Sicurezza informatica

…. di cosa abbiamo parlato

… e possibili percorsi

***pagina* di navigazione**

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

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

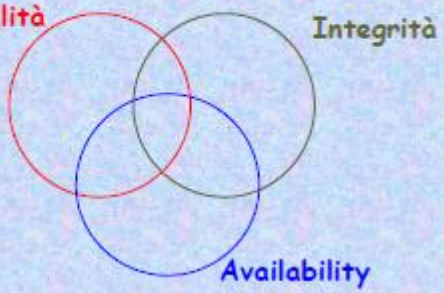
Availability

Risorse disponibili a chi è autorizzato quando necessario

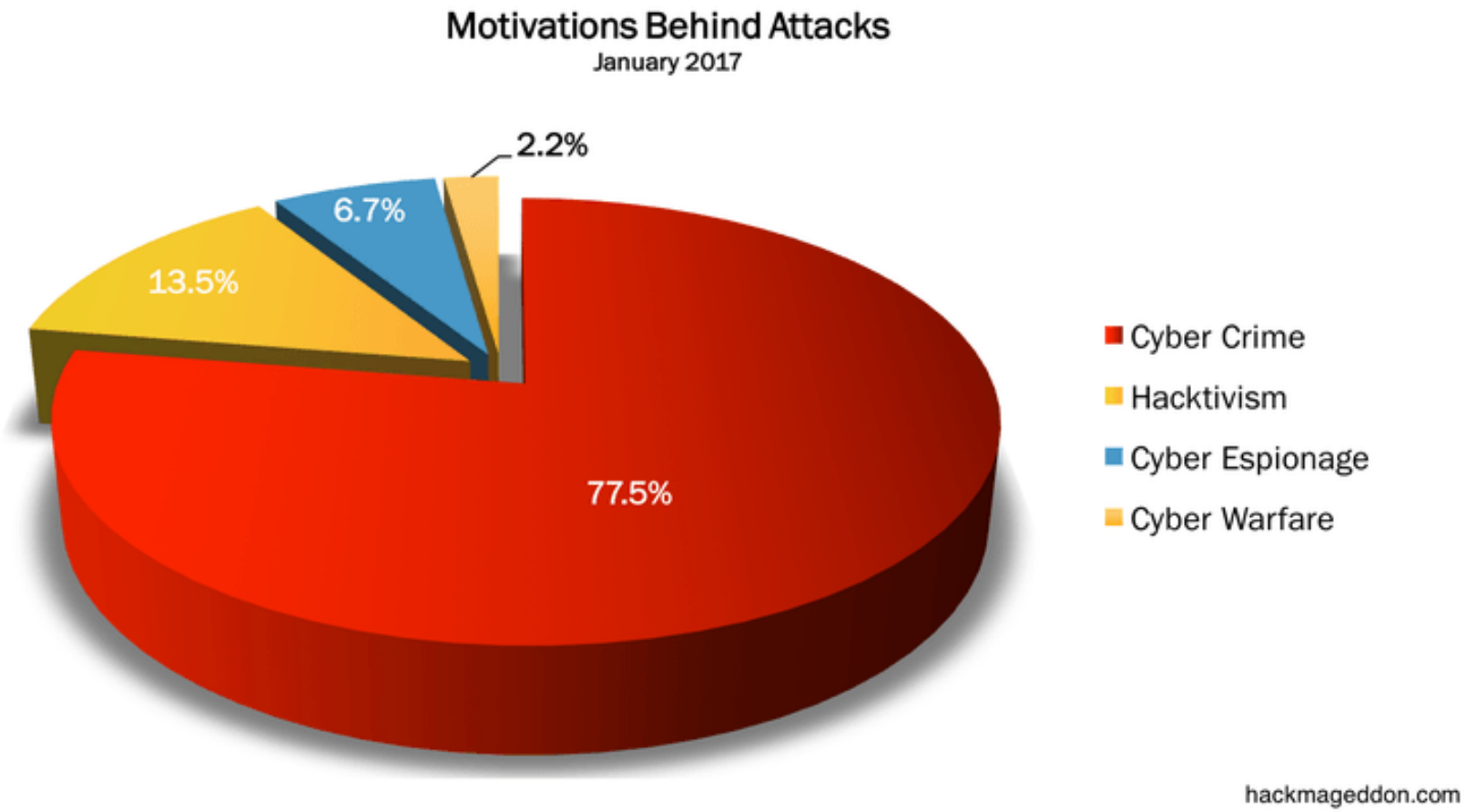
Diverse attese:
- presenza di oggetti e servizi utilizzabili
- capacità di soddisfare le richieste di servizi
- progresso: tempo di attesa limitato
- adeguato tempo del servizio

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

Alcune relazioni



Il mercato della cyber-security



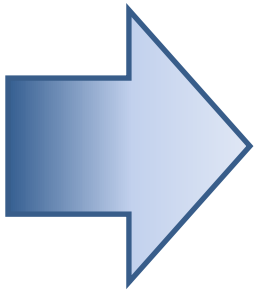
dalle slides del Dott. Enrico Cambiaso

Vecchie tecniche di attacco con scopi diversi

Ransomware (*tecnicamente "trojan" tipo worm*)

Sicurezza per chi ?

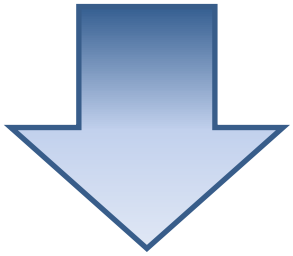
- Utenti (persone)
- Apparati dell'infrastruttura di rete (es. server DNS, router, ecc.)
- Falle nella sicurezza dell'infrastruttura possono essere veicolo di attacchi alle attività degli utenti



Sicurezza richiede compromessi

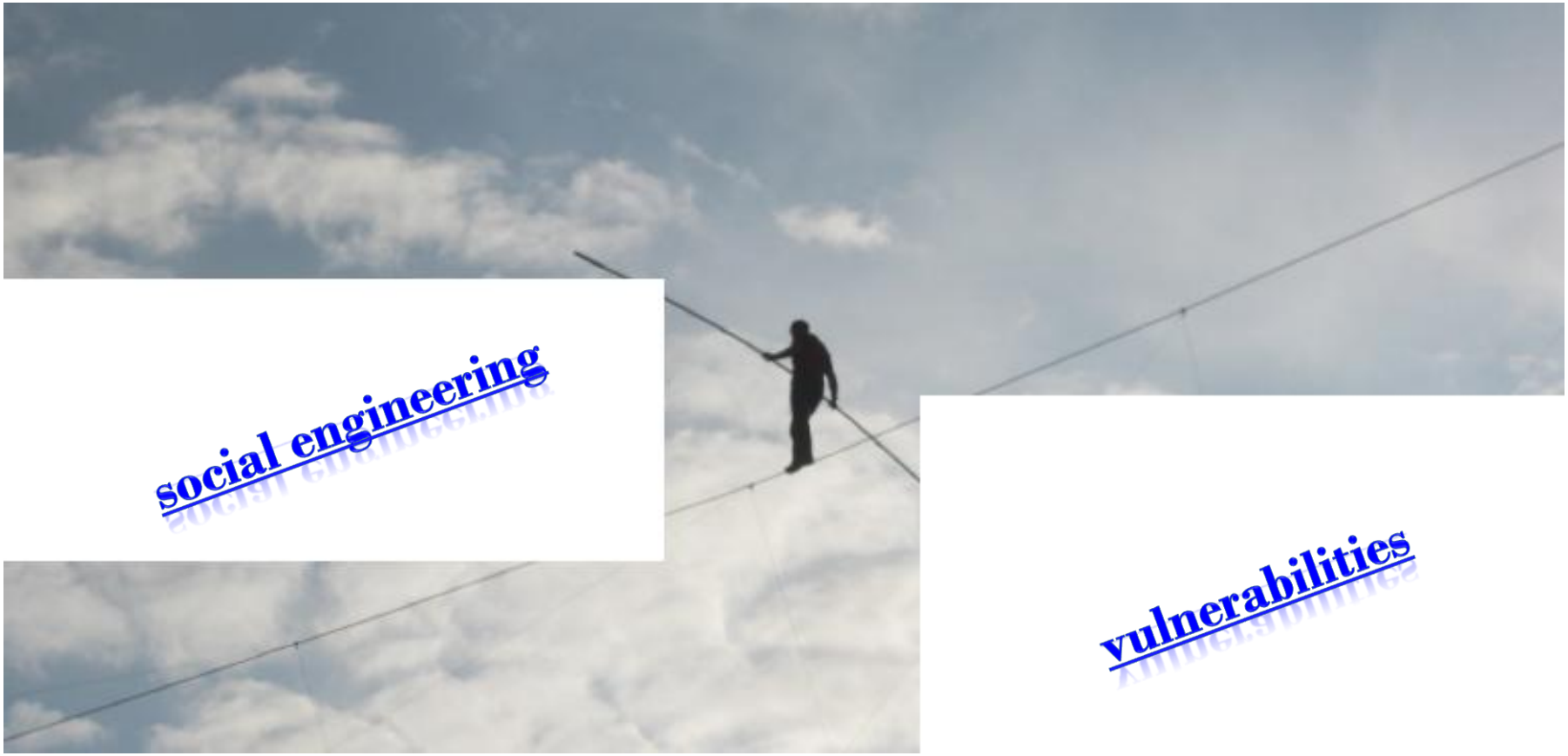
La Sicurezza richiede compromessi

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



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

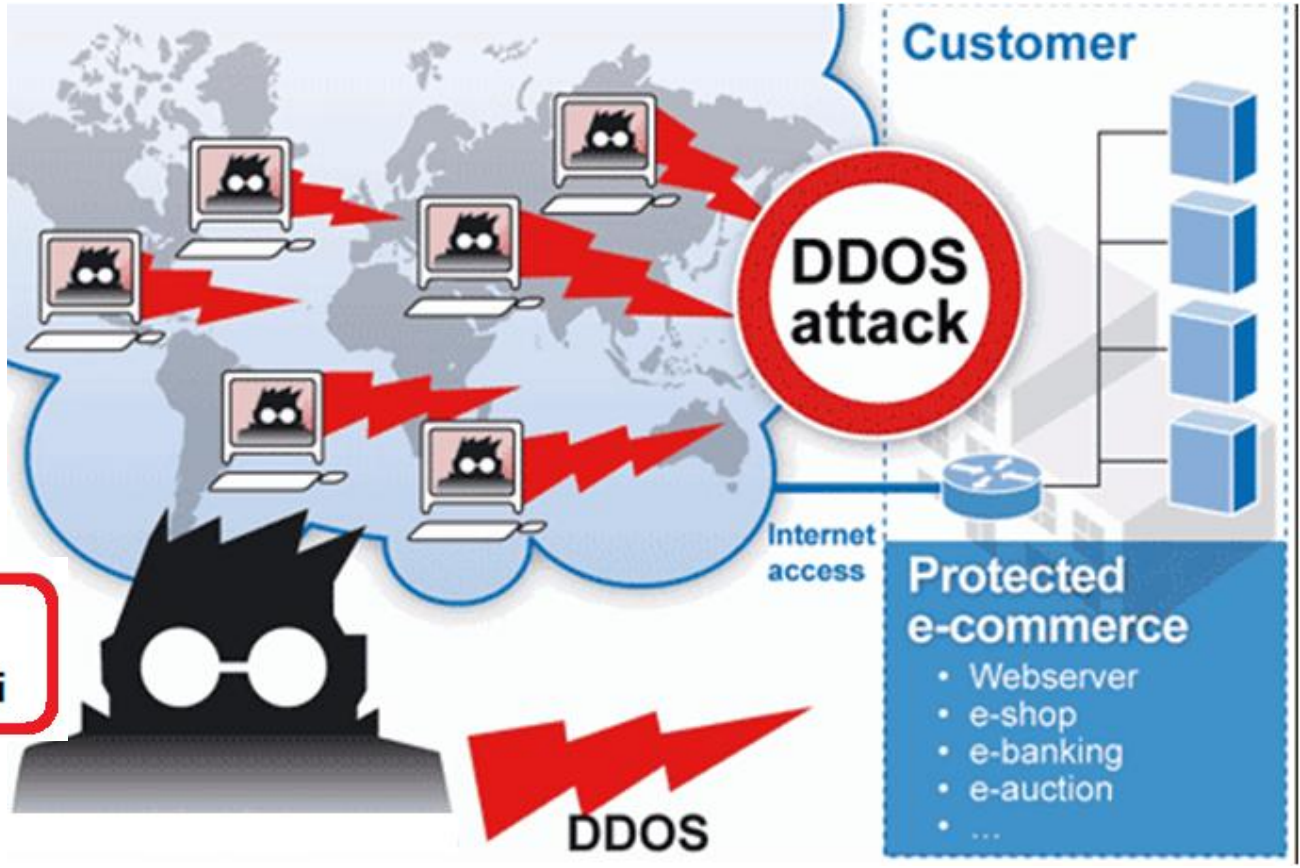
posso fidarmi di chi ha sviluppato il software?

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



Attacchi orientati ad impedire il normale funzionamento dei sistemi

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"

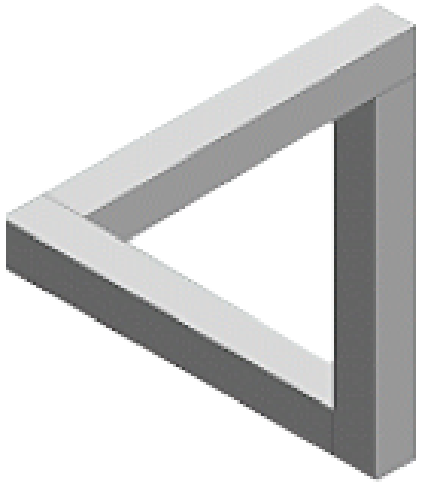
Il risultato prima di tutto

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, sofware, 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

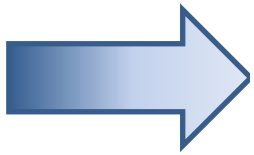
posso fidarmi

dell' IoT

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

Progettare la sicurezza

Non solo tecnologia, ma metodologia e gestione



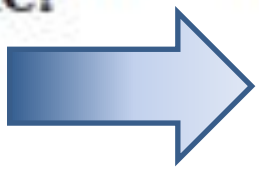
Security Manager

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

Attenzione ai servizi non richiesti e non strettamente indispensabili

Sistemisti: massima attenzione all'utente!

Utenti



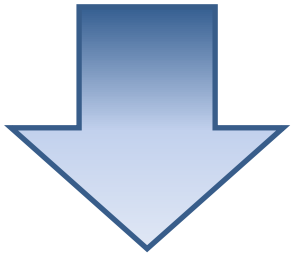
Fiducia

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 sistrma operativo"

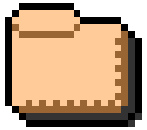
- Servono
  - architetture intrinsecamente sicure (sarà realmente possibile?)
  - serie politiche di migrazione/aggiornamento

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)

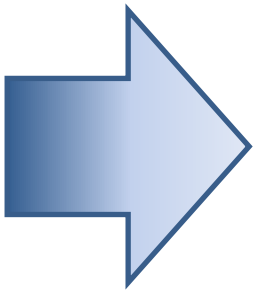
Dalle slide del prof. Montessoro – Università degli Studi di Udine

00_Conoscenza_e_consapevolezza.pdf

Confidenzialità e tracciabilità

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

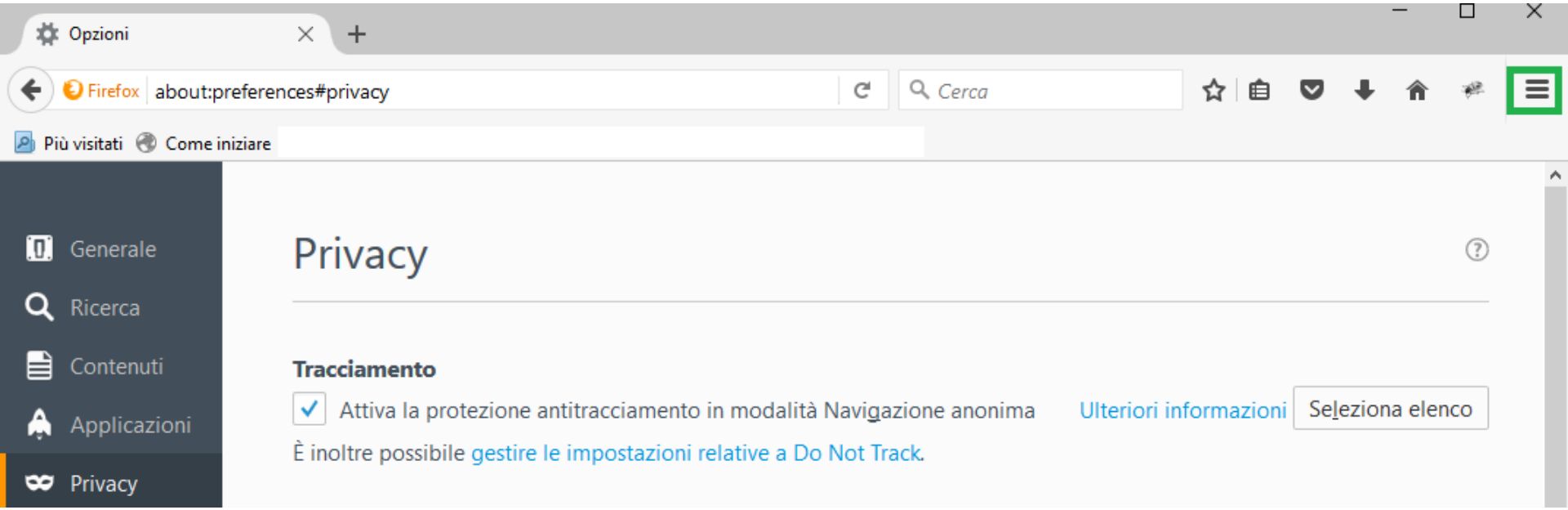
Può anche essere desiderabile la segretezza del fatto stesso che sia avvenuta una comunicazione tra due persone (proprietà meno ovvia)



Tracciabilità o anonimato ?

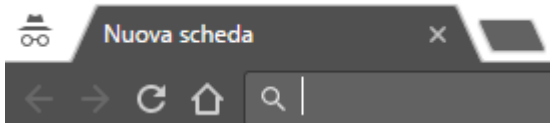
navigare in incognito

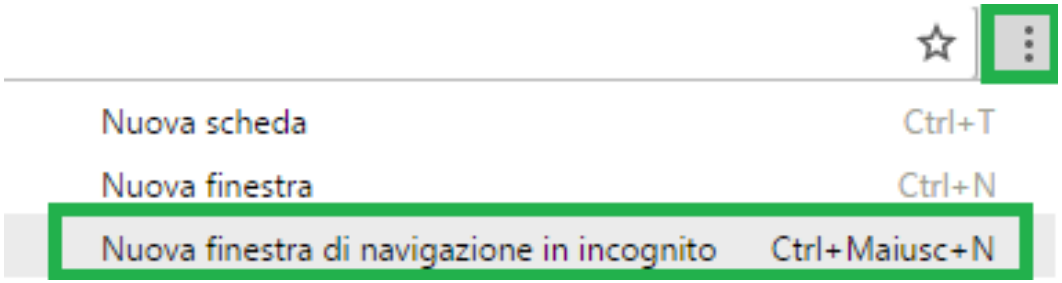
Firefox



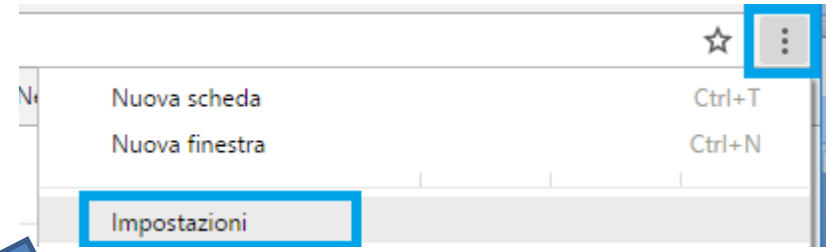
Navigazione in incognito ≠ **Navigazione anonima**

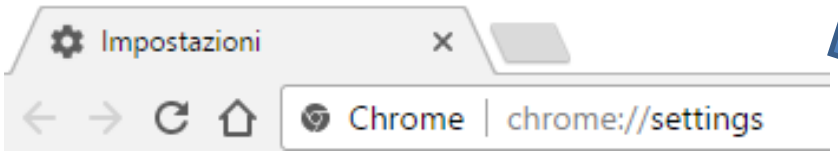
Chrome: basta un click



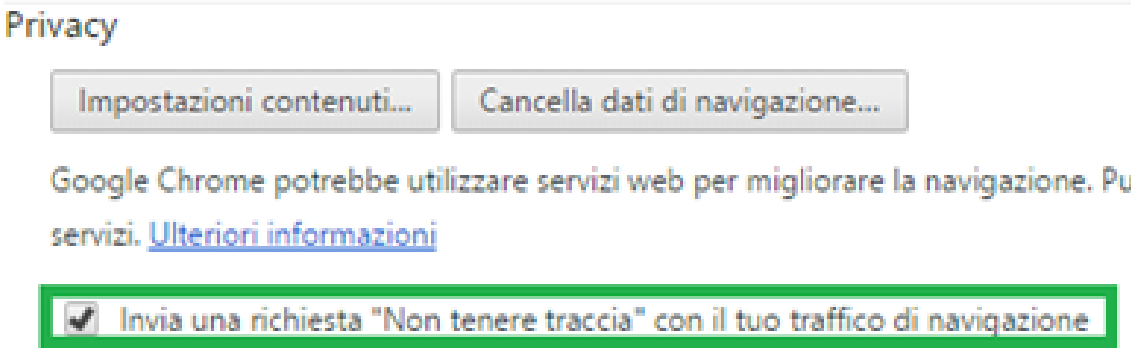


Privacy
e certificati …

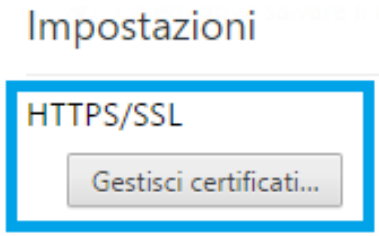




Permette di visualizzare
impostazioni avanzate
e personalizzare **opzioni di Privacy**

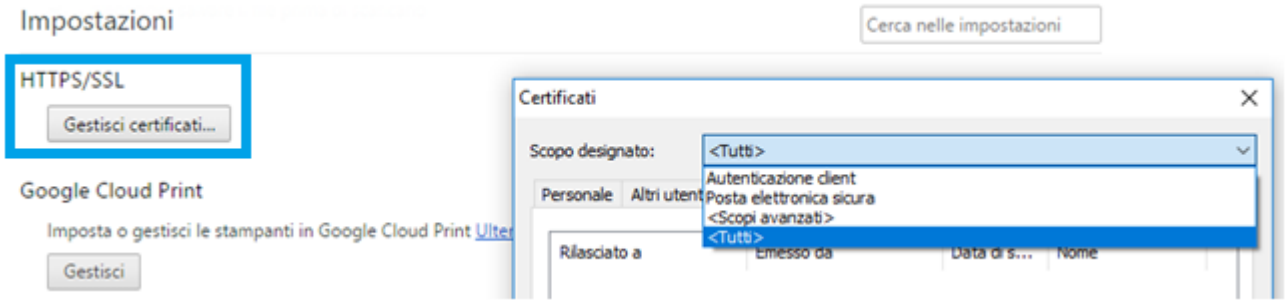


oppure personalizzare
opzioni di gestione certificati

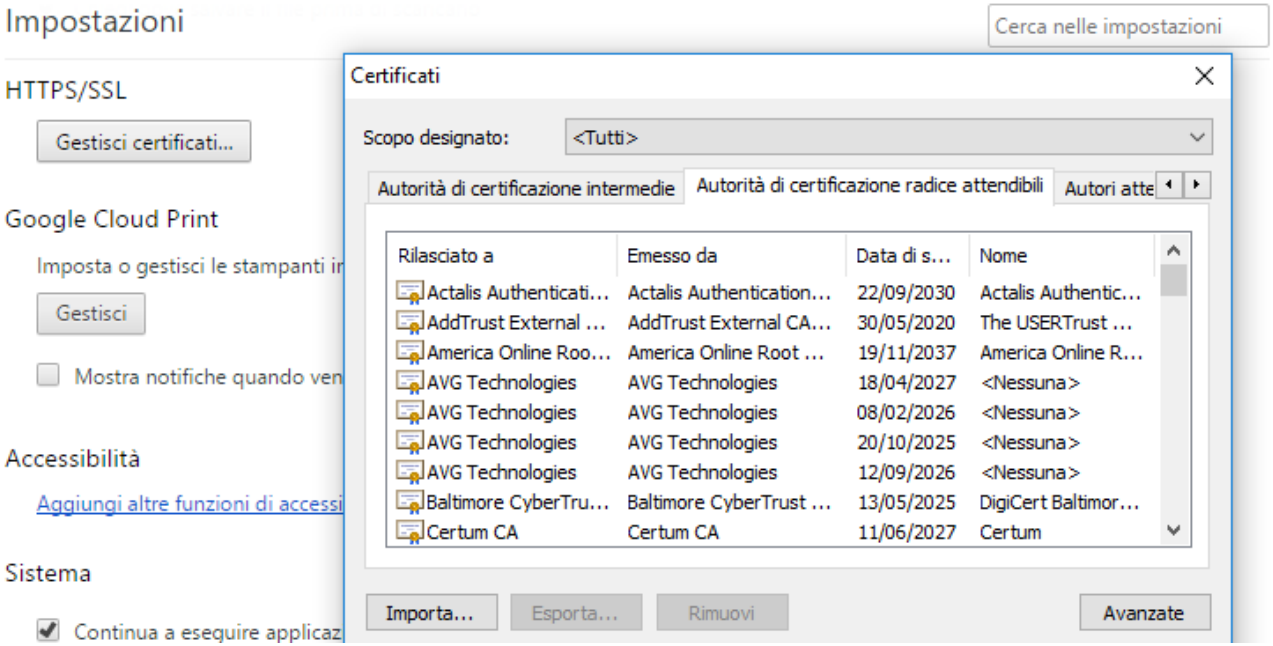


Si può, a seconda dello **scopo**

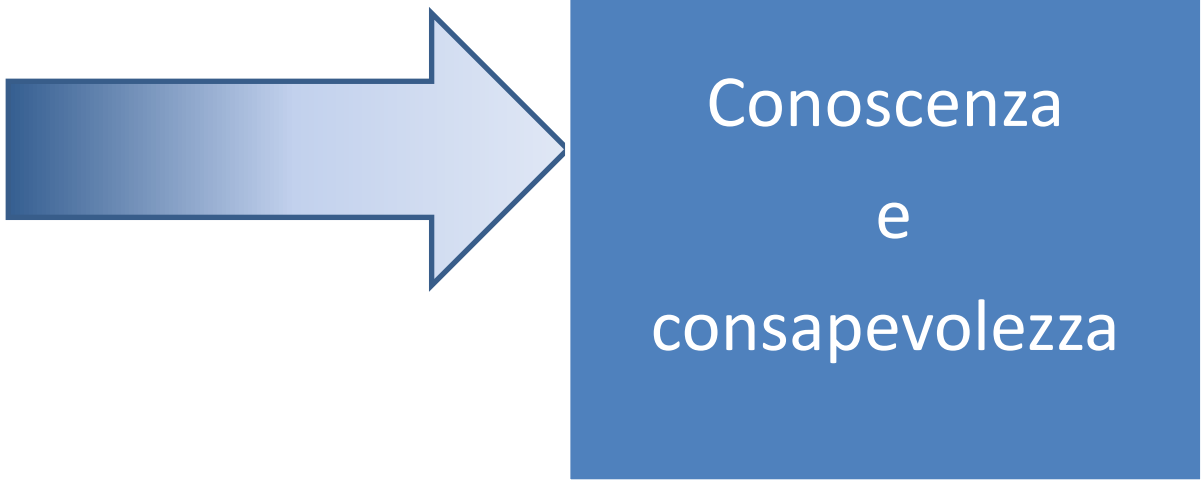
… certificati



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



… per prevenire

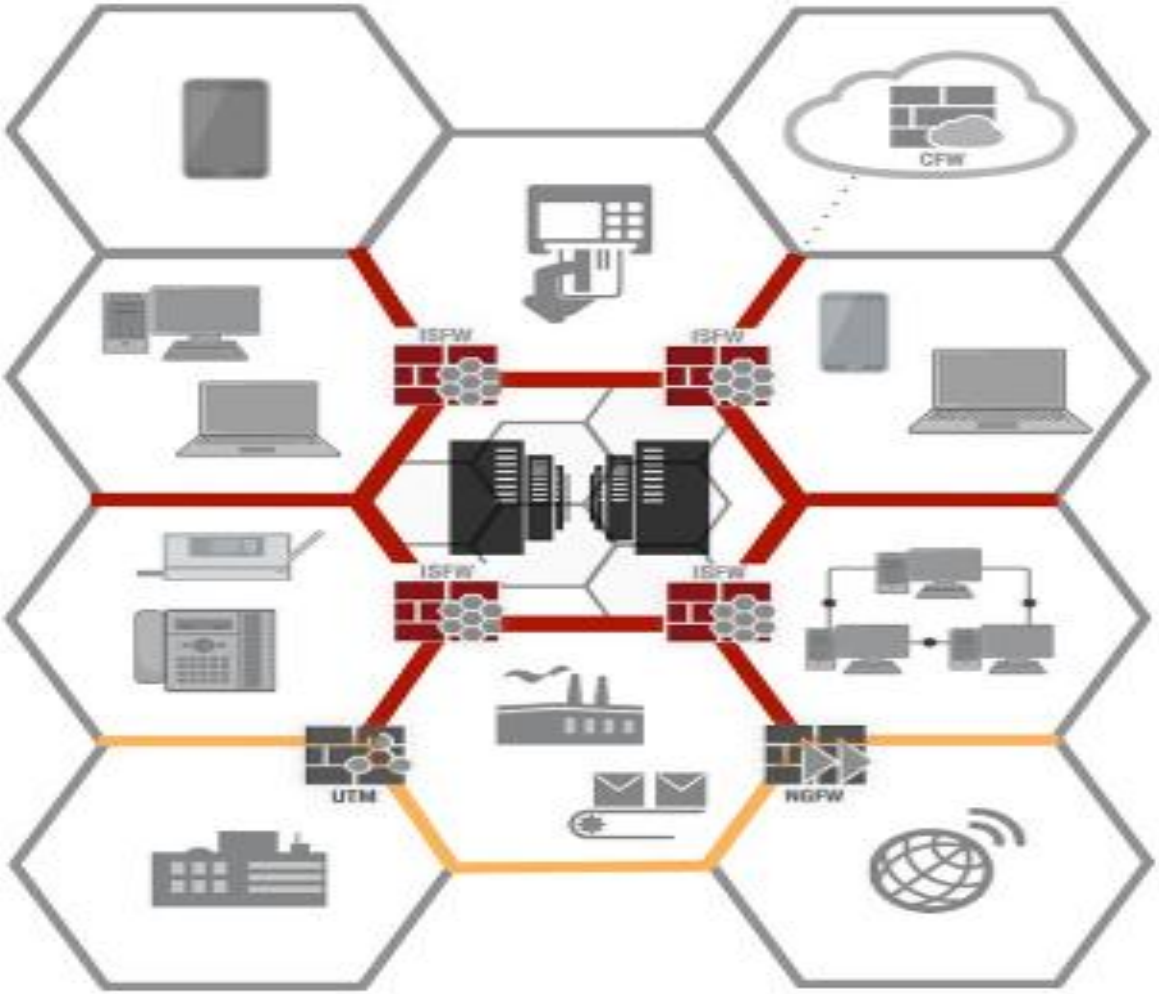


Apparati e sistemi di sicurezza di rete

Strumenti crittografici ←scambio dati sicuro

Apparati e sistemi di sicurezza di rete

Internal Segmentation Firewall (***ISFW)***

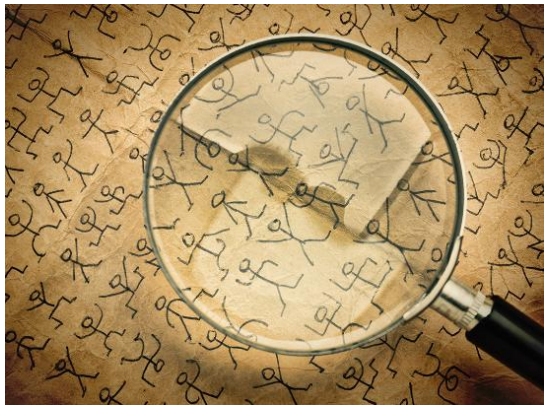


Firewall, IDS, IPS

Virtual Private Network

VPN: slide

Crittografia, Firma Digitale e Certificati

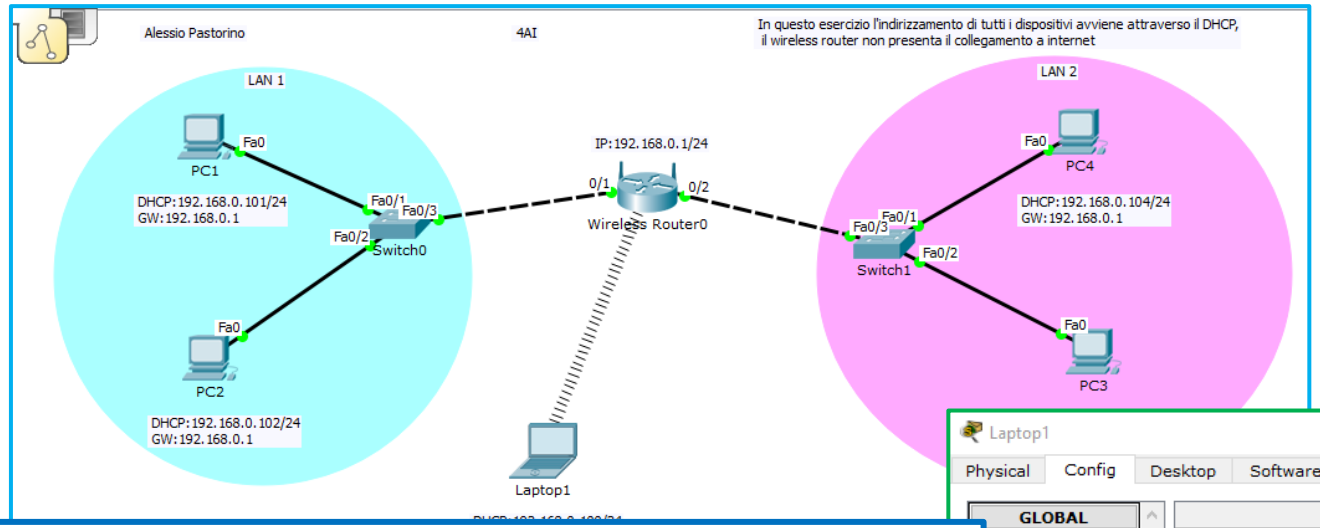


Slide e pagina di navigazione

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]