

Lezione 4 – Applicazioni e Sicurezza

Francesco Brun

Sistemi elettronici e informatici in ambito di imaging – II



Siamo sempre qui...

- Abbiamo esplorato la pila di protocolli TCP/IP

Application	Telnet	Ftp	Sntp	Http	Nntp	ecc.
Transport	Tcp		Udp			
Internet	IP					
Host -to - Network	Vari standard per LAN, WAN e MAN					

- E' giunto il momento di entrare nel dettaglio di alcuni protocolli applicativi

Il modello client/server

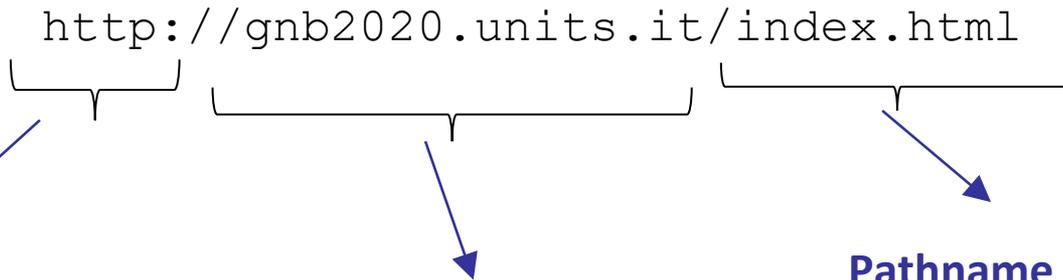
- I servizi Internet si fondano sull'idea di un fornitore e un consumatore
 - ✓ Il fornitore del servizio è il servente (**server**)
 - ✓ Il consumatore del servizio è il cliente (**client**)
- Appositamente distribuiti in Internet ci sono svariati server
- Grosse organizzazioni hanno una **server farm** (opportunamente protetta)
- Si tratta di (insiemi di) calcolatori programmati per rispondere a richieste via rete
- I termini server e client possono indicare:
 - ✓ Sia l'hardware del calcolatore destinato a offrire/ricevere il servizio
 - ✓ Il software in esecuzione su quel calcolatore
- Il server è quindi un concetto di **livello 7 ISO/OSI**

World wide web

- Il servizio Internet più utilizzato oggi è il **world wide web** (**web** o **www**)
- Si tratta di testo e immagini (**ipertesti**) messi a disposizione in forma di "pagine"
- Le pagine sono collegate tra loro mediante **link** (creando la "ragnatela")
- Si fonda su diverse "tecnologie":
 - ✓ Il protocollo **HTTP** (*Hyper Text Transfer Protocol*)
 - ✓ Un linguaggio per le pagine: **HTML** (*Hyper Text Markup Language*)
 - ✓ Il concetto di **URL** (*Uniform Resource Locator*) per reperire le pagine
- Un apposito software detto **browser** consente la "navigazione" tra pagine
- La navigazione di norma inizia mediante digitazione di un URL

URL

- Ad esempio, l'URL:



Protocollo di livello applicazione: di norma HTTP, HTTPS o FTP. Se non si specifica nulla il browser aggiunge `http://`

Nome web server: può essere l'indirizzo TCP (indirizzo IP:porta) del web server su cui risiede la risorsa ma anche un alias come `units.it`

Pathname della risorsa: è il percorso del file (in questo caso il file HTML `index.html`) all'interno del file system del web server (in questo caso nella directory «radice»).

- Nel mondo "giornalistico" si parla di visitare "l'indirizzo" web

DNS (*Domain Name System*)

- E' il sistema che **risolve nomi mnemonici in indirizzi IP** e viceversa
- (Il web senza DNS sarebbe come un cellulare senza rubrica...)
- E' realizzato tramite un database distribuito costituito dai server DNS
- Un'organizzazione compra un blocco di indirizzi IP pubblici
- Quasi sempre compra anche un **dominio** ovvero un nome mnemonico
- Un dominio (es units.it) è composto da
 - ✓ nome
 - ✓ un'estensione legata (in teoria) alla nazione dell'organizzazione
- L'insieme di nome.estensione dev'essere univoco al mondo
- Se ne occupa un'autorità coordinata a livello mondiale

Estensioni DNS

- L'estensione del dominio era stata pensata per identificare la nazione:
 - ✓ .it per l'Italia
 - ✓ .fr per Francia
 - ✓ ...
- Negli USA hanno pensato diverse estensioni:
 - ✓ .com per organizzazioni commerciali
 - ✓ .org per organizzazione non lucrative
 - ✓ .gov per organizzazioni governative
 - ✓ .edu per le università
- Oggi c'è maggiore libertà ed esistono numerosi estensioni (.net, .tv)

Configurazione DNS

- Ogni nodo necessita di sapere chi contattare per risolvere i nomi di dominio
- Oltre a IP, subnet mask e default gateway è comune configurare il DNS
- Per semplicità questi dati possono anche essere forniti in automatico (tipico di configurazioni DHCP)

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

Subnet mask:

Default gateway:

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

Alternative DNS server:

Validate settings upon exit

Advanced...

OK Cancel

Esempio (abbastanza) completo

- Possiamo ora spiegare cosa accade quando si scrive in un browser
`www.facebook.com`
- Accadono (l'ordine non necessariamente è preciso) le seguenti cose:
 1. Il browser completa l'URL con i valori di default, ovvero l'URL diventa:
`http://www.facebook.com`
 2. Il browser deve risolvere l'indirizzo `www.facebook.com`
 3. Si rivolge al sistema operativo per conoscere il server DNS da contattare
 4. Il sistema operativo risponde con l'indirizzo IP del server DNS
 5. Il browser mediante **le regole del protocollo DNS** formula la richiesta:
«Caro server DNS, mi dici l'indirizzo IP di `www.facebook.com`?»
 6. La richiesta è inoltrata al sistema operativo

Esempio (abbastanza) completo

6. La richiesta è inoltrata al sistema operativo su una connessione TCP
 - i. Il sistema operativo incapsula la richiesta DNS in segmenti TCP
 - ii. Questi segmenti TCP verranno incapsulati in pacchetti IP
 - iii. Ci si chiede se il server DNS si trova sulla nostra network
 - iv. La risposta è no. Il sistema operativo inoltra questi pacchetti al router
 - v. Aspettiamo risposta tramite il router dal server DNS
7. Riceviamo risposta che `www.facebook.com` è un alias per `173.252.120.6`
8. Il browser trasforma l'URL in:

`http://173.252.120.6:80`
9. Il browser fa richiesta della pagina principale a quel web server
10. La richiesta è formulata secondo **le regole del protocollo HTTP**

Esempio (abbastanza) completo

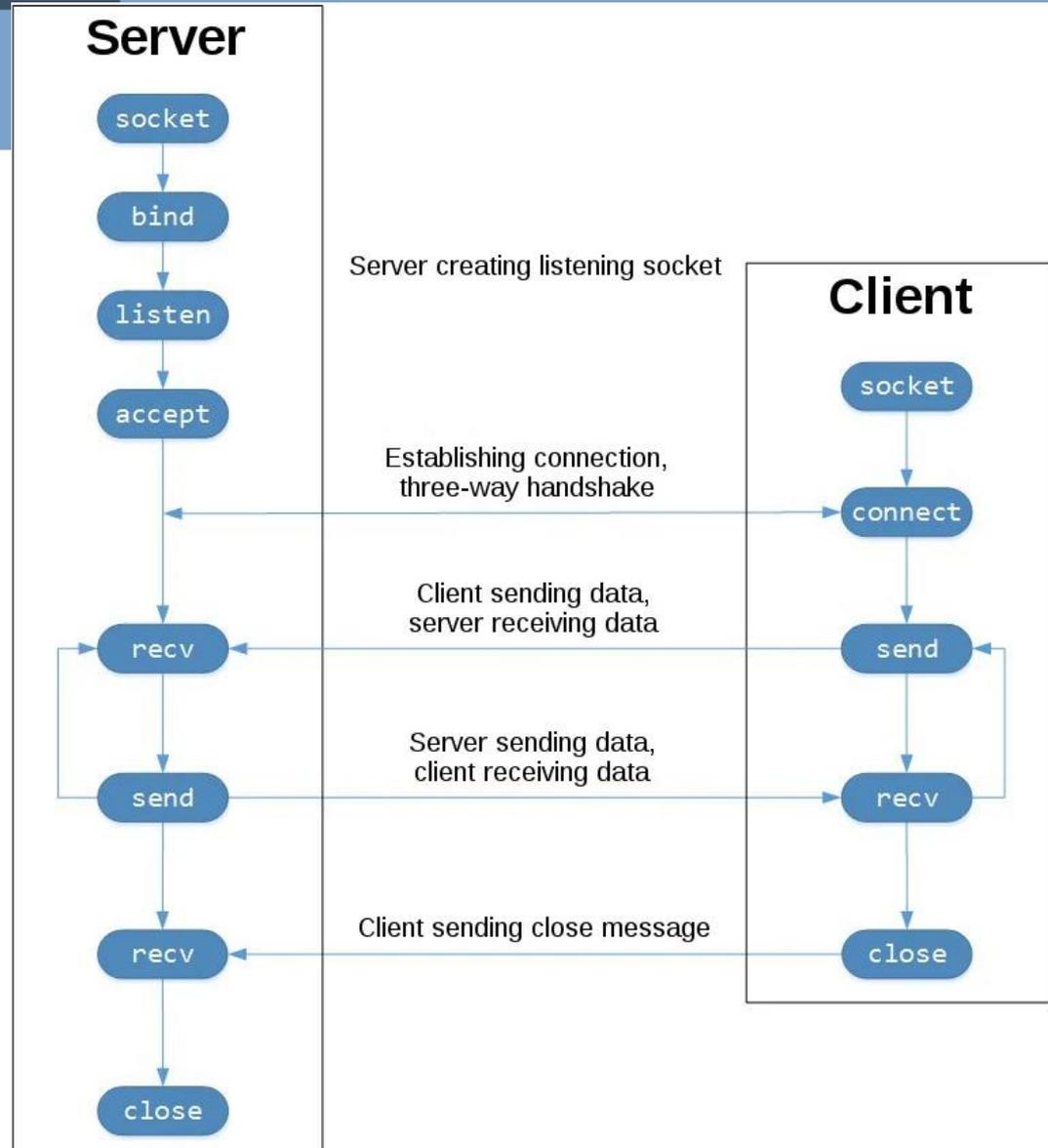
11. La richiesta è quindi: «*Caro server web, mi dai la pagina principale?*»
 12. La richiesta è inoltrata al sistema operativo
 - i. Il sistema operativo incapsula la richiesta HTTP in segmenti TCP
 - ii. Questi segmenti TCP verranno incapsulati in pacchetti IP
 - iii. Ci si chiede se il web server è nella nostra network
 - iv. La risposta è no. Il sistema operativo inoltra questi pacchetti al router
 - v. Aspettiamo risposta tramite il router dal server web di facebook
 13. Riceviamo come risposta una pagina scritta in HTML
 14. Il browser inizia a visualizzare il contenuto di questa pagina
- Spesso questa pagina HTML è generata "al volo"
 - Altre volte la pagina HTML è un file .html sul file system del web server

Posta elettronica

- Oggi è comune usare la posta elettronica attraverso il web
- In realtà è possibile configurare anche un **client di posta** (es. MS Outlook)
- Un client di posta fa uso dei seguenti protocolli:
 - ✓ **SMTP** (*Simple Mail Transfer Protocol*) per spedire un messaggio
 - ✓ **POP** (*Post Office Protocol*) oppure
 - ✓ **IMAP** (*Internet Message Access Protocol*) per ricevere
- L'invenzione di SMTP non fu brillante per vari motivi tra cui:
 - "Each character is transmitted as a 8-bit byte with the high-order bit cleared to zero"*
 - ovvero era stato pensato per mandare mail solo in ASCII e senza allegati
- Far evolvere il protocollo e superare questi limiti non fu facile

Applicazione TCP

- Un'applicazione personalizzata tipicamente usa il **modello client-server**
 - Il *lato server* passivamente aspetta e risponde alle richieste dei client
 - Il *lato client* inizia la comunicazione ed effettua richieste

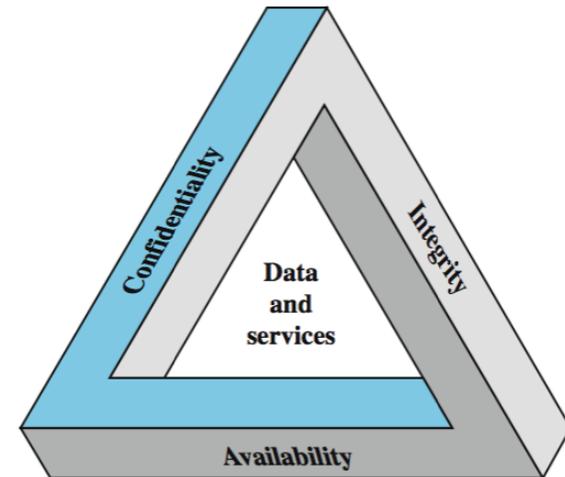


La sicurezza nelle reti

- La sicurezza nelle reti è un problema complesso e implica **proteggere** le risorse:
 - Hardware di livello applicativo (server, dischi, ...)
 - Software
 - Dati
 - Apparati di rete (cavi, switch e router)
- È fondamentale però rispondere alle domande:
 - Cosa significa «proteggere» le risorse?
 - In che modo tali risorse sono minacciate?
 - Cosa bisogna fare per contrastare tali minacce?
 - Quali strumenti ci sono per contrastare tali minacce?
- Inevitabilmente bisognerà trovare un compromesso tra quali risorse è prioritario proteggere e qual è il **costo** necessario per farlo

Cosa significa «proteggere»

- Proteggere significa garantire:
 - **Riservatezza / Confidenzialità**
 - **Integrità**
 - **Disponibilità dei servizi**
- In molti contesti può significare anche in aggiunta:
 - **Autenticità**
 - **Tracciabilità**
- Ognuno di questi aspetti ha un significato specifico e le relative minacce verranno affrontate con strumenti specifici



Minacce e attacchi

- Una **minaccia** è una **possibile** violazione della sicurezza
- La violazione **effettiva** è chiamata **attacco**
- Gli attacchi possono essere di vario tipo. È interessante ricordare che possono essere:
 - **Interni**: iniziati da un'entità interna al sistema
 - **Esterni**: iniziati da un'entità esterna tramite la rete Internet
- Può sembrare strano, ma è opportuno considerare l'ipotesi di minacce provenienti da membri interni all'organizzazione/rete che si vuole proteggere
- Spesso alcuni attacchi sono partiti (inconsapevolmente) da dipendenti/utenti interni
- Minacce sono anche dovute ad **eventi accidentali** (es. guasto di un disco)

Confidenzialità / Riservatezza

- Solo il mittente ed il destinatario “legittimo” dovrebbero essere in grado di comprendere il contenuto del messaggio
- Nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è autorizzato a conoscere
- Se informazioni confidenziali risultano rilevabili da utenti non autorizzati allora c'è un problema di riservatezza

- Confidenzialità (o privacy) implica anche poter controllare **quali informazioni** possono essere collezionate o memorizzate (es. [cookie](#) nel mondo web)

Integrità

- Mittente e destinatario desiderano essere certi che i messaggi scambiati non siano **alterati** da una terza parte senza che se ne accorgano
- Impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali
- Sono necessari strumenti per potere verificare facilmente che un dato è stato alterato in modo non autorizzato

Disponibilità

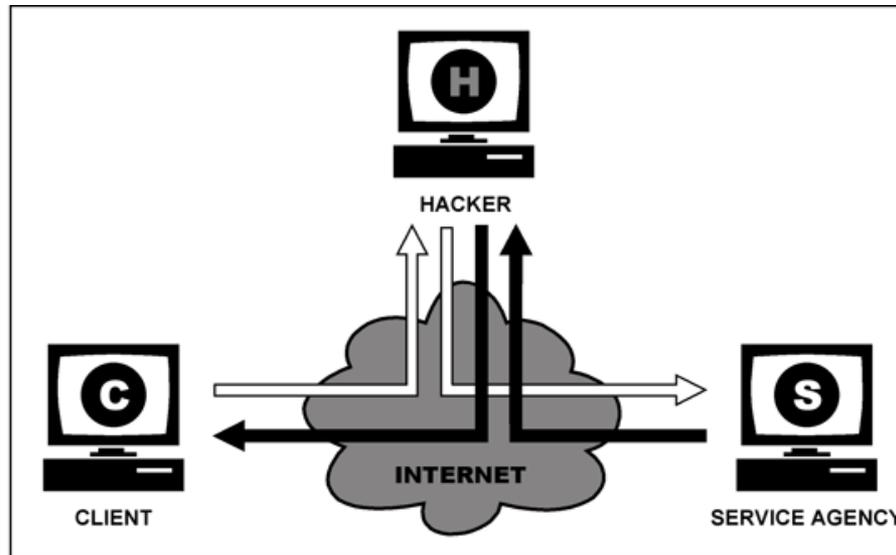
- I servizi offerti in rete devono essere protetti da eventuali **attacchi che hanno il solo scopo di interrompere il servizio**
- Questo implica rendere disponibili a ciascun utente abilitato le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti
- Nei sistemi informatici i requisiti di disponibilità si traducono in **prestazioni** e **robustezza** dell'hardware applicativo e degli apparati di rete
- Es. il sistema informativo (e informatico) di un ospedale dev'essere attivo 24/7
- Nel mondo commerciale un servizio non disponibile implica perdere clienti

Autenticità e tracciabilità

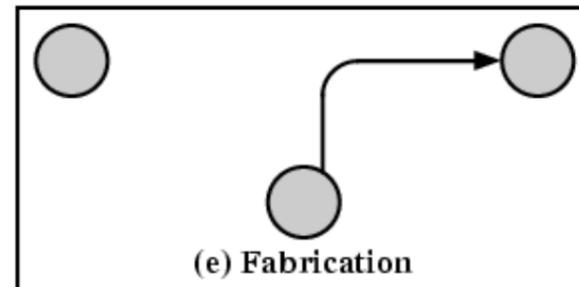
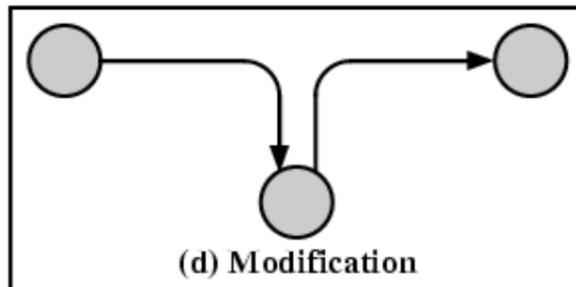
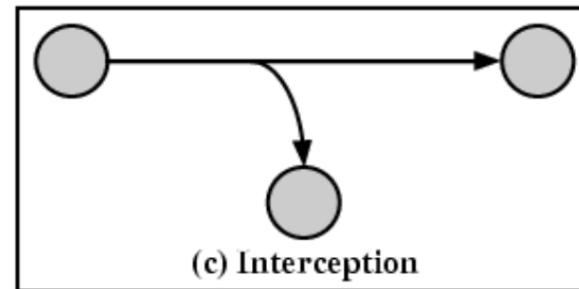
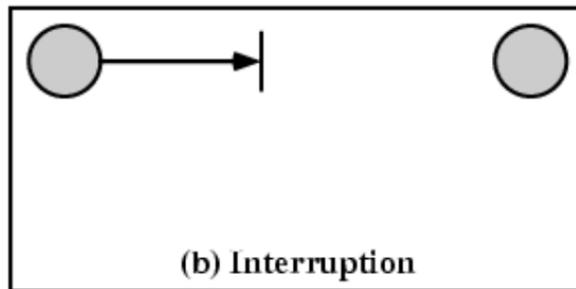
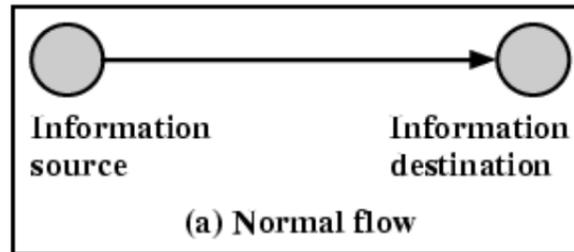
- **Autenticità** significa che mittente e destinatario di una comunicazione/messaggio desiderano essere reciprocamente sicuri dell'identità della controparte
 - Si vuole in sostanza che la controparte sia realmente chi dice di essere
 - L'autenticità è un concetto diverso dalla confidenzialità
 - Ad es. uno sportello bancomat presuppone che chi è in possesso della scheda bancomat e conosce il PIN è autorizzato a effettuare un prelievo
- **Tracciabilità** implica che le azioni di un'entità devono essere tracciate in modo univoco in modo tale da supportare la non-ripudiabilità e l'isolamento delle responsabilità
 - Ad es. nessun utente deve poter negare in tempi successivi di aver spedito un certo messaggio

Attachi informatici

- Supponiamo che due parti intendano comunicare in maniera sicura attraverso la rete
- Una terza parte può ascoltare (stando "in mezzo") i messaggi scambiati ed eventualmente alterarli, cancellarli o crearne di falsi o impersonando una delle due parti



Esempi di attacco



Esempi di attacco

La terza parte "attaccante" (**hacker**) può:

- ascoltare/intercettare i messaggi inviati (**sniffing**)
- inserire messaggi fasulli nel flusso della comunicazione (**spoofing**) anche al fine di fingere di essere una delle due parti
- dirottare la comunicazione, piazzandosi "in mezzo", ad es. fingendo con una parte di essere l'altra e viceversa (**hijacking** e **man-in-the-middle**)
- impedire al servizio offerto di essere utilizzabile (es. sovraccaricando le risorse del servizio) (**denial of service**)

Ognuno di questi attacchi richiede strategie di difesa specifica

Cosa bisogna fare per contrastare le minacce?

- Questa è la domanda più difficile e la risposta può variare
- Nuovi minacce e nuove debolezze possono nascere col tempo
- Le risorse da proteggere sono sistemi complessi composti da sotto-sistemi
 - Trovare il compromesso tra sicurezza del sistema e sicurezza dei suoi componenti
- Manca soprattutto una **“cultura” della sicurezza informatica**
- La sicurezza non viene percepita come un beneficio
 - Fino a quando non avviene un incidente di sicurezza
- Per molti utenti è percepita come un rallentamento delle performance
 - Es. cambiare password periodicamente è “scomodo” o “noioso”
- Per molti manager è percepita come un costo non necessario

Quali strumenti ci sono per contrastare tali minacce?

- Nell'**uso delle reti** si possono incontrare in varie forme tecniche di:
 - Crittografia
 - Firma digitale
 - Autenticazione

Queste tecniche possono anche essere combinate tra loro

- Nella **progettazione delle reti** si possono utilizzare soluzioni di:
 - Isolamento degli apparati di rete (es. DMZ)
 - Controllo e monitoraggio degli accessi
 - Ridondanza dei sistemi
- In queste diapositive ci concentriamo sulle tecniche che incontriamo come utenti di una rete di calcolatori (quindi crittografia, firma digitale, ...)

Tecniche per garantire autenticazione

- Obiettivo: garantire l'identità degli interlocutori
- Una prima tecnica è basarsi su qualcosa che l'utente:

- **Conosce** (es. password, PIN)



- **Possiede** (un badge, una smart card)



- **È** (es. impronta digitale o dell'iride)



Tecniche per garantire autenticazione

- Per **un'autenticazione più forte** si possono combinare diversi fattori

- Qualcosa che si possiede e si conosce



+ PIN

- Qualcosa che si possiede e si è



+



Autenticazione a username e password

- Il metodo di autenticazione più semplice è quello basato su username e password
 - L'utente inserisce un nome che lo identifica (lo username), solitamente non segreto (talvolta il suo indirizzo email), e una parola segreta (la password)
- Attacchi possibili:
 - Intercettazione (se la password passa in chiaro)
 - Guessing/cracking
 - ✓ si può fare un attacco a pura forza bruta...
 - ✓ o più spesso un “**attacco a dizionario**”, provando parole di senso compiuto (o loro minime variazioni)
- Una password dovrebbe essere lunga, non essere una parola di senso compiuto, dovrebbe essere cambiata di frequente e diversa da quella usata per altri servizi
 - Ma questo si scontra con la “comodità” e la “pigrizia” degli utenti...

One-time password (OTP)

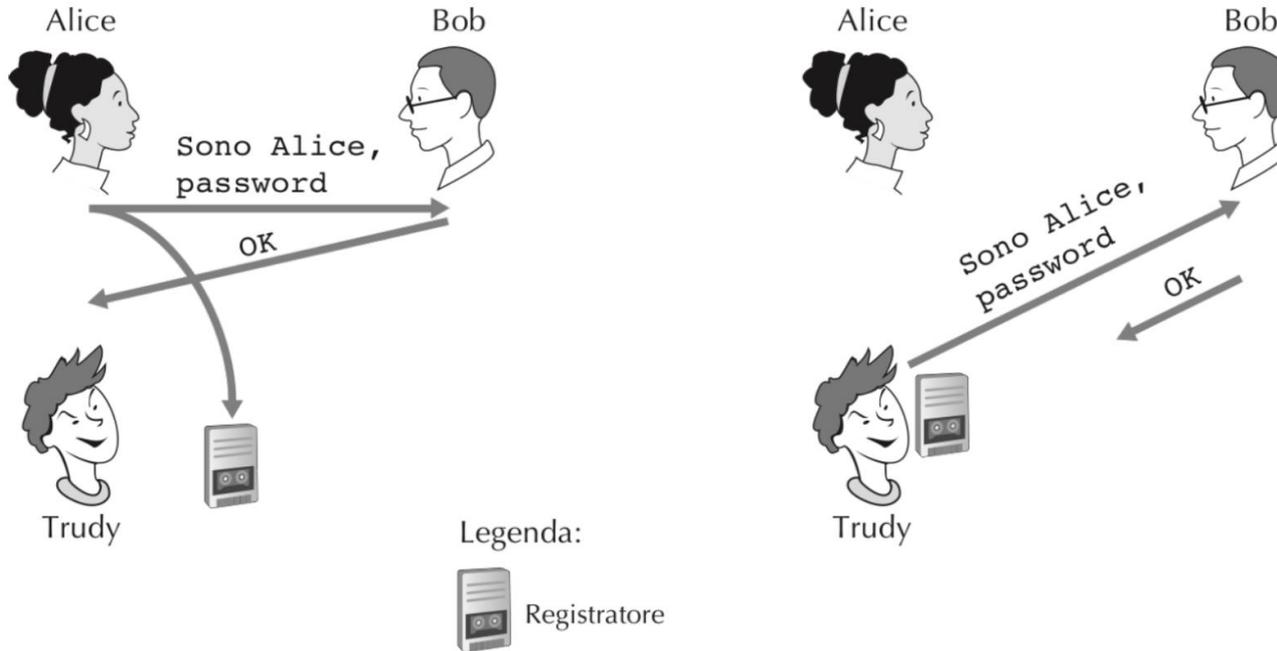
- Con il termine “one-time password” ci si riferisce a sistemi in cui viene generata una **nuova password ad ogni accesso** da parte dell’utente, per risolvere il problema dell’intercettazione
- Queste password “monouso” vengono generate sulla base di un contatore (esiste quindi una sequenza di password successive) o più spesso sulla base dell’istante temporale
- Spesso i sistemi one-time password si appoggiano:
 - su “token”, dispositivi hardware che forniscono all’utente la password da inserire



- SMS inviato su cellulare dell’utente
- Spesso la one-time password viene utilizzata congiuntamente ad un PIN

Autenticazione + crittografia

- La sola autenticazione mediante username, password e/o OTP non è sufficiente
- Un attaccante potrebbe registrare e replicare il meccanismo di autenticazione



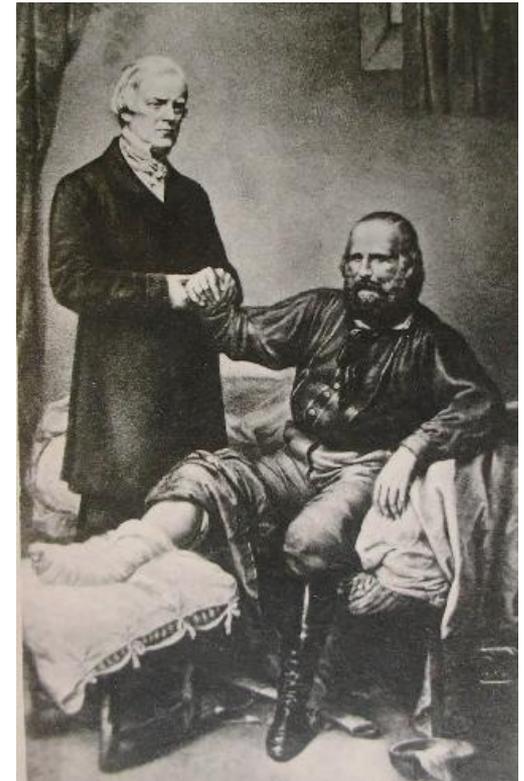
- Una strategia migliore è fare in modo che l'autenticazione avvenga su un **canale sicuro**

Crittografia

- Il problema da risolvere è: dato un messaggio che sembra provenire da un utente, come posso essere sicuro che esso arriva *effettivamente* da tale utente?
- L'idea è: invece di trasmettere il messaggio (es. la password) in chiaro ne viene trasmessa una **versione "indecifrabile"** per tutti o, se serve, decifrabile solo dal destinatario

*Garibaldi fu ferito
fu ferito ad una gamba
Garibaldi che comanda
che comanda il battaglione!*

*Goroboldo fo foroto
fo foroto od ono gombo
Goroboldo co comondo
co comondo ol bottogloon*



Funzione hash

- In linea di principio per rendere un messaggio decifrabile solo tra due utenti è necessario che questi due utenti si siano preventivamente scambiati la chiave per decifrare il messaggio
- Se le due parti si sono già scambiate la chiave per decifrare in qualche modo (con qualche altro mezzo) la cosa, in linea di principio, funzionerebbe
- Il problema però è: **come ci si può scambiare la chiave sullo stesso canale che si vuole utilizzare per comunicare?**
- Una prima osservazione da fare però è: il destinatario deve sempre e comunque decifrare il messaggio?
 - Per es. una password non deve essere nota e trasmessa «in chiaro»
 - Tipicamente si salva e/o trasmette un **hash** della password

Funzione hash

- Una funzione hash trasforma un messaggio di lunghezza arbitraria in output di lunghezza fissa chiamato hash o digest del messaggio originale mediante algoritmi che hanno le seguenti proprietà:
 - **Coerenti**: ad input uguali corrispondono output uguali
 - **Casuali**, o apparire tali: per impedire l'interpretazione accidentale del messaggio originale
 - **Univoci**: la probabilità che due messaggi generino il medesimo hash deve essere virtualmente nulla
 - **Non invertibili**: risalire al messaggio originale dall'output deve essere impossibile
- Piuttosto che salvare/trasmettere la password si salva/trasmette la sua hash
- Questa è già una prima soluzione per evitare di trasmettere "in chiaro"
 - Intercettare la hash consente però comunque di impersonare l'utente

Crittografia asimmetrica

- Ci piacerebbe un metodo di crittografia tale da consentire di decifrare un messaggio e per il quale non ci si deve scambiare un “segreto” (o chiave) tra le due parti
- Una soluzione è la crittografia asimmetrica.
- Ogni partner di comunicazione dispone di una **coppia di chiavi**:
 - chiave pubblica (*public key*)
 - chiave privata (*private key*)
- Le chiavi sono tenute insieme tramite un “**portachiavi**” che unisce le due chiavi attraverso un algoritmo matematico:
 - I dati crittografati con la chiave pubblica possono essere decrittati solo con la chiave privata
 - La chiave privata è realmente tale, ovvero non dev’essere nota ad altri
 - La chiave pubblica viene invece distribuita

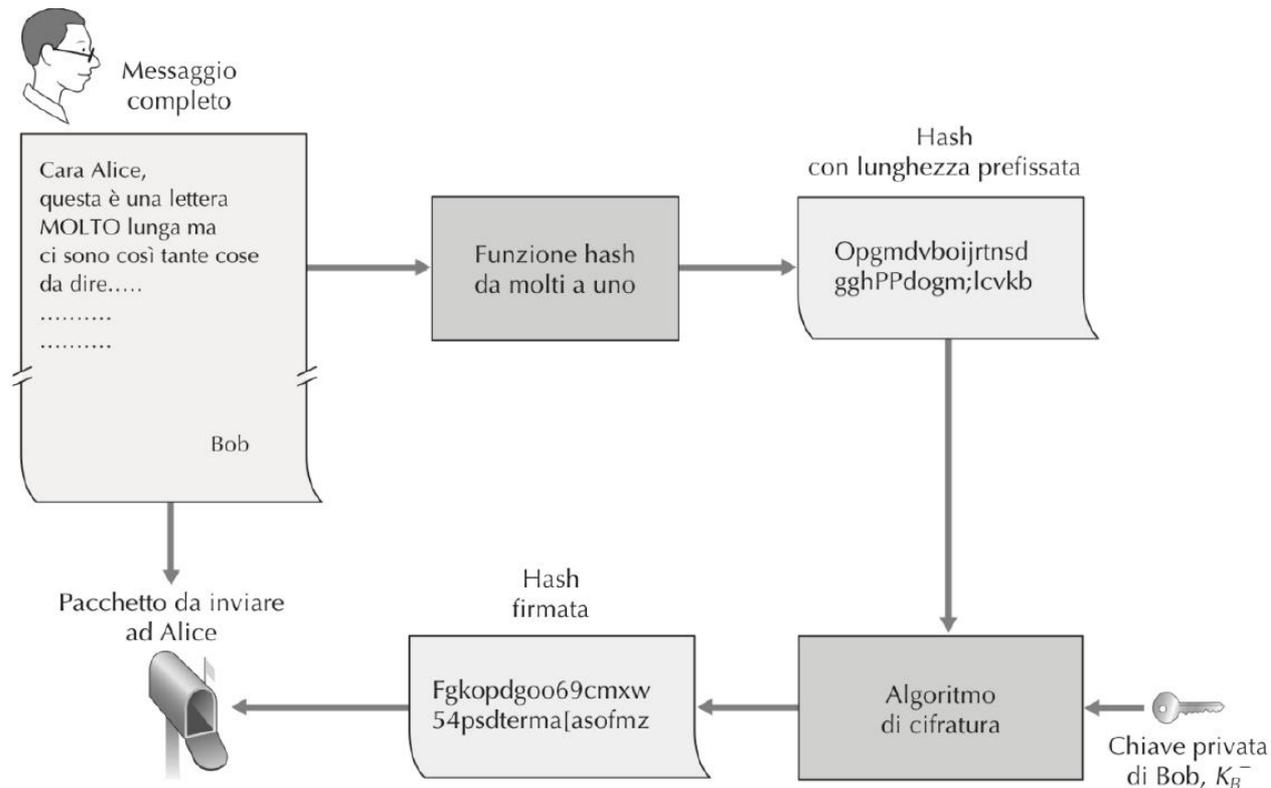
Crittografia asimmetrica

- Il principio di utilizzo è Il mittente codifica il suo messaggio con la **chiave pubblica del destinatario** e invia questo “testo segreto” al destinatario
- Dal momento in cui viene crittografato, questo messaggio può essere decodificato solo dal destinatario con la sua chiave privata
 - Per questo motivo, il canale di scambio è in linea di principio liberamente selezionabile: se anche il messaggio crittografato viene intercettato, l’utente malintenzionato non potrà accedere al suo contenuto
- Il principale algoritmo di crittografia asimmetrica è denominato **RSA**
- Sfrutta un principio matematico basato sull'elevata complessità computazionale della fattorizzazione in numeri primi

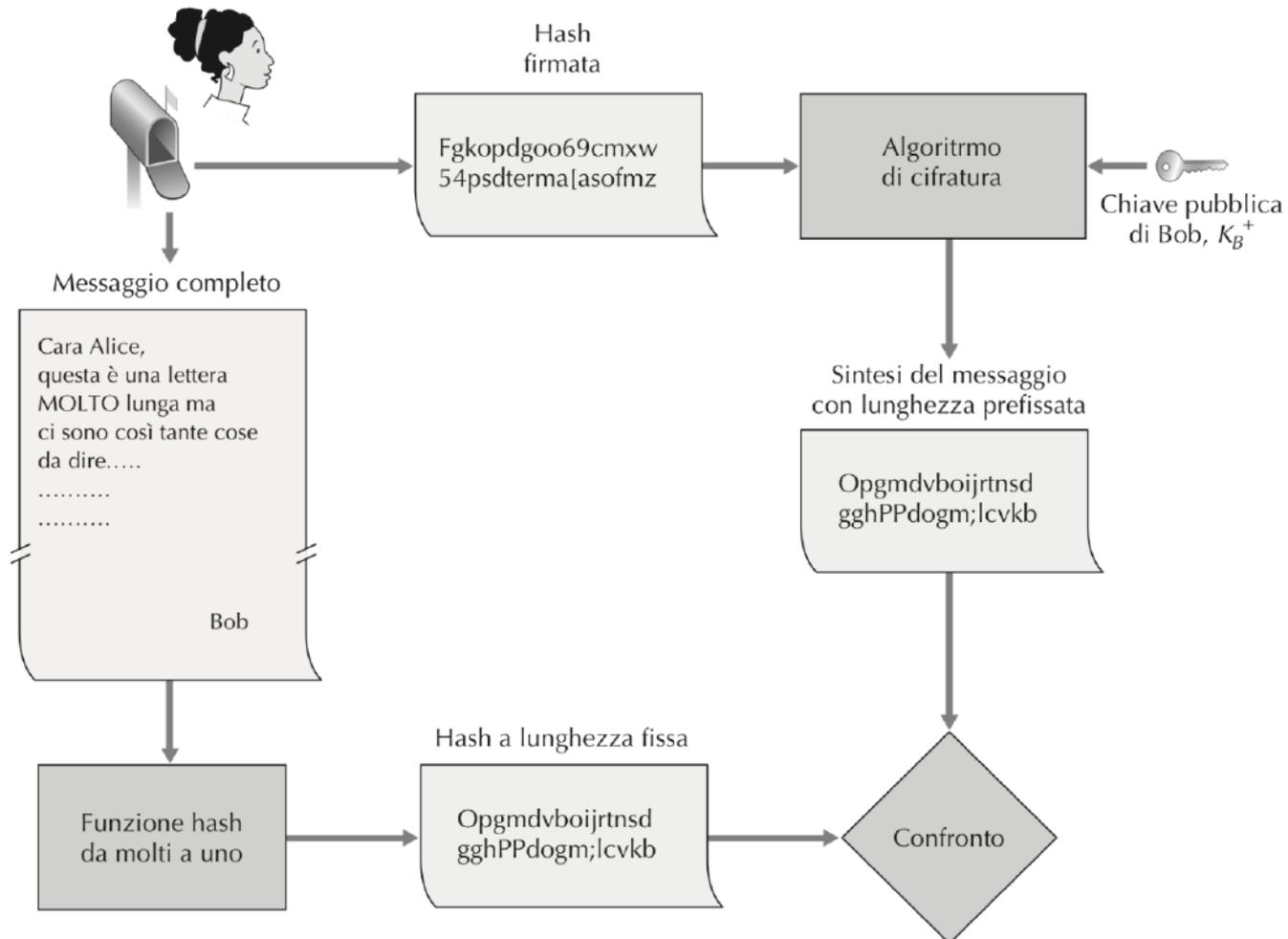
(vedi il video su Asymmetric Encryption)

Firma digitale

- La crittografia asimmetrica può essere utilizzata anche dal mittente per garantire la sua identità (firma digitale)

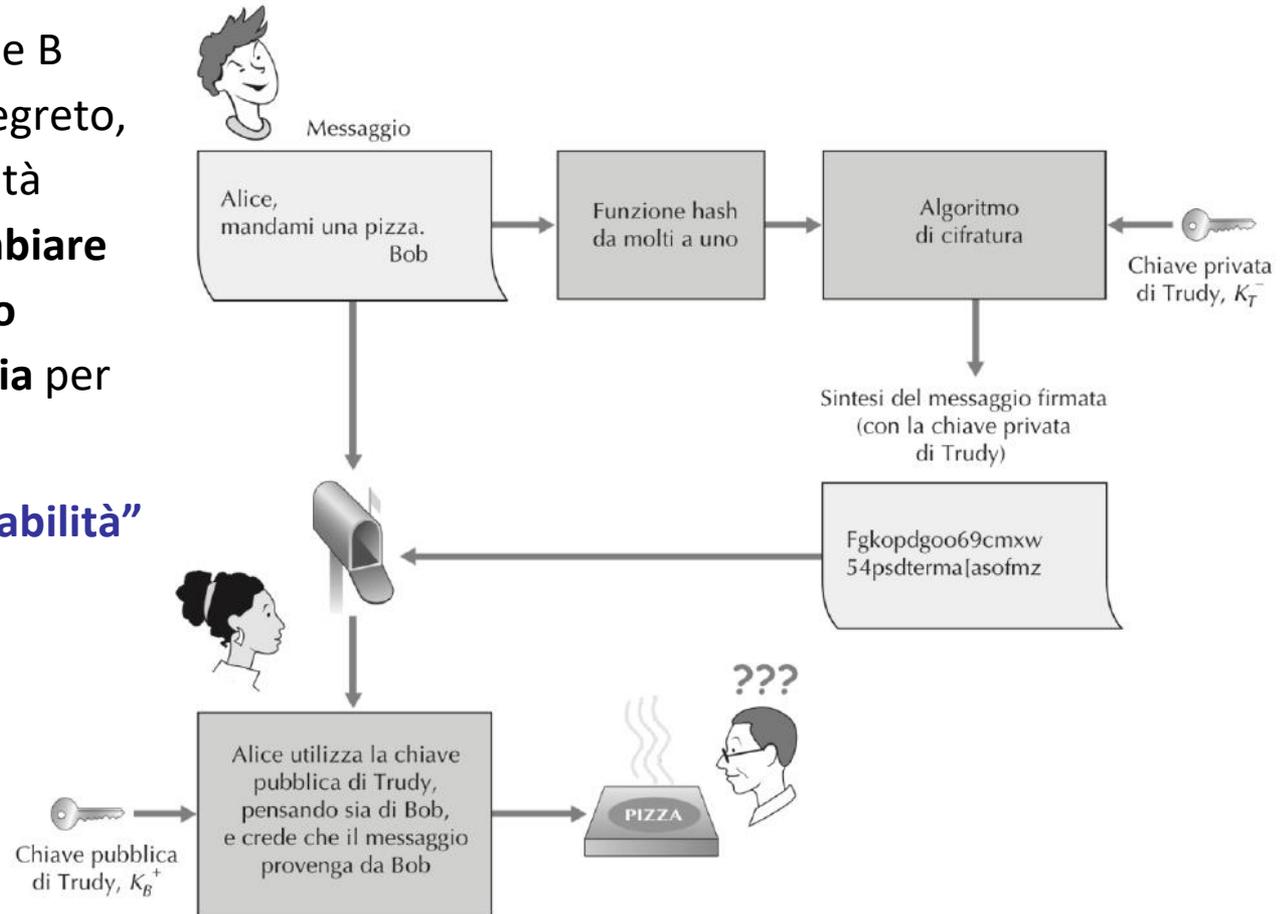


Firma digitale: destinatario



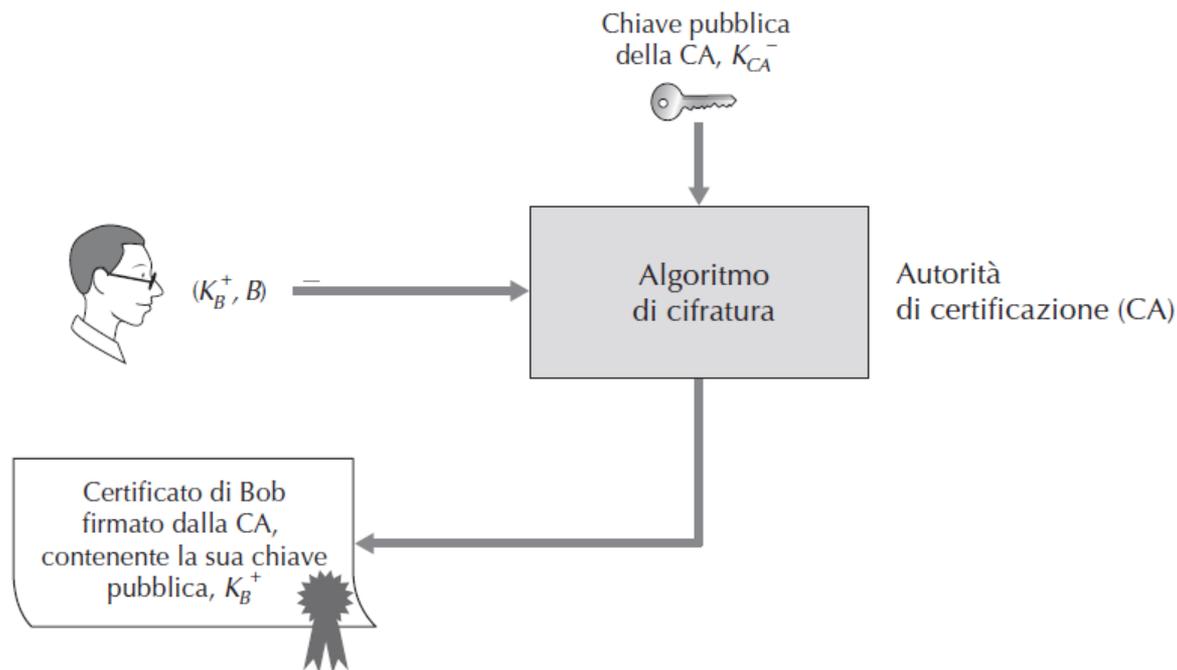
Certification Authority (CA)

- Per quanto due utenti A e B possano scambiare un segreto, non è garantita autenticità perché A **potrebbe scambiare la chiave con un perfetto sconosciuto che si spaccia per B**
- Serve una sorta di **“affidabilità” delle chiavi pubbliche**



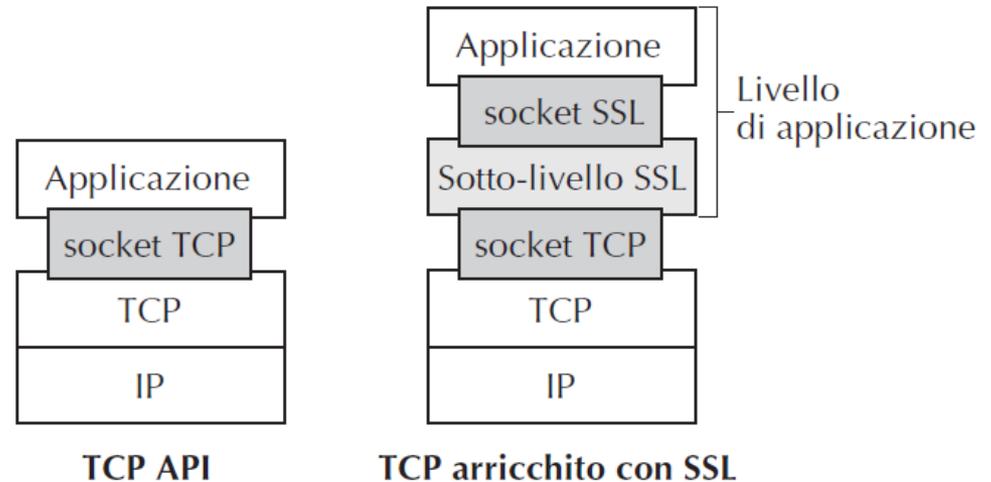
Certification Authority

- È necessaria la **certificazione** della chiave pubblica
 - Utenti, browser, router e così via devono avere la certezza che la chiave pubblica sia proprio quella del corrispondente
- Sono nate autorità di certificazione (**CA, certification authority**):
 - Hanno l'incarico di convalidare l'identità ed emettere certificati
 - Es. Infocert, Poste Italiane, Aruba,



Secure sockets layer (SSL) e HTTPS

- Versione di **TCP arricchita** con servizi di sicurezza per offrire riservatezza, integrità dei dati e autenticazione del client e del server
- Protocollo progettato inizialmente con il nome di SSL poi diventato TLS
- Nel web viene usato SSL quando l'URL inizia con **https://** anziché **http://**
- Il certificato del server a cui ci si connette deve provenire da una CA di cui ci si fida
- Il tutto si inserisce in un contesto denominato **public key infrastructure (PKI)** che implica quindi l'esistenza di CA, chiavi, ecc...

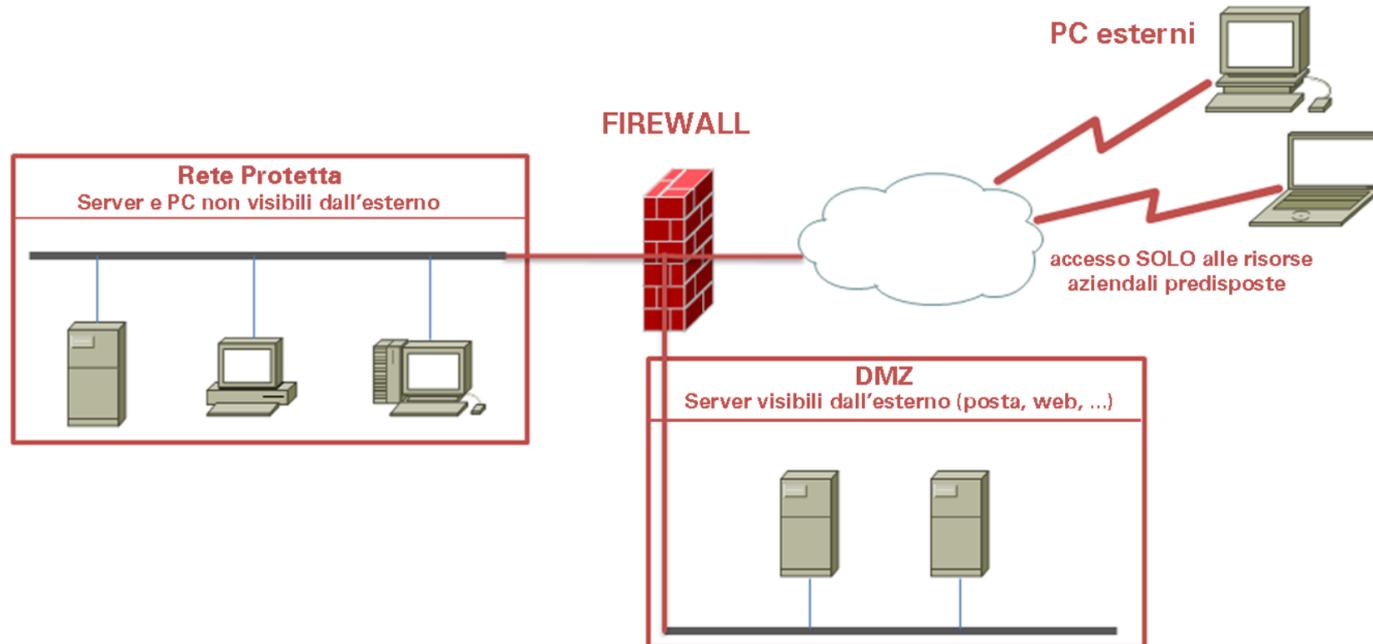


Posta elettronica: sicurezza

- La posta elettronica fu mal ingegnerizzata dal punto di vista della sicurezza
- La password di posta è trasmessa "in chiaro"
 - Anche in questo caso viene utilizzato SSL in combinazione con i protocolli di posta
- La posta elettronica fu pensata come la posta ordinaria
- Per spedire una lettera **non è obbligatorio il mittente**
 - Specificate il destinatario, aggiungete un francobollo e imbucate...
- La posta elettronica allo stesso modo non impone di specificare il mittente
- Si può mentire sul mittente o impersonare fraudolentemente un vero mittente
 - Nascono lo **spam**, il **phishing** e altre minacce informatiche trasmesse via e-mail

Firewall

- Letteralmente: “muro tagliafuoco”
- Si tratta dell'**insieme di apparati e soluzioni** solitamente disposti all'interfaccia tra la rete locale e la rete Internet per garantire la sicurezza della rete



Firewall: obiettivi

- **Controllare il traffico** di rete:
 - permettendo solo quello autorizzato dalle politiche di sicurezza
 - rilevando e segnalando eventuali tentativi di violazione della politica di sicurezza
 - svolgendo eventualmente funzioni aggiuntive di monitoraggio
- **Separare** risorse potenzialmente compromissibili da quelle sensibili:
 - **rete interna**: conosciuta e ritenuta affidabile con le risorse più critiche (*trusted*)
 - **rete perimetrale (DMZ, DeMilitarized Zone)**: contenente le risorse meno critiche
 - **rete pubblica/esterna** (*untrusted*)
- Realizzare architetture di rete modulari con policy di sicurezza diverse

Firewall: funzionamento

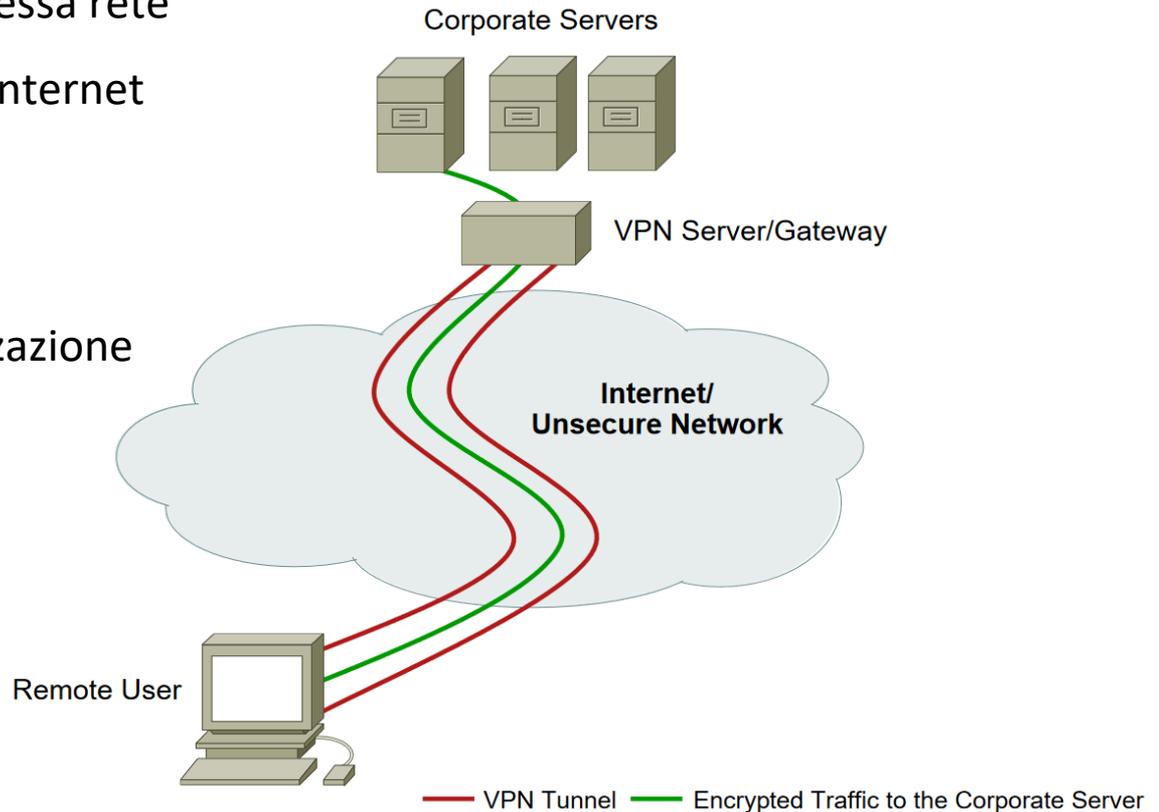
- Un firewall «filtra» il traffico entrante e valuta se inoltrarlo ai nodi interni o bloccarlo
- L'amministratore della rete definisce la *Access Control List (ACL)* specificando quale traffico è permesso e quale è bloccato (*firewall rules*)

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
1	All ICMP	ICMP (1)	ALL	0.0.0.0/0	ALLOW
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
1000	Custom TCP Rule	TCP (6)	1024-65535	10.0.0.0/16	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

(vedi il video sul firewall)

VPN (Virtual Private Network)

- Obiettivo: far comunicare due nodi privati come se fossero sulla stessa rete pur essendo sparsi per la rete Internet
- Motivazioni:
 - Sedi dislocate di un'organizzazione
 - Telelavoro
 - Mobilità



VPN remote access

- Due sedi remote di un'organizzazione possono essere collegate tra loro in modo «privato» lasciando ai router l'incombenza di creare il tunnel VPN tra le sedi
- Una VPN può essere utilizzata anche per **remote access** (da casa o in mobilità)
- In questo caso tipicamente si hanno due strategie:
 - Installare un software di tunneling IPsec VPN (es. *CISCO AnyConnect*, *OpenVPN*)
 - Usare una *webVPN* per il solo traffico HTTP
- L'università di Trieste offre entrambe le soluzioni per studenti e personale. Si veda: <https://www2.units.it/servizi-ict/rete/?file=vpn.htm>

Riassunto dei concetti chiave

- Client e server
- World wide web: HTTP, HTML, URL
- DNS e dominio
- Posta elettronica: SMTP, POP, IMAP
- Socket nei linguaggi di programmazione
- Riservatezza / Confidenzialità
- Integrità
- Disponibilità dei servizi
- Autenticità
- Tracciabilità
- Crittografia a chiave asimmetrica
- Firma digitale
- Hash
- SSL e HTTPS
- Spam e phishing
- Firewall
- VPN