



CYBERSECURITY e INDUSTRIA 4.0

I punti deboli di una rete aziendale e le possibili contromisure

Prof. Gian Luca FORESTI

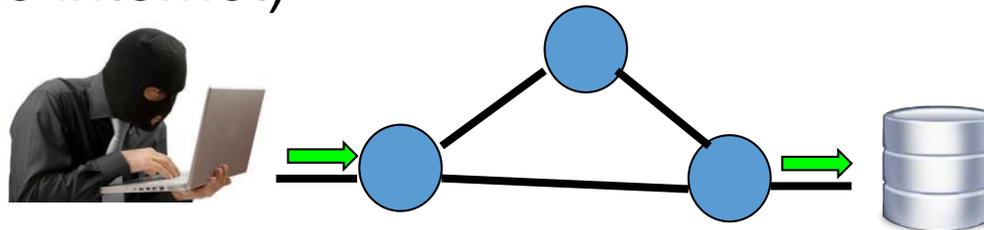
Dipartimento di Scienze Matematiche, Informatiche e Fisiche (DMIF)

Università di Udine



- **Cybersecurity** – Proteggere informazioni e risorse dall'accesso / alterazione / cancellazione da parte di soggetti non autorizzati
- **Cybersecurity nelle applicazioni aziendali** significa affrontare le problematiche di
 - Sicurezza nella memorizzazione dei dati (file testo/audio/immagini/video)
 - Sicurezza nella trasmissione dei dati (all'interno della rete aziendale o da/verso l'esterno - rete internet)

Utente
Agente SW



Server aziendale

Cybersecurity – Elementi chiave



- Identificazione e autenticazione
- Autorizzazione
- Disponibilità



Memorizzazione/gestione
sicura dei dati su sistemi
aziendali

Cybersecurity – Elementi chiave (2)



- Riservatezza
- Integrità
- Paternità



Trasmissione dati su
canali non sicuri



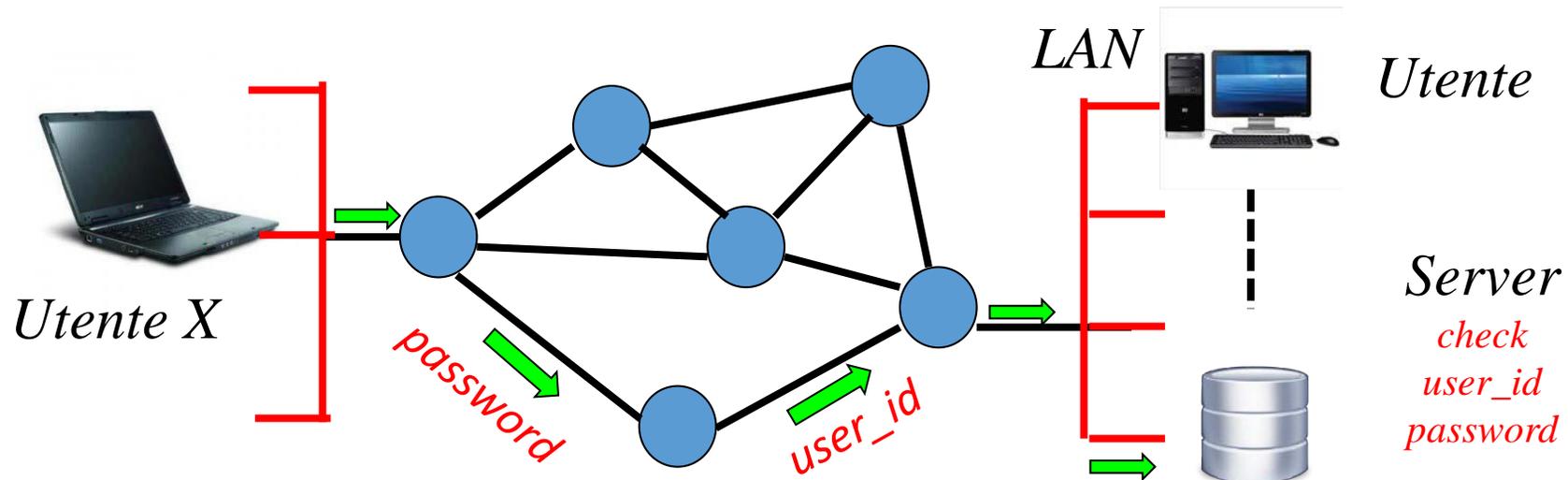
Identificazione e autenticazione



- Processo di acquisizione dei dati per identificare un utente (e.g., **login**, indirizzo e-mail, etc.) e **verificarne l'identità** (e.g., **password**)

Identificazione: risponde alla domanda "Chi sei?"

Autenticazione: risponde alla domanda "Come puoi dimostrare di essere davvero tu?"



Tecniche di autenticazione - Password



- **Something You Know**
(pin, password,...)



- Fondamentale utilizzare **password** non banali
- Una password con otto caratteri casuali con maiuscole, minuscole, cifre e un paio di segni di interpunzione (**difficile da ricordare !!!**)

10^{14} possibili password diverse



Provando 1.4×10^{10} password/sec sono necessarie
circa 2 ore

Tecniche di autenticazione – Password (2)

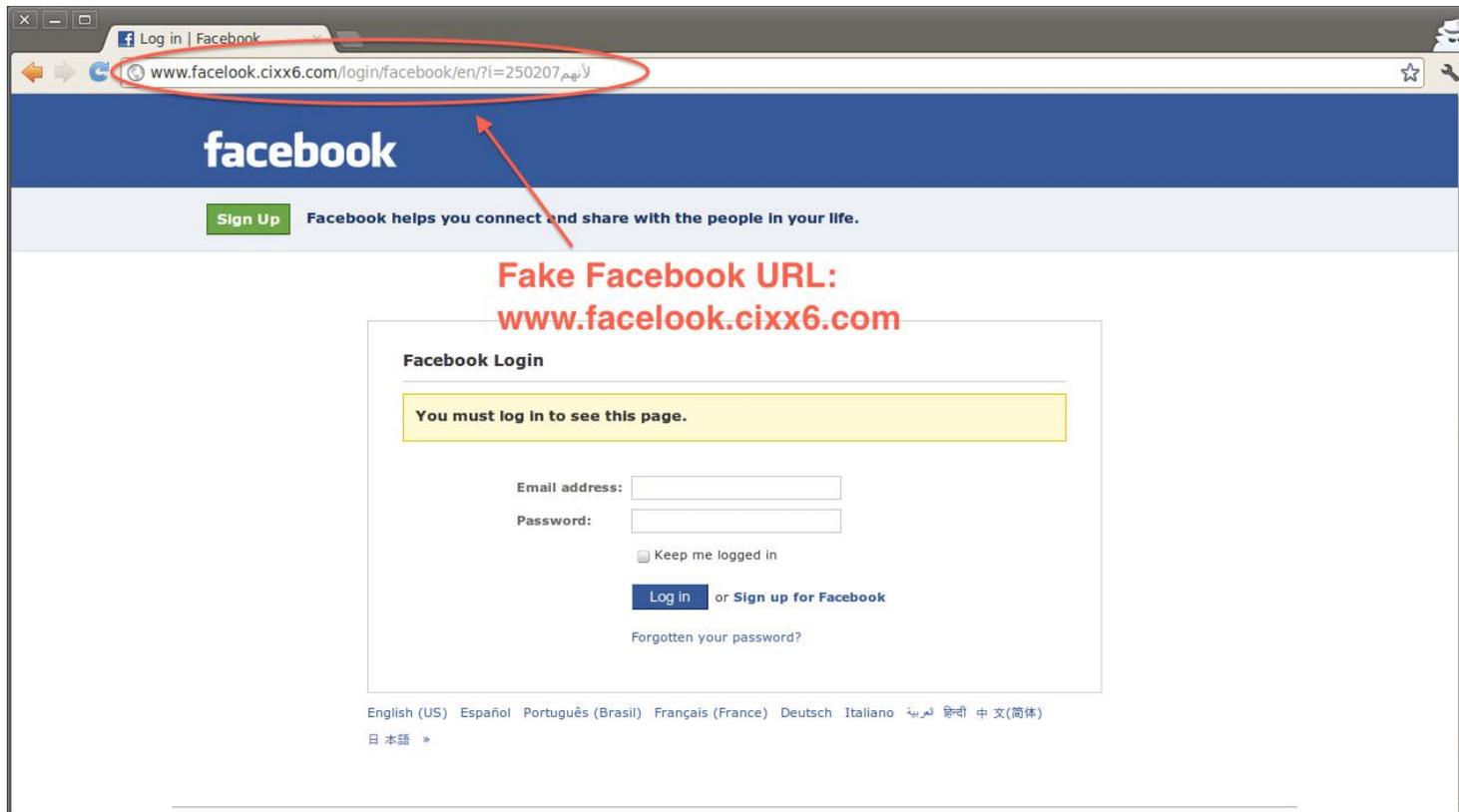


Pattern	Calculation	Result	Time to Guess (2.6×10^{18} tries/month)
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	26^4	5×10^5	
8 chars: lower case alpha	26^8	2×10^{11}	
8 chars: alpha	52^8	5×10^{13}	
8 chars: alphanumeric	62^8	2×10^{14}	3.4 min.
8 chars alphanumeric +10	72^8	7×10^{14}	12 min.
8 chars: all keyboard	95^8	7×10^{15}	2 hours
12 chars: alphanumeric	62^{12}	3×10^{21}	96 years
12 chars: alphanumeric + 10	72^{12}	2×10^{22}	500 years
12 chars: all keyboard	95^{12}	5×10^{23}	
16 chars: alphanumeric	62^{16}	5×10^{28}	

Furto delle password



- **Phishing:** Un possibile attaccante convince il dipendente ad inserire la propria password su un sito *fasullo*



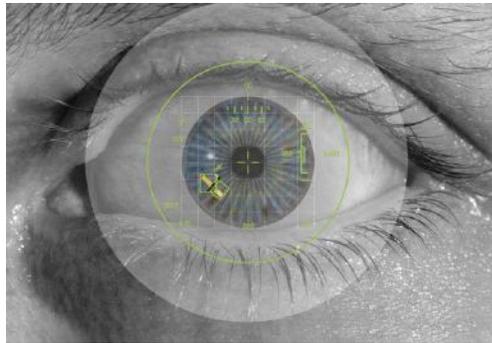
2018 – 140 milioni di attacchi di phishing nel mondo

2018 – Germania, Russia, Inghilterra, Italia (4 posto)

Tecniche di autenticazione - Biometria



- **Something You Are** (biometria: impronte digitali, iris/retina,...)



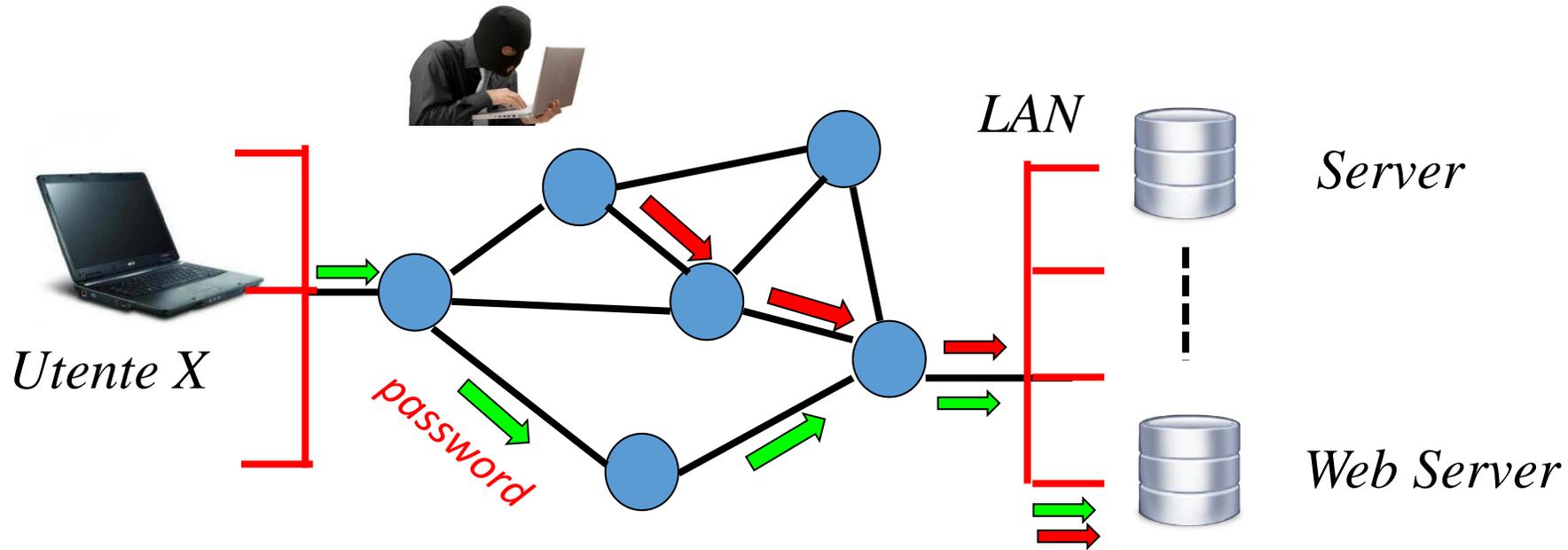
- **Something You Have**
(badge, smart card,...)



Autorizzazione e disponibilità



- Una volta che un utente è stato autenticato, la fase di autorizzazione specifica cosa quell'utente può fare

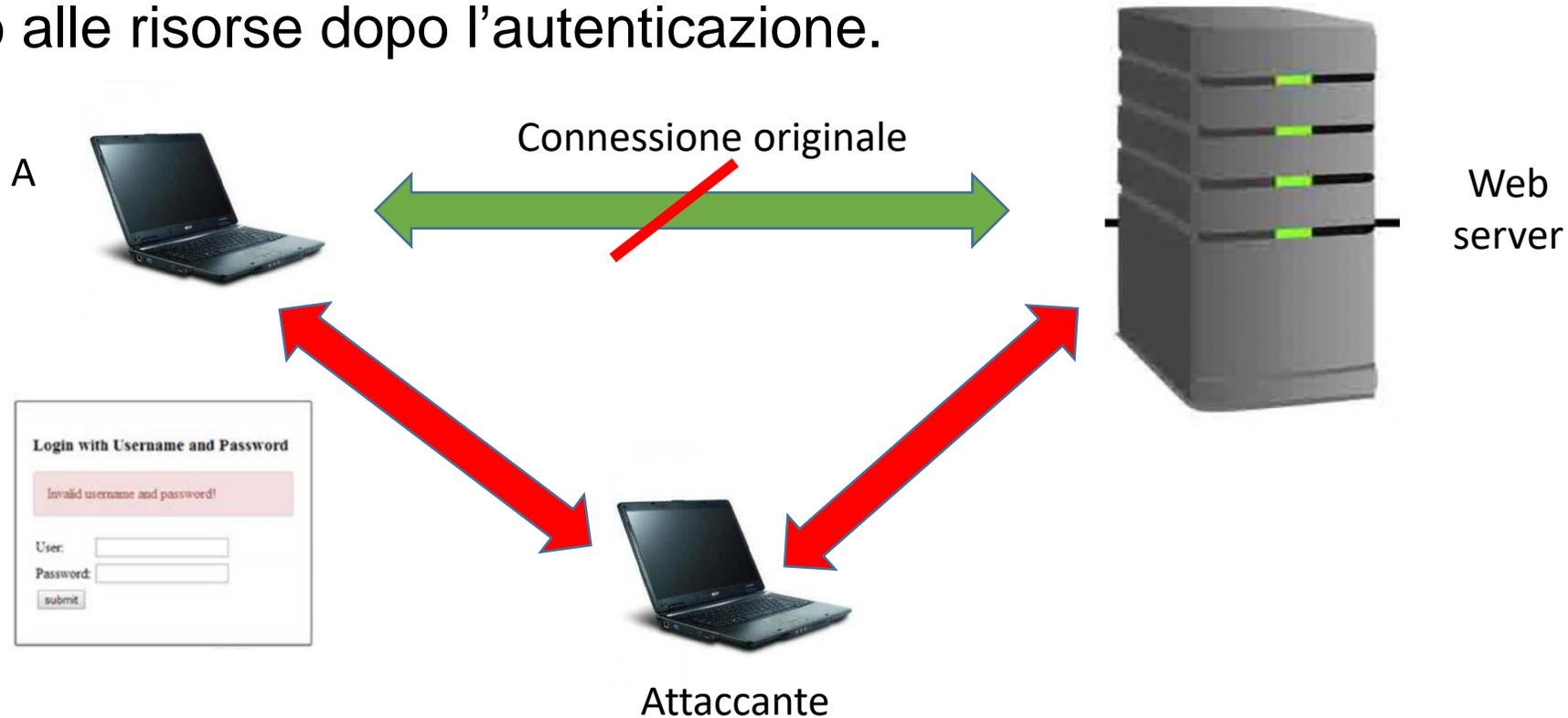


- Gli attacchi **DoS** (**Denial of service**) sono volti a limitare la disponibilità di una data risorsa.

Attacco Man-in-the-middle



- **Furto sessione TCP:** Un possibile attaccante (entrato nella rete con un altro account) dirotta il traffico dell'utente X in modo da ottenere l'accesso alle risorse dopo l'autenticazione.



SW HCI ingannevole - Come proteggersi?



False schermate di accesso

Guardia di Finanza
insieme per la legalità

Attenzione!!!

È stata rivelata un'attività illegale. Il sistema operativo è stata bloccata per una violazione delle leggi della Repubblica Italiana!
È stata fissata una seguente violazione: Dal tuo indirizzo IP **www.freedivx.it** era eseguito un accesso alle web-pagine contenenti la pornografia, la pornografia minorile, zoofilia, nonché la violenza dei bambini. Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile.
**Dalla posta elettronica era effettuato anche la distribuzione dello spam con un senso recondito terroristico.
Il bloccaggio di computer serve per troncane l'attività illegale dalla parte tua.**

I tuoi dati: **IP: www.freedivx.it**
Posizione: Italy
ISP:

Per togliere il bloccaggio devi pagare una multa di 100 euro.
Hai due seguenti varianti di pagamento:

1) Effettuare il pagamento tramite l'Ukash.
Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK).

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica deposito@cyber-gdf.net.

2) Effettuare il pagamento tramite il Paysafecard:
Per questo inserisci per favore il numero ricevuto (nel caso di necessità insieme con la password) nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK).

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica deposito@cyber-gdf.net.

Ukash Dove passo trovare Ukash?
Puoi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, stazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di terminale **Epay, Epipoli**.

Recati presso il punto vendita dotato di terminale **Epay, Epipoli** a te più vicino. Richiedi un voucher in contanti al negoziante. Il negoziante dovrà stampare e consegnarti un voucher Ukash con codice PIN da 19 cifre.

epay **epipoli**
relationships marketing group

paysafecard
pay cash. pay safe.

www.freedivx.it

L'utente
conosce il
software/sito
web e quindi
pensa che sia
affidabile

SW HCI ingannevole - Come proteggersi?



Avere un sistema per rendere sicuri gli schermi di login (chiave, immagine o frase personalizzata)

Antivirus (anche se difficilmente potrà individuare attacchi personalizzati su misura)

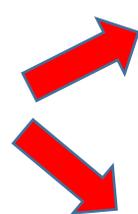


Malware (Virus)



- Programma (parte di SW) in grado di compiere azioni illecite in un computer/rete

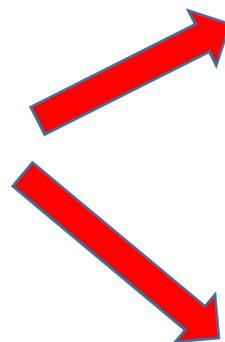
Azioni di un malware



Modificare dati, trasmettere dati, ...

Infettare altri programmi/PC

Come si diffonde il malware?



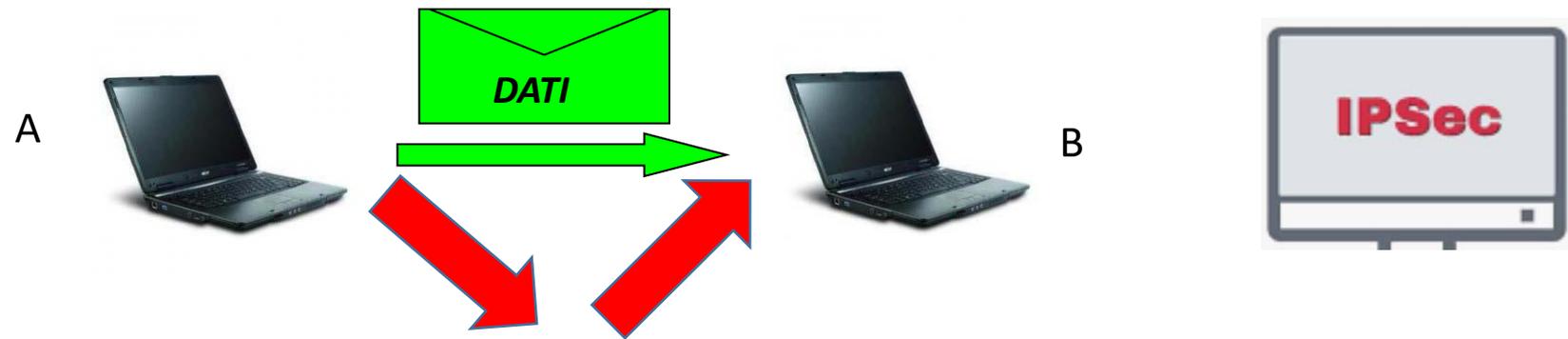
Exploit (“sfruttare”) - **Errori nel codice del sistema operativo** (o altre app)

Utenti che eseguono codice non sicuro (attach alle email o programmi scaricati dalla rete)

Riservatezza



- Nelle comunicazioni aziendali si deve garantire che nessun altro possa intercettare i dati/informazioni (**attacco PASSIVO**)
- Contromisure: **Tecniche di crittografia**



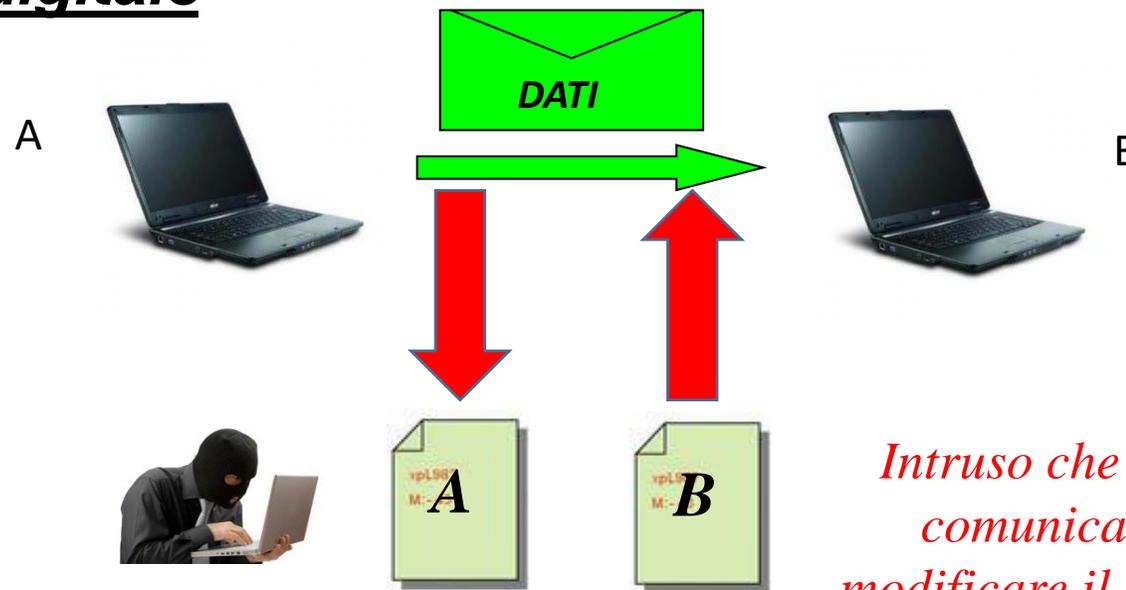
Intruso, se anche riesce ad intercettare il messaggio, non può leggerne il contenuto

**Uso di protocolli sicuri per le app aziendali:
IPSec, Https, etc.**

Integrità



- Le informazioni/dati aziendali non devono essere alterati.
- Un attaccante che intercetta una comunicazione non deve poter modificare il contenuto (**attacco ATTIVO**).
- Contromisure: **Firma digitale**

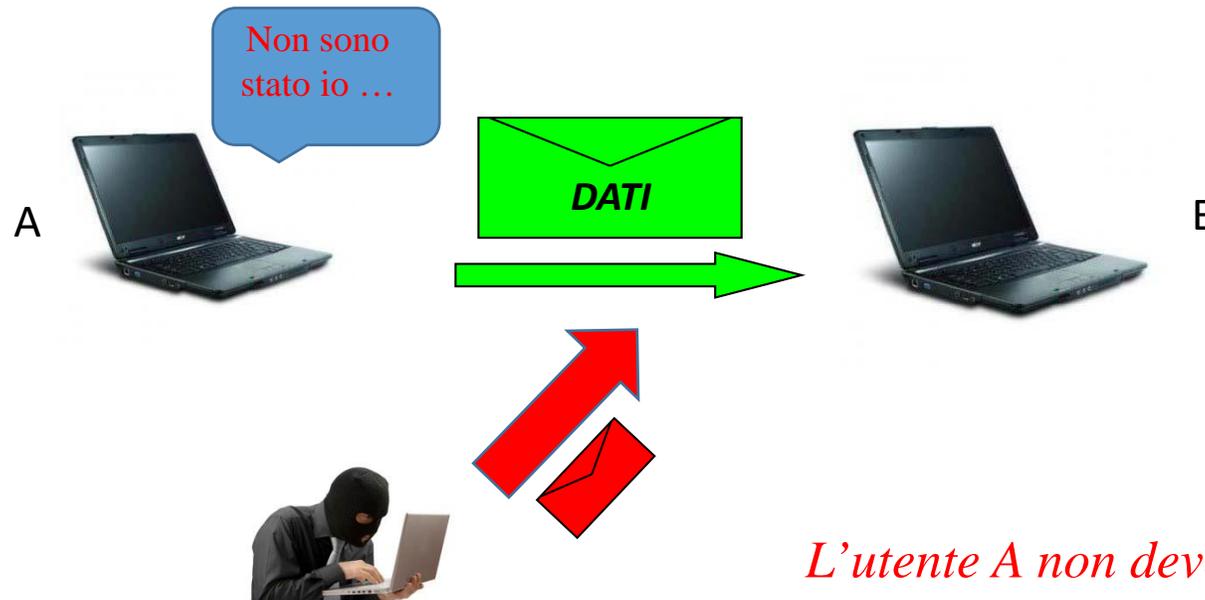


Intruso che dovesse intercettare la comunicazione non deve poter modificare il contenuto del messaggio

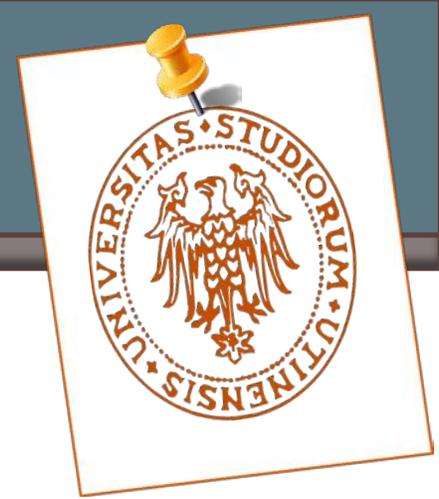
Paternità (non ripudiabilità)



- Nella comunicazione di un messaggio, è importante garantire che l'autore non possa in seguito negare di averlo spedito (è una conseguenza di autenticazione + integrità)



L'utente A non deve poter affermare che il messaggio da Lui inviato sia falso (sostenendo ad esempio che sia stato inviato da un hacker)



SOLUZIONI ?

Come proteggersi? Cifratura / Firma Digitale

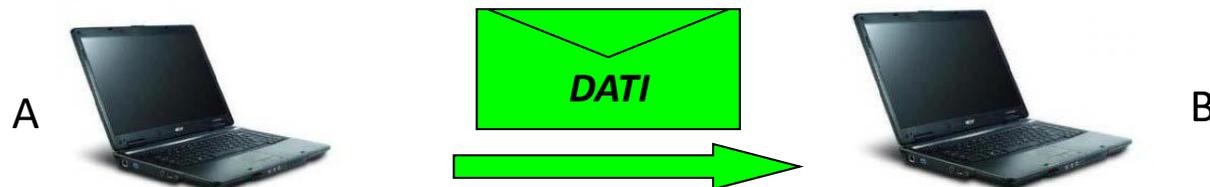


*I dati e le informazioni devono essere **CIFRATI** in modo che **SOLO** chi è autorizzato possa utilizzarli.*

*I dati e le informazioni devono essere **FIRMATI** digitalmente in modo che si abbia la certezza che **nessun** altro al di fuori del mittente possa averli creati.*



EncFS



P (Testo in chiaro)

$$C = E(P, K_{pubB})$$

$$P = D(C, K_{privB})$$

$$C_{FD} = E(P, K_{privA})$$

$$P = D(C, K_{pubA})$$

$$C = E(E(P, K_{privA}), K_{pubB})$$

$$P = D(D(C, K_{pubA}), K_{privB})$$

Come proteggersi? Firewall



Programmi che analizzano il traffico di rete in entrata/uscita dall'azienda

- Rilevano comportamenti anomali che potrebbero essere causati da **malware**
- Quando rilevano un comportamento anomalo chiedono all'utente cosa fare



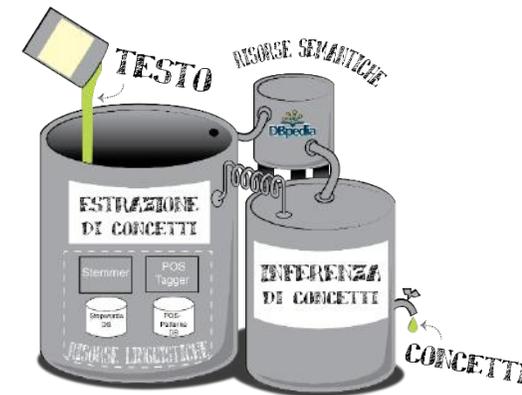
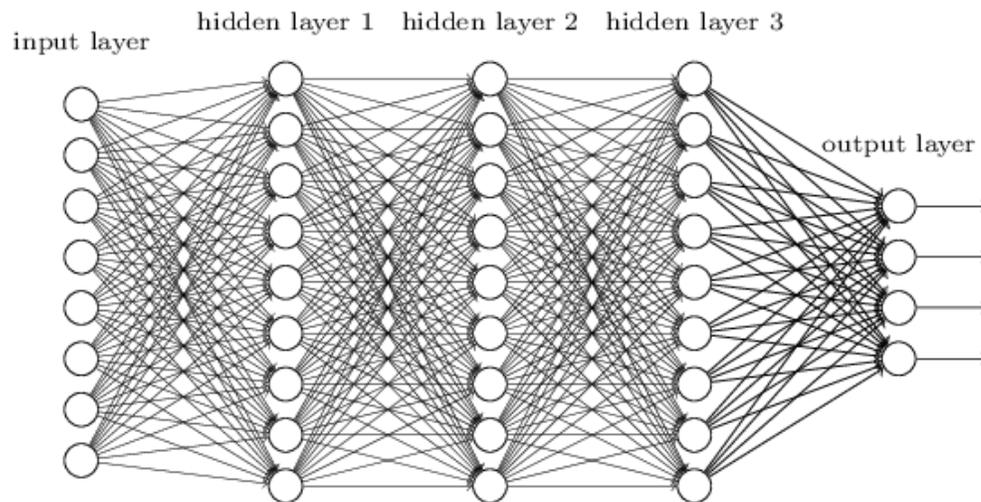
Se l'utente non conosce il firewall e le sue regole, non sa come comportarsi...

“Un programma sta tentando di accedere alla porta TCP 25. Blocco la connessione?”

Sviluppi futuri – Machine Learning



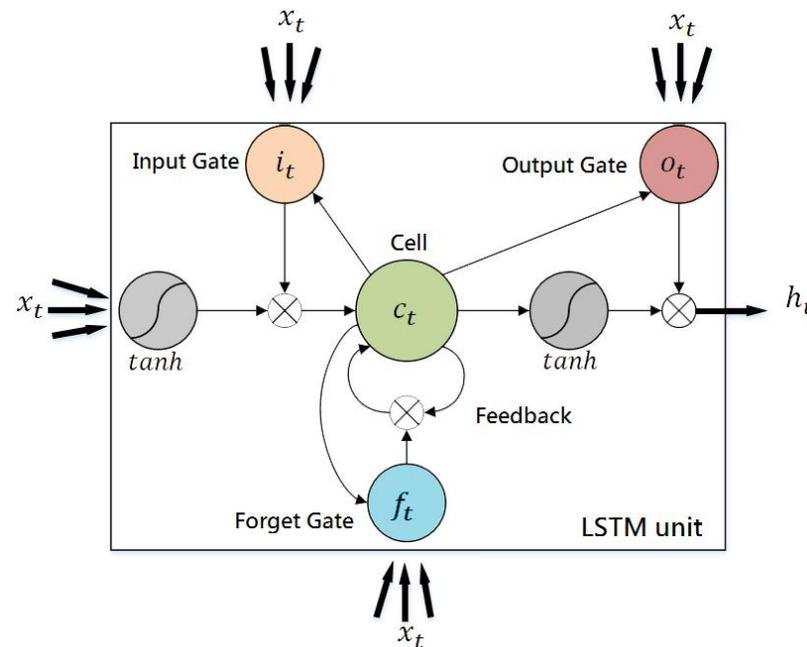
Allo studio ci sono algoritmi di **Machine Learning** che apprendono i comportamenti degli utenti e dei programmi sulla rete aziendale cercando di identificare comportamenti anomali

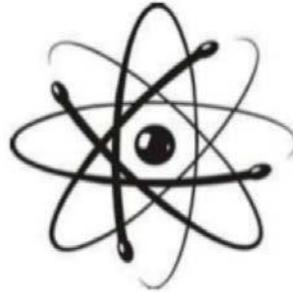


Sviluppi futuri – Machine Learning (2)



Gli algoritmi di **Machine Learning** analizzano automaticamente il traffico di rete, costruendo una policy di sicurezza basata sugli eventi normali/anomali, che si adatta alle esigenze dell'azienda (trade-off tra sicurezza e disponibilità delle risorse per gli utenti)





Crittografia Quantistica

2018 – **10 miliardi di Euro** di danni in Italia per attacchi informatici (1 miliardo di investimenti...)