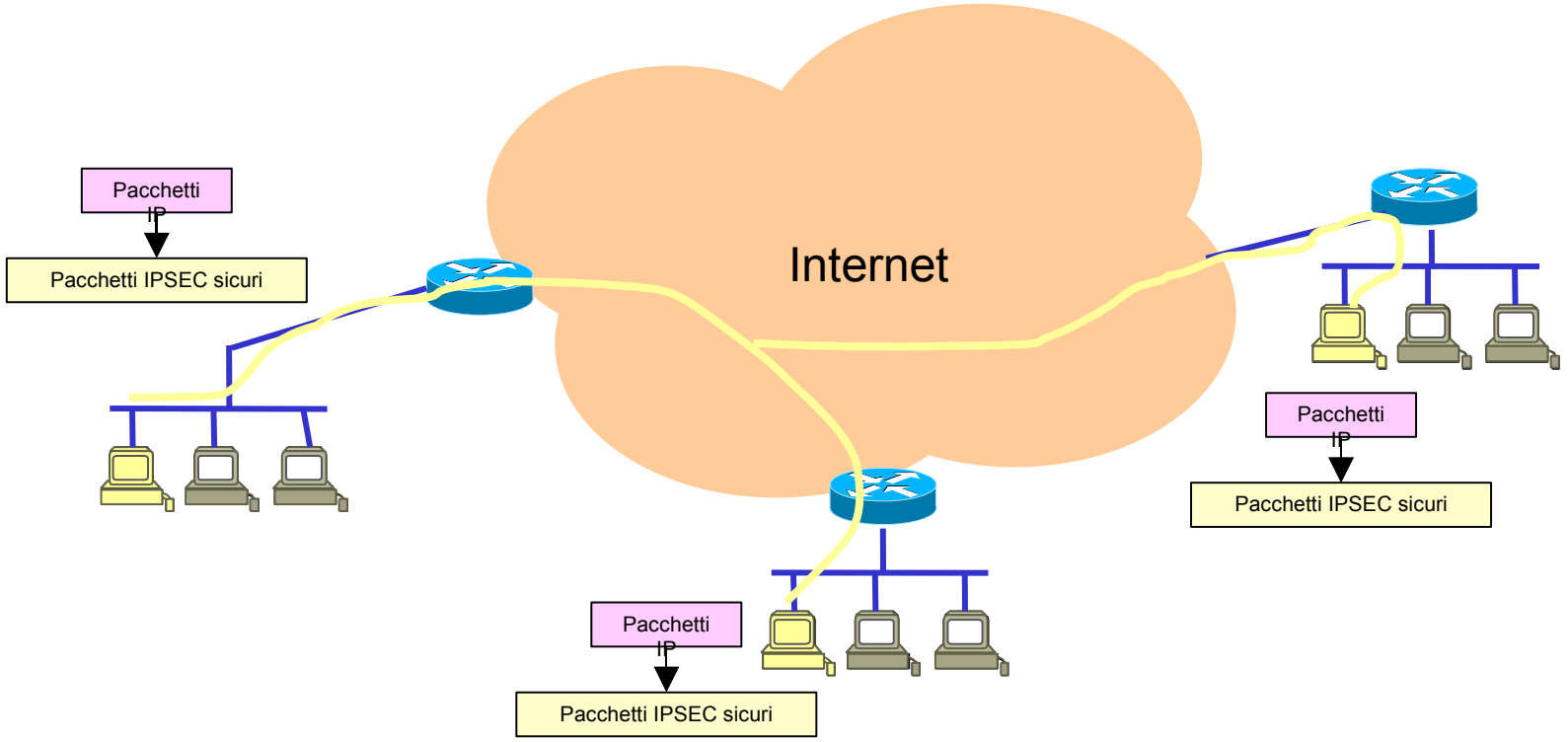
De-Militarized Zone: zona a sicurezza intermedia fra rete interna e Internet



Sicurezza a livello IP: IPSEC

- Offre cifratura e autenticazione end2end operando a livello IP
- Definisce:
  - ✓protocolli: **Authentication Header**, **Encapsulating Security Payload**
  - ✓**Security Associations**: associazioni di sicurezza fra hosts (simile al flow-state di IntServ!!)
  - ✓**Internet Key Exchange**: metodo di distribuzione delle chiavi
  - ✓**Transport e Tunnel mode**: modalità di trasporto, si imbusta e si cifra solo il payload (transport), o tutto il pacchetto IP (tunnel)

Virtual Private Networks



Emulazione di una LAN privata su Internet pubblica

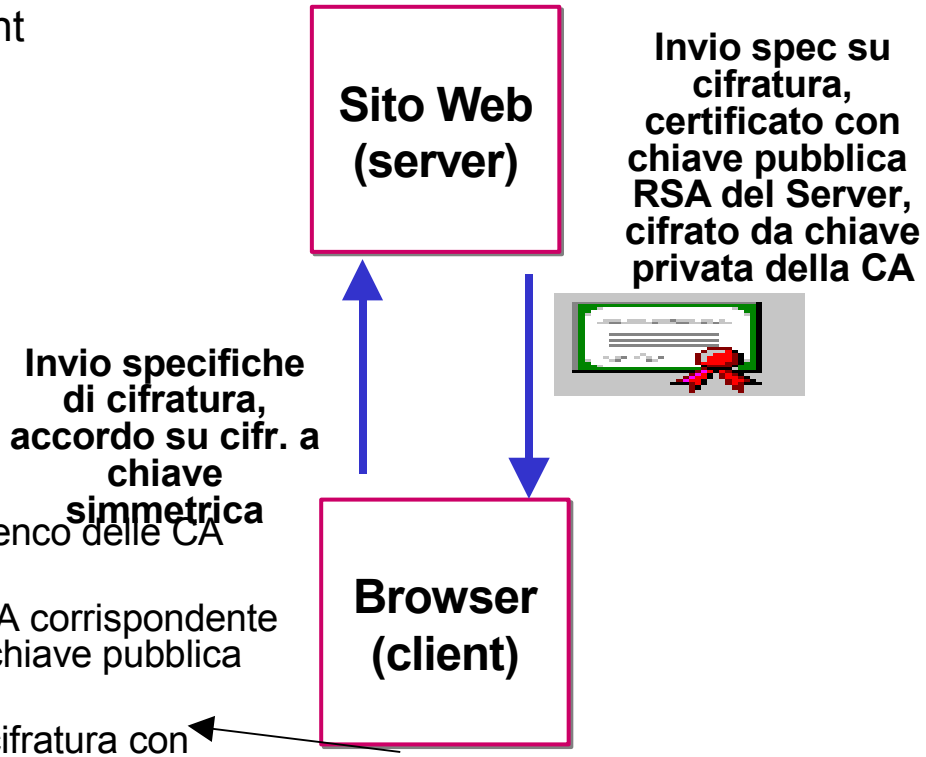
Sicurezza a livello Transport: SSL

- Secure Socket Layer: sviluppato da Netscape Communication, molto usato per e-commerce sicuro
- Sostituisce l'interfaccia socket (fra TCP e le applicazioni) rendendola sicura
- Individuato da URL del tipo https://….(port 443)

- Fornisce: Riservatezza, Integrità e Autenticazione (soprattutto del server verso il client)
- SSL Handshake Protocol e SSL Record Protocol

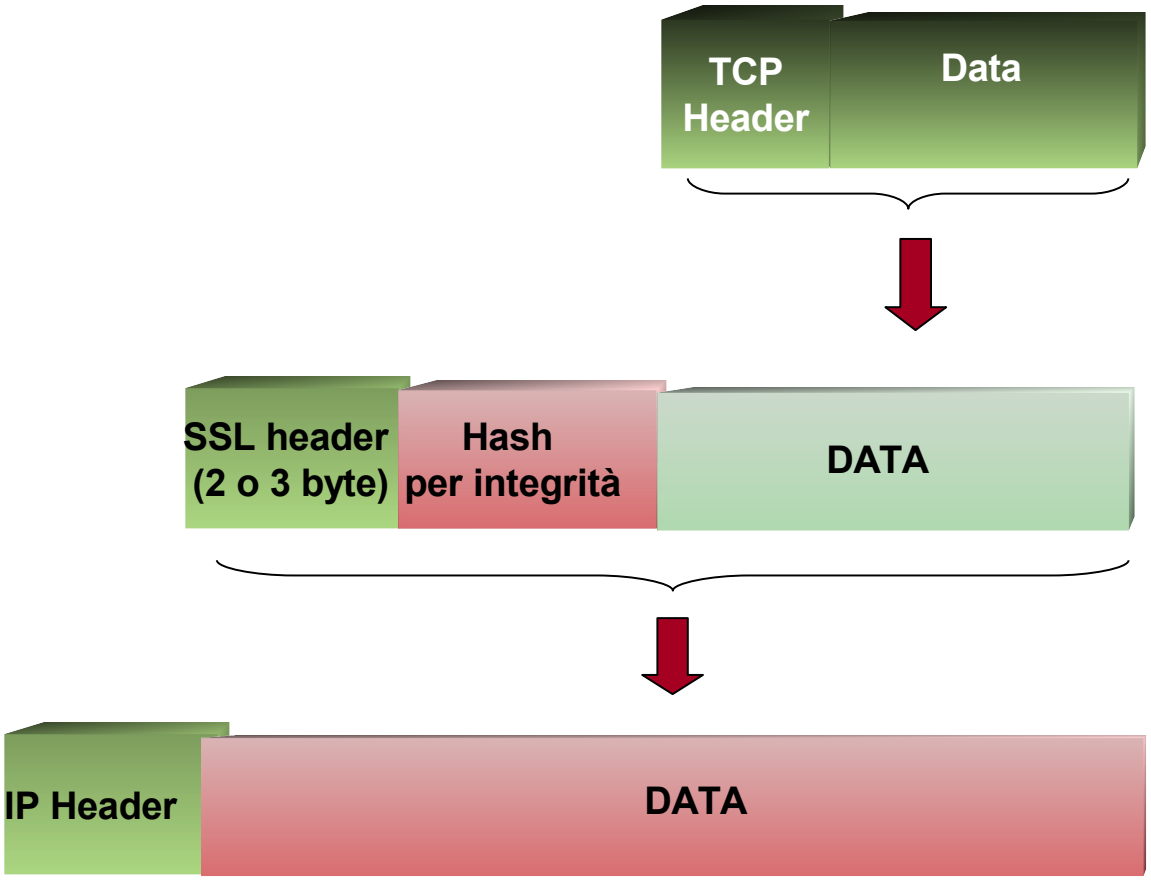
SSL Handshake Protocol

- Negoziazione sull'algoritmo di cifratura, e scambio di chiavi e certificati. Usa RSA a chiave pubblica.
- Autenticazione del server verso il client
- Generazione della chiave di sessione



1. Verifica autenticità del certificato dall'elenco delle CA possibili
2. Selezione della chiave pubblica della CA corrispondente per decifrare il certificato e ottenere la chiave pubblica del server
3. Generazione chiave simmetrica e sua cifratura con chiave pubblica del server e suo invio al server
4. Uso chiave simmetrica come chiave di sessione

SSL Record Protocol



→ Livello TCP

Incapsula dati e info di autenticazione e cifra con chiave simmetrica

→ Livello IP

Sicurezza nelle Applicazioni: PGP

- Scritto da Zimmermann nel 1991, Pretty Good Privacy (PGP)
- Fornisce: riservatezza, integrità e autenticazione
- Usa :
  1. chiave simmetrica di sessione,
  2. chiave pubblica asimmetrica,
  3. firma digitale,
  4. hashing per l'integrità
  5. autenticazione mediante server PGP di distribuzione delle chiavi pubbliche
4. Mail rese sicure e imbustate in SMTP

Preambolo

Il copyright imposto sui documenti pubblicati sul sito MMEDIA5.DET.UNIFI.IT ha lo scopo di consentire la libera circolazione del lavoro a scopo educativo, mantenendo pero' il doveroso riconoscimento agli autori delle varie parti. Si vuole, inoltre, consentire l'ulteriore distribuzione del lavoro sotto qualunque forma, anche con modifiche, mettendo pero' il successivo ricevente in grado di conoscere da chi il materiale sia stato originariamente scritto e da chi rivisto o modificato. Per questo, si impone il Copyright su tutto il materiale, ma si concede gratuitamente licenza per l'uso e l'ulteriore distribuzione, con la possibilita' di modificare il materiale, purche' vengano seguite le regole scritte piu' avanti.

Il diritto di cui sopra e' concesso con la restrizione che il materiale modificato e redistribuito sia soggetto alle stesse restrizioni del materiale originario, e che la distribuzione avvenga a titolo gratuito o con la sola copertura delle spese vive con un piccolo margine per le spese generali di distribuzione. Inoltre, la re-distribuzione del materiale o la distribuzione di materiale modificato dovranno essere fatte in modo da garantire che ulteriori distribuzioni vengano fatte mantenendo le condizioni originarie.

Ogni utente di MMEDIA5 potra' proporre all'Universita' di Firenze la pubblicazione di documenti in MMEDIA5. Scrivere a: fpirri@ing.unifi.it

Tali documenti saranno soggetti ai termini qui specificati. Le condizioni per la licenza di pubblicazione e modifica sono riportate di seguito.

LICENZA PER IL MATERIALE "MMEDIA5"
CONTENUTO NEL SITO WEB "MMEDIA5.DET.UNIFI.IT" CONDIZIONI PER L'USO, LA MODIFICA E LA DISTRIBUZIONE

1.- Questa licenza e' applicabile al materiale contenuto nel sito WEB del Laboratorio di Tecnologia della Telematica, Dipartimento di Elettronica e Telecomunicazioni dell'Universita' di Firenze, via di S. Marta 3, 50139 Firenze - Italia (attualmente con indirizzo internet: http://mmedia5.det.unifi.it/) che riporta al suo interno un avviso o legame con un file contenente la presente licenza. In questa licenza, con MMEDIA5 si intende un qualunque documento originariamente presente nel sito. Per "documento derivato" si intende ogni documento che contenga porzioni oppure un intero documento MMEDIA5, con o senza modifiche, con o senza traduzioni in altra lingua, con o senza variazioni di supporto di memorizzazione o stampa; in questa licenza ogni documento di questo tipo e' indicato come "documento derivato". Per licenziatario si intende qualunque persona o organizzazione che copia, consulta, legge, memorizza su un qualunque supporto, produce o
distribuisce a terzi un MMEDIA5 o un documento derivato. Per UNIVERSITA' si intende l'Universita' di Firenze.

2.-Un licenziatario puo' copiare, consultare, leggere, memorizzare su un qualunque supporto, produrre e distribuire a terzi un MMEDIA5, purche' su ogni copia, produzione, esibizione o distribuzione sia evidenziato il copyright originario, il ricevente sia adeguatamente informato della provenienza del materiale e dell'esistenza di questa licenza e questa licenza sia inserita indivisibilmente e senza modifica alcuna assieme all'MMEDIA5.

L'eventuale cessione o distribuzione devono essere a titolo gratuito. E' comunque ammessa l'imposizione di un rimborso delle spese legate al supporto fisico di memorizzazione dello MMEDIA5, con un piccolo margine per il recupero delle spese generali legate alla riproduzione fisica.

3.- Il licenziatario puo' produrre documenti derivati, ai sensi dell'articolo 1, e distribuirli a terzi purche' siano rispettate tutte le seguenti condizioni:
3.1- ogni documento derivato deve riportare chiaramente la data e l'autore delle modifiche effettuate;
3.2- il licenziatario deve assicurare che ogni documento derivato sia sottoposto alla stessa licenza del documento originario, cosi' che la terza parte ricevente sia impegnata a sua volta negli stessi termini di questa licenza;
3.3- ogni documento derivato deve riportare, all'inizio e in buona evidenza questa licenza o un legame ad un file che la contiene, e il file deve essere distribuito indivisibilmente dal documento derivato;

4.- Al licenziatario e' espressamente vietato copiare, consultare, leggere, memorizzare su un qualunque supporto, produrre e distribuire a terzi un MMEDIA5, se non nelle forme e nei modi previsti in questa licenza. Ogni forma di inosservanza di questa norma comporta l'immediata revoca di ogni diritto concesso con questa licenza.

5.- L'uso di materiale soggetto a Copyright senza un esplicito assenso del proprietario del Copyright e' proibito dalla legge. L'UNIVERSITA' pone come prerequisito per ogni uso di MMEDIA5 l'accettazione di questa licenza. Quindi,e' fatto espresso divieto, a chiunque non intenda accettare i termini di questa licenza, di usare MMEDIA5 in alcun modo. Peraltro, non e' richiesta alcuna forma di accettazione esplicita della licenza, l'uso di MMEDIA5 costituisce implicita accettazione e conferisce al licenzatario tutti i diritti qui espressi.

6.- Ogni volta che MMEDIA5 od un documento derivato vengono distribuiti, al ricevente e' automaticamente estesa questa licenza. Al licenziatario non e' permesso imporre altri obblighi sul ricevente oltre la presente licenza. In ogni caso il licenziatario non e' considerato responsabile dell'uso che il ricevente fa di MMEDIA5.

7.- Se per qualunque motivo, compresi regolamenti o leggi dello Stato, non e' possibile per il licenziatario imporre questa licenza, o parti di essa, al ricevente, allora il licenziatario non puo' distribuire MMEDIA5, ne' parti di esso, ne' documenti derivati, in alcun modo.

8.- L'UNIVERSITA' potra' pubblicare revisioni di questa licenza. Le nuove versioni avranno intendimenti similari, ma potranno differire nei dettagli per far fronte a nuove situazioni. Ogni nuova versione avra' un proprio numero distintivo e sara' applicata ai documenti MMEDIA5 da allora pubblicati.

9.- Usi di MMEDIA5 diversi da quanto sopra specificato potranno essere autorizzati dall'UNIVERSITA'. Queste autorizzazioni non comporteranno variazioni per i licenziatari preesistenti.

10.- Essendo la licenza gratuita, l'UNIVERSITA' fornisce MMEDIA5 cosi' come si trova, e non assume alcuna garanzia di esattezza dei contenuti, o di adeguatezza a qualsiasi scopo. Inoltre, le singole parti di MMEDIA5 sono espressione dei vari autori o revisori menzionati e non espressione dell'UNIVERSITA', non comportano ne' implicano accettazione del contenuto da parte dell'UNIVERSITA'.