

Sicurezza informatica

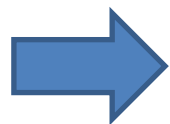
.... di cosa abbiamo parlato
... e possibili percorsi

Cybersecurity

sottoclasse della *information security*



cybersecurity : ambito dell' *information security* prettamente ed **esclusivamente dipendente dalla tecnologia informatica**



approccio mirato ad enfatizzare le ***misure di protezione***

Sicurezza: obiettivi



- Confidenzialità
- Autenticazione
- Non-ripudio
- Controllo Accessi
- Integrità
- Anonimia
- Disponibilità Risorse

Sicurezza: obiettivi

Confidenzialità

Privacy, Segretezza



Informazioni { trasmesse
memorizzate
(anche la semplice esistenza di un oggetto)
sono accessibili in lettura
solo da chi è autorizzato

Autenticazione

messaggi



entità
(Identificazione)



tempo
(Timestamp)



Non-ripudio



{ Chi invia
Chi riceve

non può negare la
trasmissione del
messaggio

Controllo Accessi

Accesso alle informazioni
controllato da o per
il sistema



Sicurezza: obiettivi e paradigma CIA

Integrità

Solo chi è autorizzato può modificare l'attività di un sistema o le informazioni trasmesse



modifica = scrittura, cambiamenti, cancellazione, creazione, ritardi, replay e riordino di messaggi, ...

Anonimia

Protezione dell'identità o del servizio utilizzato.



... meglio "Grado di anonimia"

Disponibilità Risorse

Risorse disponibili a chi è autorizzato quando necessario

Availability



Diverse attese:

- presenza di oggetti e servizi utilizzabili
- capacità di soddisfare le richieste di servizi
- progresso: tempo di attesa limitato
- adeguato tempo del servizio

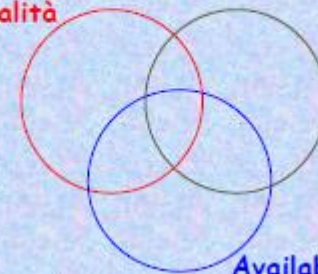
Obiettivi:

- risposta pronta
- allocazione fair
- utilizzabilità
- fault tolerance
- concorrenza controllata (accessi simultanei, gestione deadlock, accesso esclusivo)

Alcune relazioni

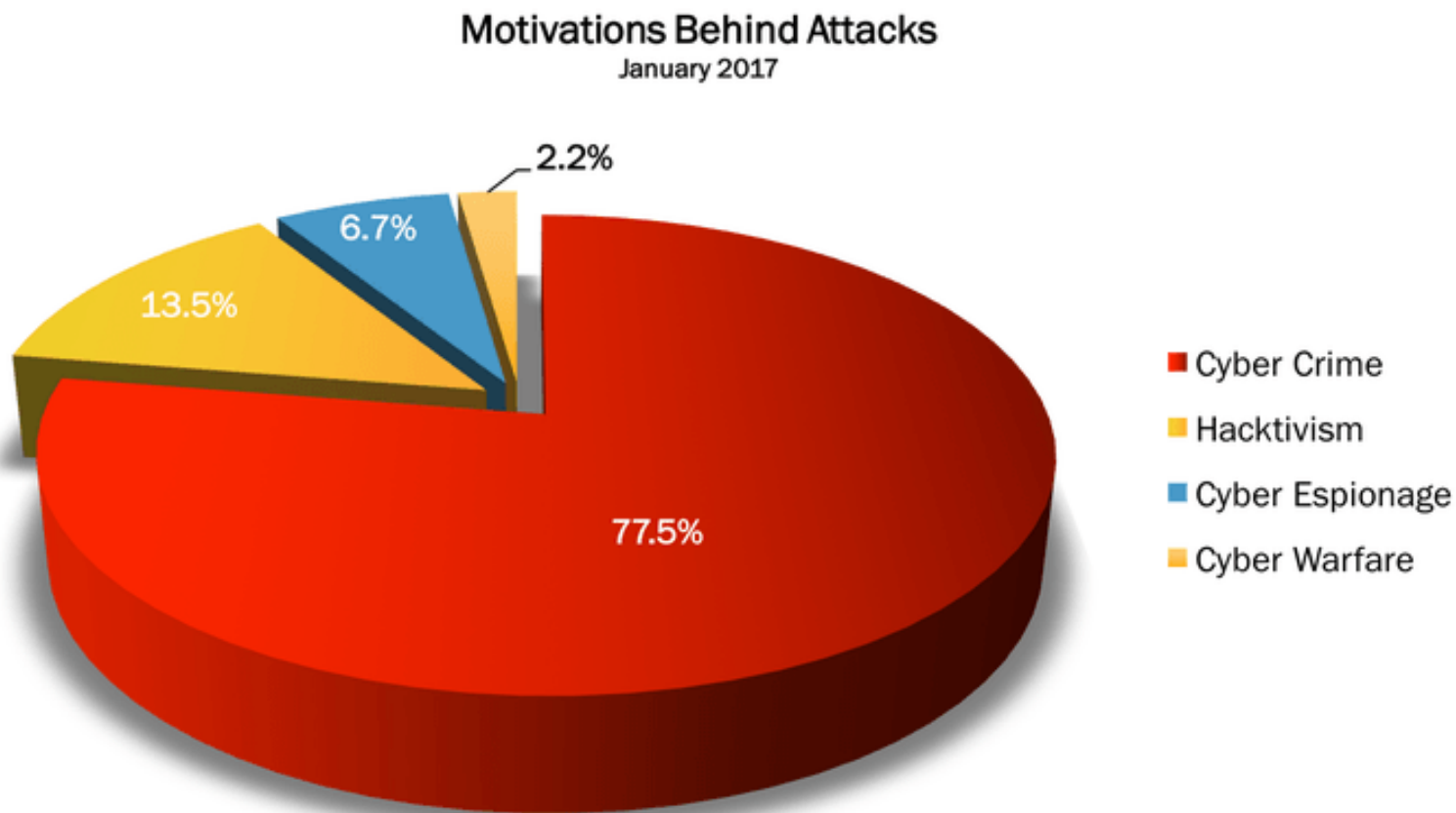
Confidenzialità

Integrità



Availability

Il mercato della cyber-security



hackmageddon.com

dalle slides del Dott. Enrico Cambiaso

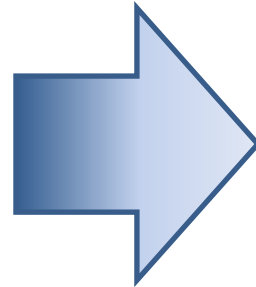
Vecchie tecniche di attacco con scopi diversi



Ransomware (tecnicamente "trojan" tipo worm)

Sicurezza per chi ?

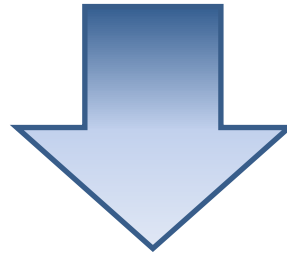
- **Utenti (persone)**
- **Apparati dell'infrastruttura di rete (es. server DNS, router, ecc.)**
- **Falle nella sicurezza dell'infrastruttura possono essere veicolo di attacchi alle attività degli utenti**



Sicurezza richiede compromessi

La Sicurezza richiede compromessi

La quantità di sicurezza che si può ottenere dipende da ciò a cui si può rinunciare pur di ottenerla.



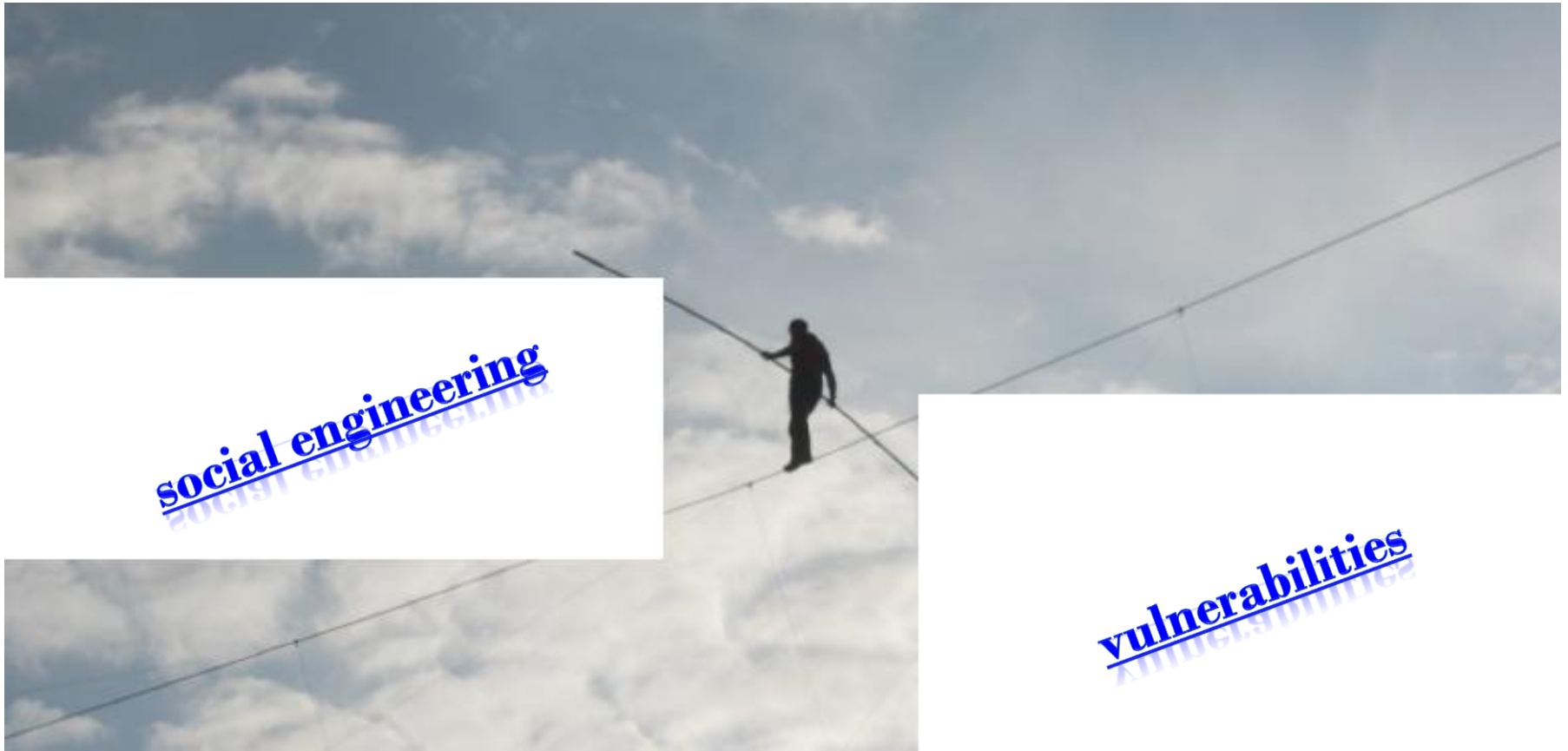
Tracciabilità o
anonimato ?

Equilibrio tra
vulnerabilità e
comportamenti

conoscenza e
consapevolezza
per decidere

Fiducia
e buon senso

Equilibrio tra tecnologia e comportamenti



social engineering

vulnerabilities

Vulnerabilità della Rete

I nemici:

→ Complessità

→ Interazione

→ Compatibilità

→ Fattore umano

da "Sicurezza Informatica",
A. Ghirardini

Complessità



Programmi complessi, con molti moduli scritti da tanti programmatori diversi

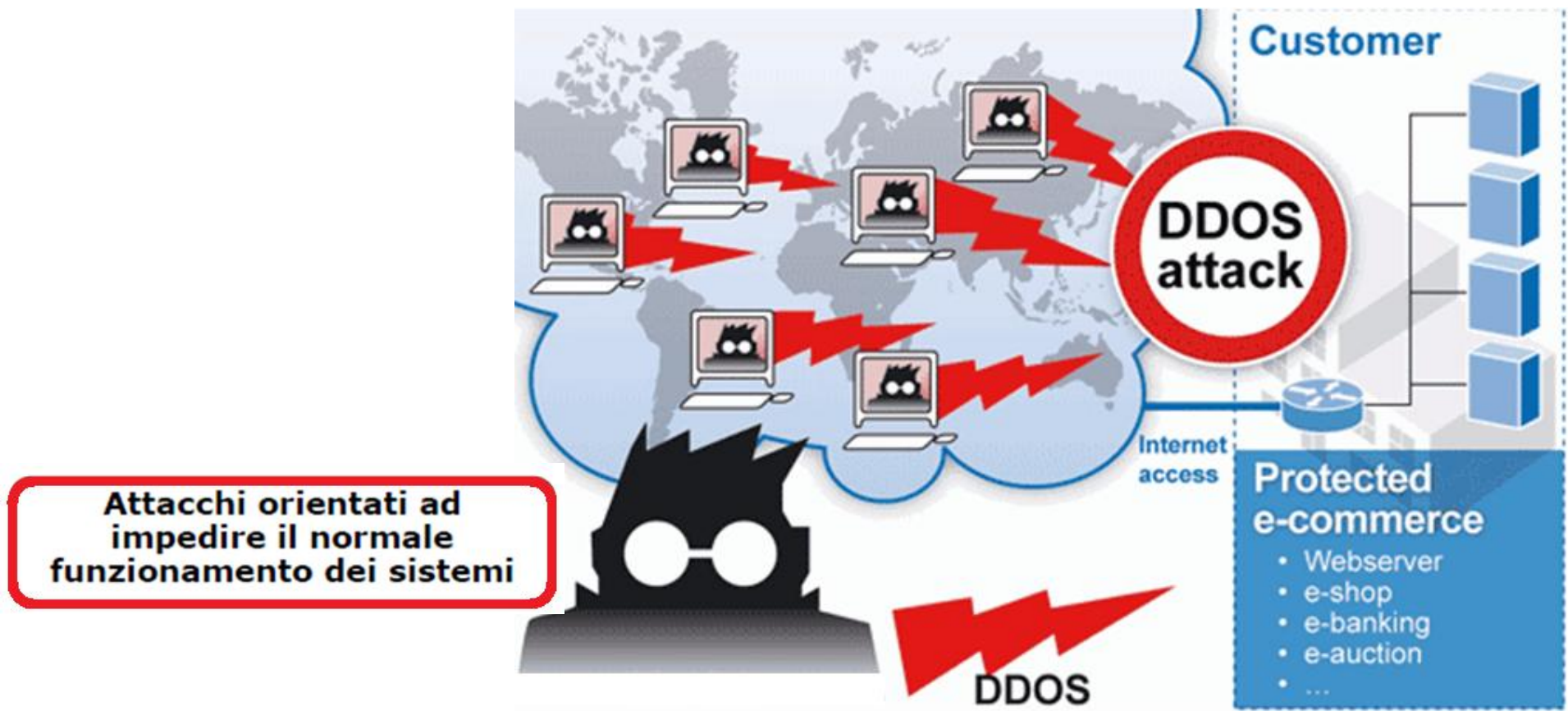
posso fidarmi di chi ha sviluppato il software?

Comunicazioni tra i moduli attraverso canali noti e non noti

Gli utenti vogliono sistemi facili da utilizzare

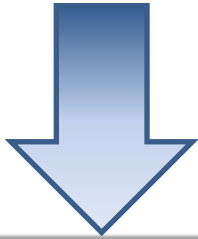
La trappola della complessità

Il nemico peggiore della sicurezza è la complessità



Maggiore è la complessità, più facile è l'attacco

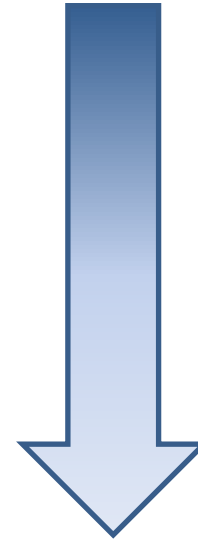
Interazione



Comunicazioni tra i programmi all'interno di un computer

Comunicazioni tra computer attraverso la rete

Compatibilità

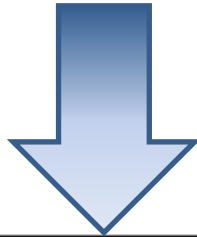


Con sistemi già esistenti, sviluppati prima che sorgessero le esigenze di sicurezza

Con i sistemi di rete esistenti, in massima parte non gestiti da noi

Esigenza di distribuire e rendere accessibili dati e informazioni

Fattore umano



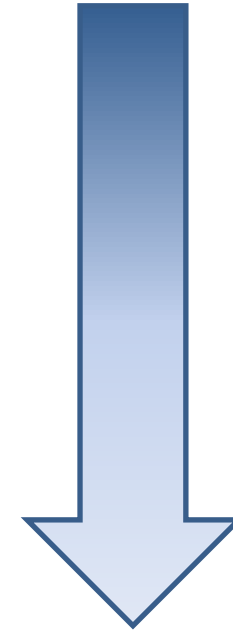
Manca un po' di "buon senso"

Il risultato prima di tutto

Attività frenetiche, non c'è tempo per riflettere/pianificare

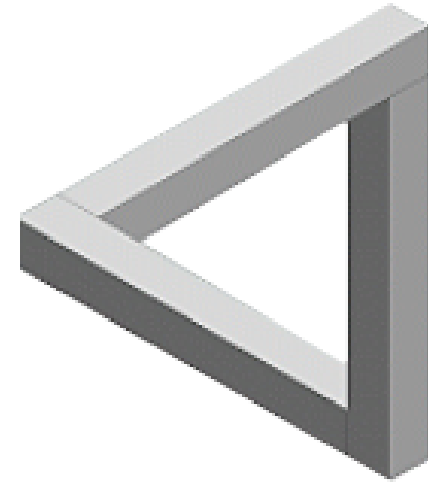
Mancano politiche rigorose di sicurezza

Obiettivo Fiducia



Due dimensioni della fiducia

- **Fiducia** negli strumenti, negli sviluppatori e nei fornitori degli strumenti, conoscenza e consapevolezza dei limiti delle tecnologie
 - hardware, software, reti, ecc.
- **Fiducia** nei servizi, negli sviluppatori e nei gestori dei servizi, conoscenza e consapevolezza di regole e rischi
 - gestione dei dati e utilizzo delle informazioni



Dalle slide del prof. Montessoro – Università degli Studi di Udine



[00 Conoscenza e consapevolezza.pdf](#)

Fiducia e Buon senso



In equilibrio
tra tecnologia
e comportamenti



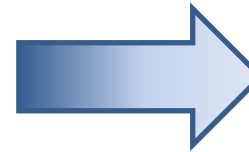
posso fidarmi
dell' IoT



Gli utenti vogliono
usare con facilità
velocità ... proprie "cose"

Progettare la sicurezza

**Non solo tecnologia, ma
metodologia e gestione**



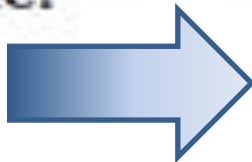
Security Manager

**HW, SW e servizi vengono
progettati sempre *peggio!***

**Attenzione ai servizi non richiesti
e non strettamente indispensabili**

**Sistemisti: massima attenzione
all'utente!**

Utenti

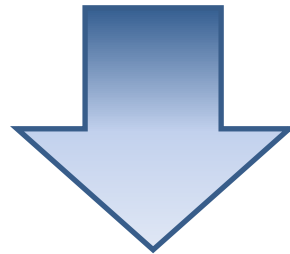


**Fiducia
e buon senso**

Vulnerabilità della Rete

**I protocolli di Internet
nascono negli anni '60**

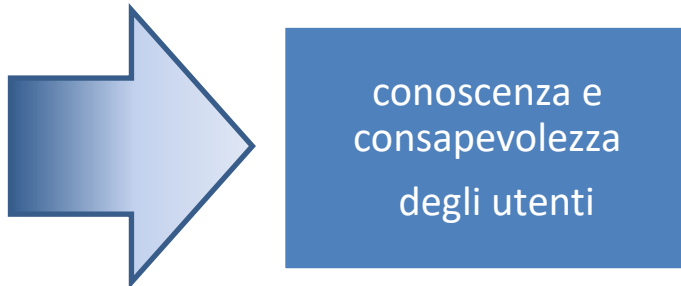
→ Non pensati per la sicurezza!



ESTENSIONI ALL'ARCHITETTURA DI RETE

Un nuovo contesto

- No "control-alt-del"
- No "riformatta il disco e reinstalla il sistema operativo"
- Servono
 - architetture intrinsecamente sicure
(sarà realmente possibile?)
 - serie politiche di migrazione/aggiornamento



Conoscenza e consapevolezza



Dalla Internet delle persone...

...alla Internet delle cose



Dalle slide del prof. Montessoro – Università degli Studi di Udine



[01 introduzione alla sicurezza informatica/](#)

La dura verità

- Un progettista deve trovare TUTTE le vulnerabilità del suo sistema
- Un hacker deve trovarne SOLO UNA
- Il progettista viene inevitabilmente sconfitto

(Mike Muller, CTO, ARM, "The Ugly Truth", IoT Security Summit 2015)

Dalle slide del prof. Montessoro – Università degli Studi di Udine

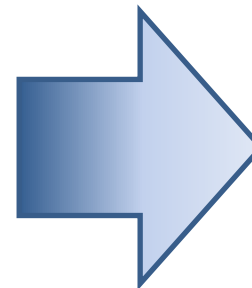


[00 Conoscenza e consapevolezza.pdf](#)

Confidenzialità e tracciabilità

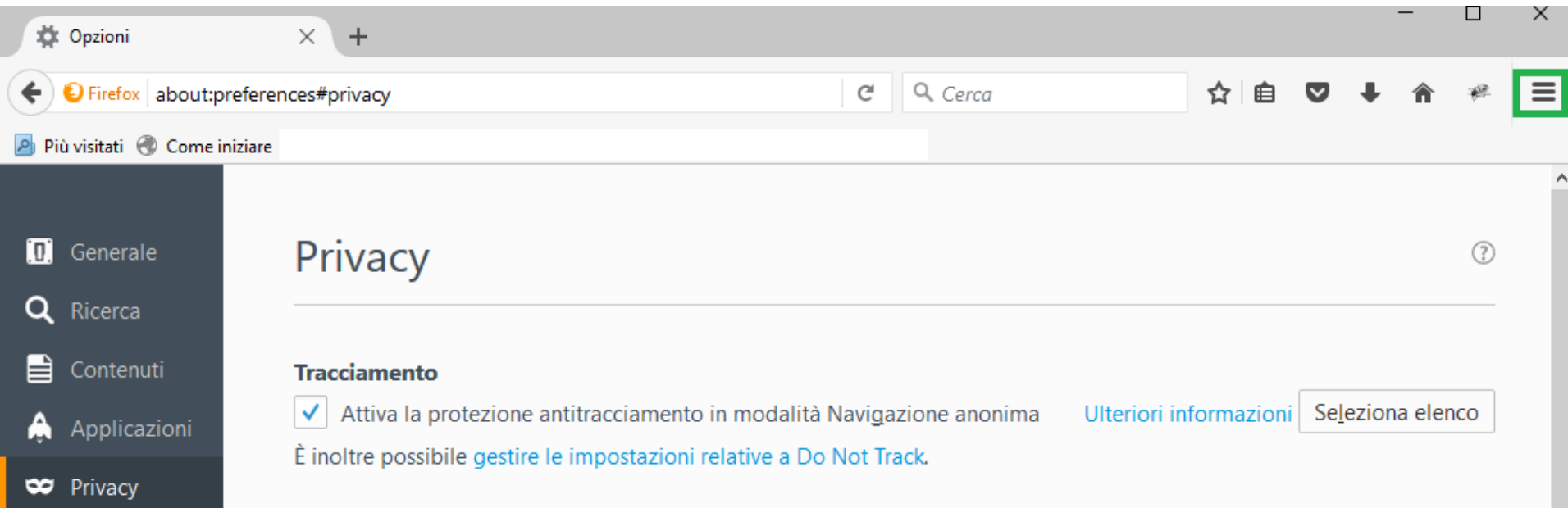
**Il contenuto del messaggio
può essere letto soltanto dal
destinatario (proprietà banale)**

**Può anche essere desiderabile
la segretezza del fatto stesso che
sia avvenuta una comunicazione
tra due persone (proprietà meno
ovvia)**



Tracciabilità o
anonimato ?

navigare in incognito



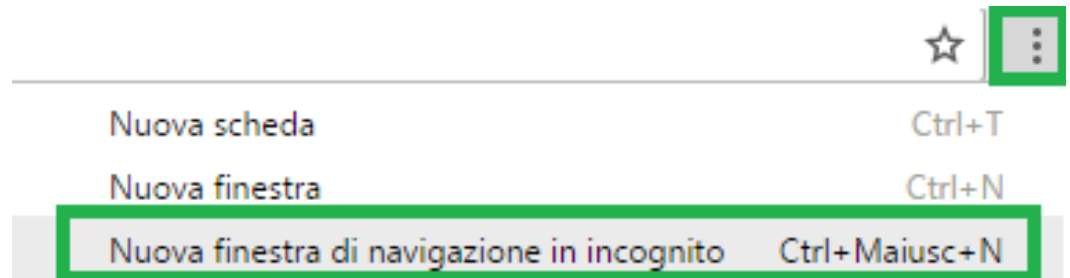
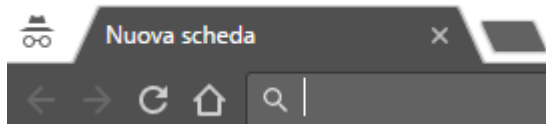
The screenshot shows the Firefox browser interface with the 'Privacy' settings page open. The address bar shows 'about:preferences#privacy'. The left sidebar contains menu items: 'Opzioni', 'Generale', 'Ricerca', 'Contenuti', 'Applicazioni', and 'Privacy'. The main content area is titled 'Privacy' and features a section for 'Tracciamento' (Tracking) with a checked checkbox for 'Attiva la protezione antitracciamento in modalità Navigazione anonima' (Activate anti-tracking protection in Private Browsing mode). A button labeled 'Seleziona elenco' (Select list) is visible next to the checkbox. Below the checkbox, there is a link to 'Ulteriori informazioni' (More information) and a note: 'È inoltre possibile gestire le impostazioni relative a Do Not Track.' (It is also possible to manage settings related to Do Not Track.)

Navigazione
in incognito



Navigazione
anonima

Chrome: basta un click

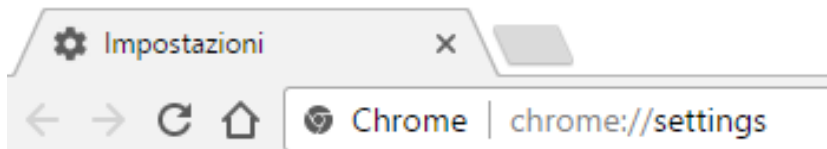
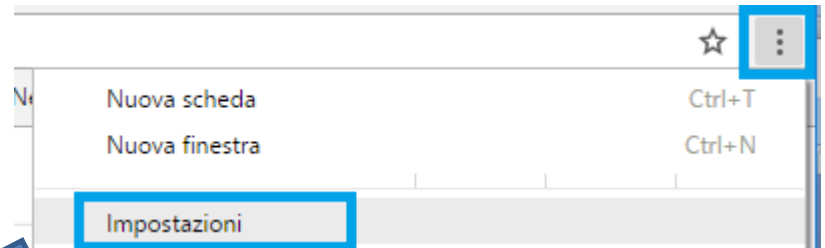


Sei passato alla navigazione in incognito

Le pagine visualizzate nelle schede in incognito non vengono memorizzate nella cronologia del browser, nell'archivio di cookie o nella cronologia delle ricerche dopo avere chiuso tutte le schede in incognito. I file scaricati o i preferiti creati verranno conservati.

Non sei completamente invisibile: se navighi in incognito, la tua navigazione non viene nascosta al tuo datore di lavoro, al provider di servizi Internet o ai siti web che visiti.

Privacy e certificati ...



Permette di visualizzare
impostazioni avanzate
e personalizzare **opzioni di Privacy**

Privacy

Impostazioni contenuti...

Cancella dati di navigazione...

Google Chrome potrebbe utilizzare servizi web per migliorare la navigazione. Puoi disattivare questi servizi. [Ulteriori informazioni](#)

Invia una richiesta "Non tenere traccia" con il tuo traffico di navigazione

Impostazioni

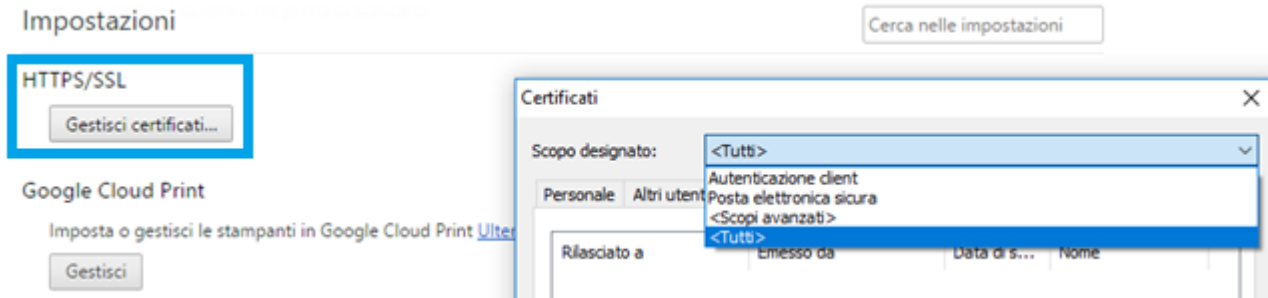
HTTPS/SSL

Gestisci certificati...

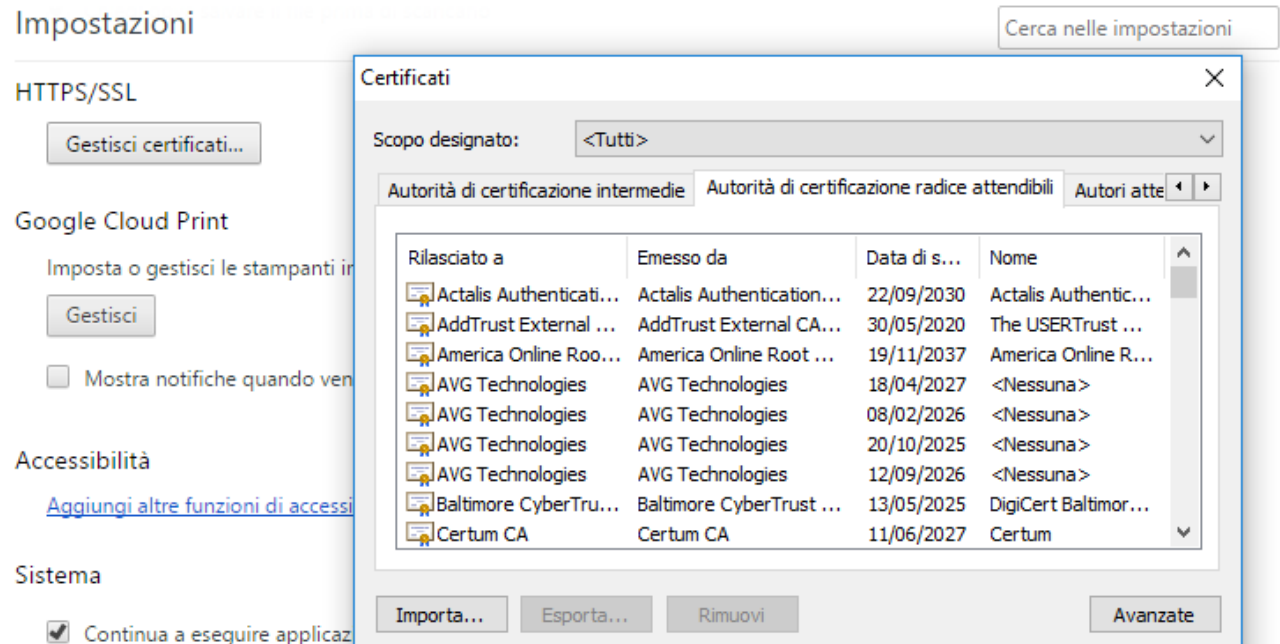
oppure personalizzare
opzioni di gestione certificati

Si può, a seconda dello **scopo**

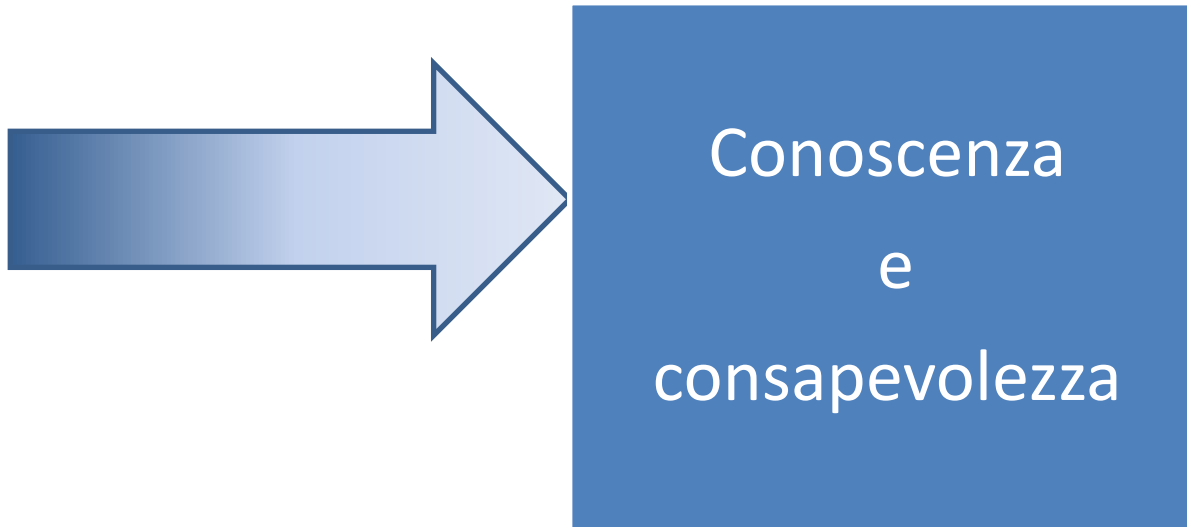
... certificati



importare/esportare **certificati personali**
o di **diverse Autorità di certificazione** o **Autori**



... per prevenire

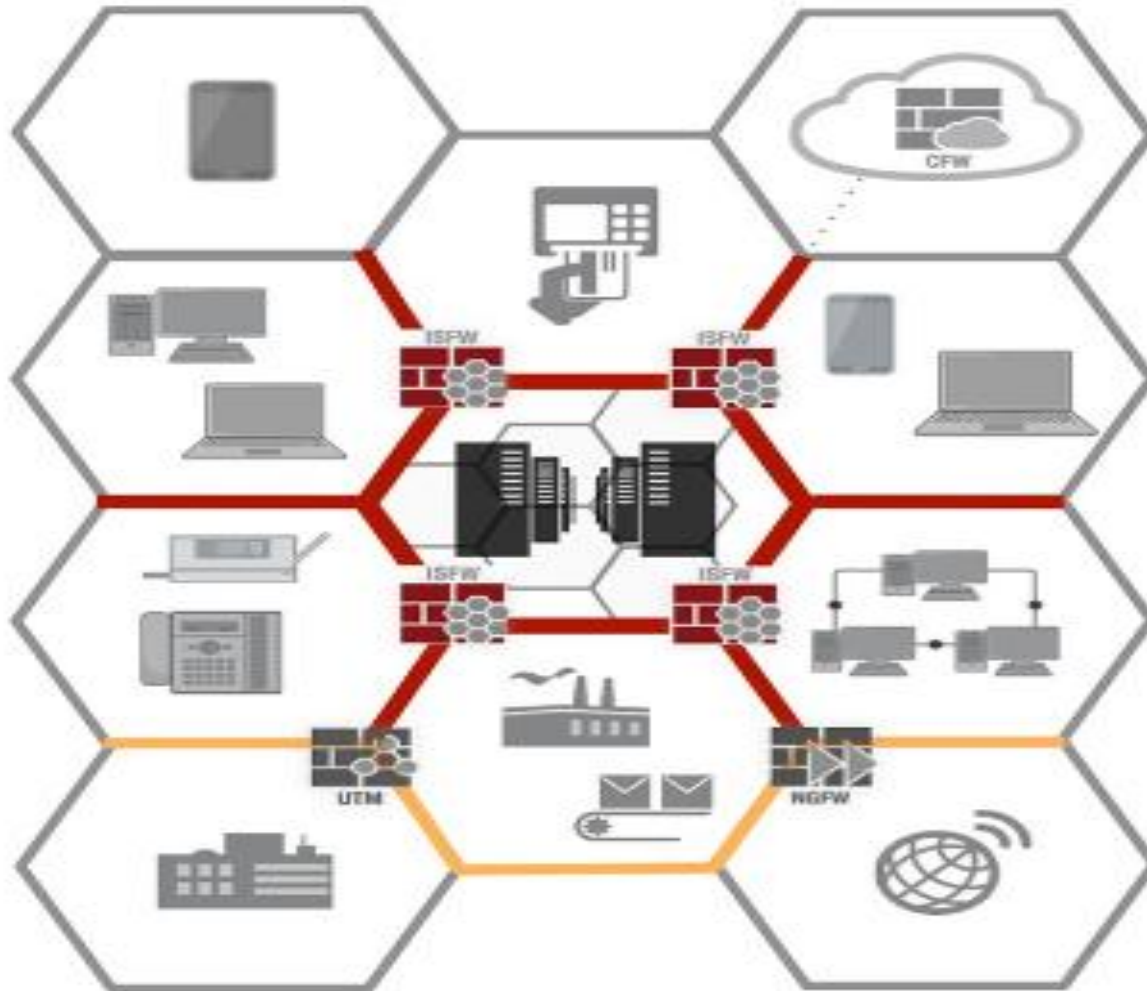


Apparati e sistemi di sicurezza di rete

Strumenti crittografici ← scambio dati sicuro

Apparati e sistemi di sicurezza di rete

Internal Segmentation Firewall (*ISFW*)



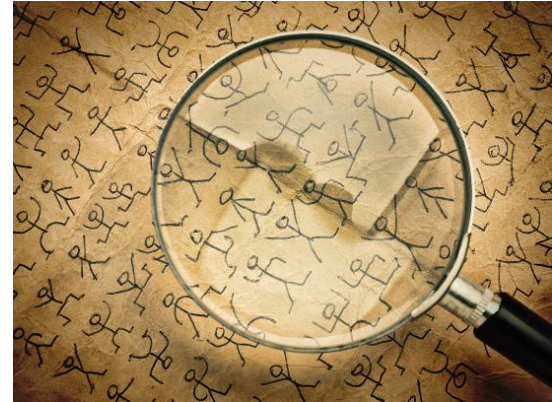
[Firewall, IDS, IPS](#)

Virtual Private Network



[VPN: slide](#)

Crittografia, Firma Digitale e Certificati



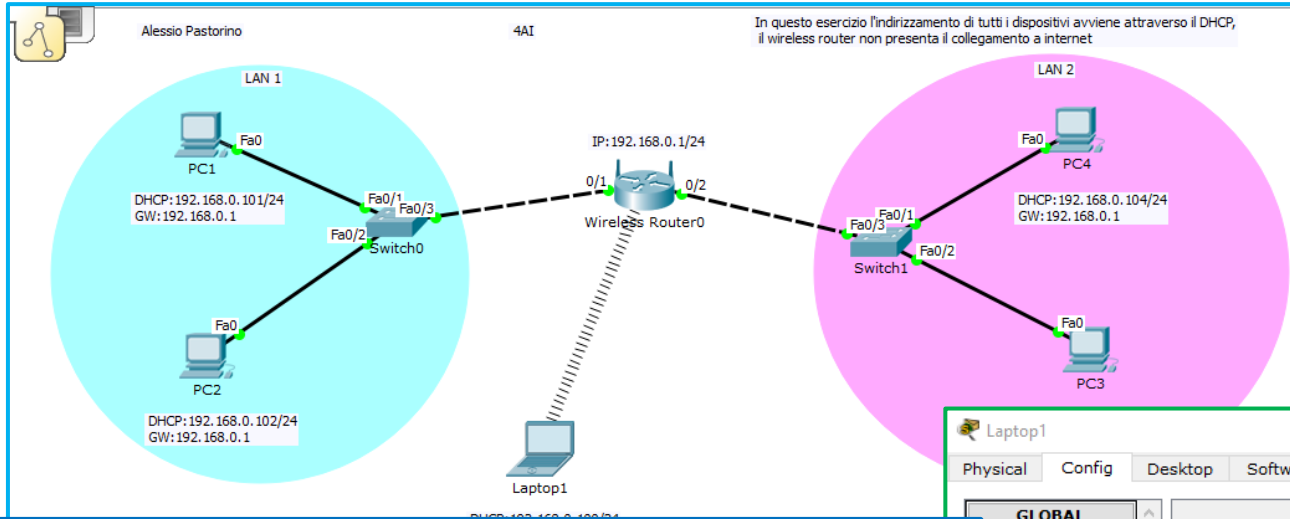
[Slide](#) e [pagina](#) di navigazione

Sicurezza nelle Reti Mobili

Le trasmissioni d'informazioni via etere sono più soggette a problematiche di sicurezza rispetto a quelle che usano il cavo come mezzo fisico. Ascoltare le comunicazioni su una tratta radio può essere, in alcuni casi, abbastanza semplice e non richiede l'accesso a particolari posizioni fisiche.



Esempio in Packet Tracer



da presentazione
alunno 4AI

Wireless Router0

Physical Config GUI

GLOBAL

Settings

Algorithm Settings

INTERFACE

Internet

LAN

Wireless

Wireless Settings

SSID: Default

Channel: 6

Authentication

Disabled WEP WEP Key

WPA-PSK WPA2-PSK PSK Pass Phrase: devopassare

WPA WPA2

RADIUS Server Settings

IP Address

Shared Secret

Encryption Type: AES

Laptop1

Physical Config Desktop Software/Services

Wireless0

Port Status: On

Bandwidth: 54 Mbps

MAC Address: 00D0.BC85.929D

SSID: Default

Authentication

Disabled WEP WEP Key

WPA-PSK WPA2-PSK PSK Pass Phrase: devopassare

WPA WPA2

User ID

Password

Encryption Type: AES

IP Configuration

DHCP

Static

IP Address: 192.168.0.100

Subnet Mask: 255.255.255.0

IPv6 Configuration

DHCP

Auto Config

Static