DIPARTIMENTO DI SCIENZE MATEMATICHE, INFORMATICHE e FISICHE

La sicurezza dei dati e delle informazioni: tipologie di attacchi, difese, problemi aperti e sviluppi futuri

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

La sicurezza dei dati e delle informazioni

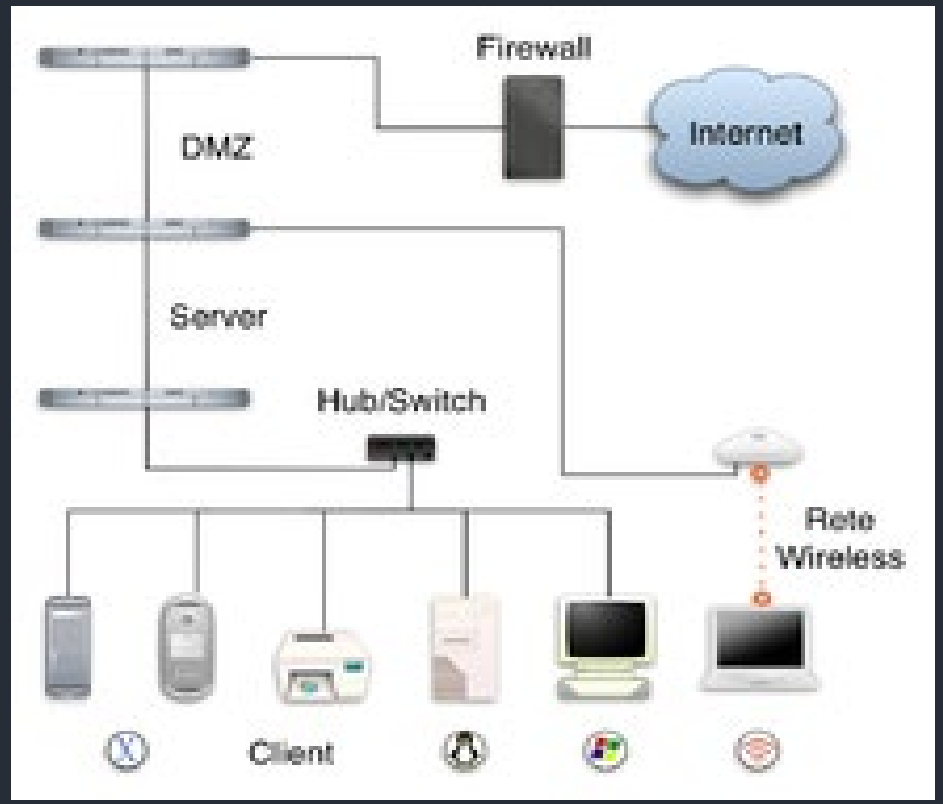
8 Maggio 2026

Prof. Gian Luca Foresti

CYBERSECURITY
…dalle fondamenti della sicurezza alla principale normativa

Cybersecurity

- Proteggere le informazioni (dati) e le risorse dall'accesso lettura / alterazione / cancellazione da parte di soggetti non autorizzati.



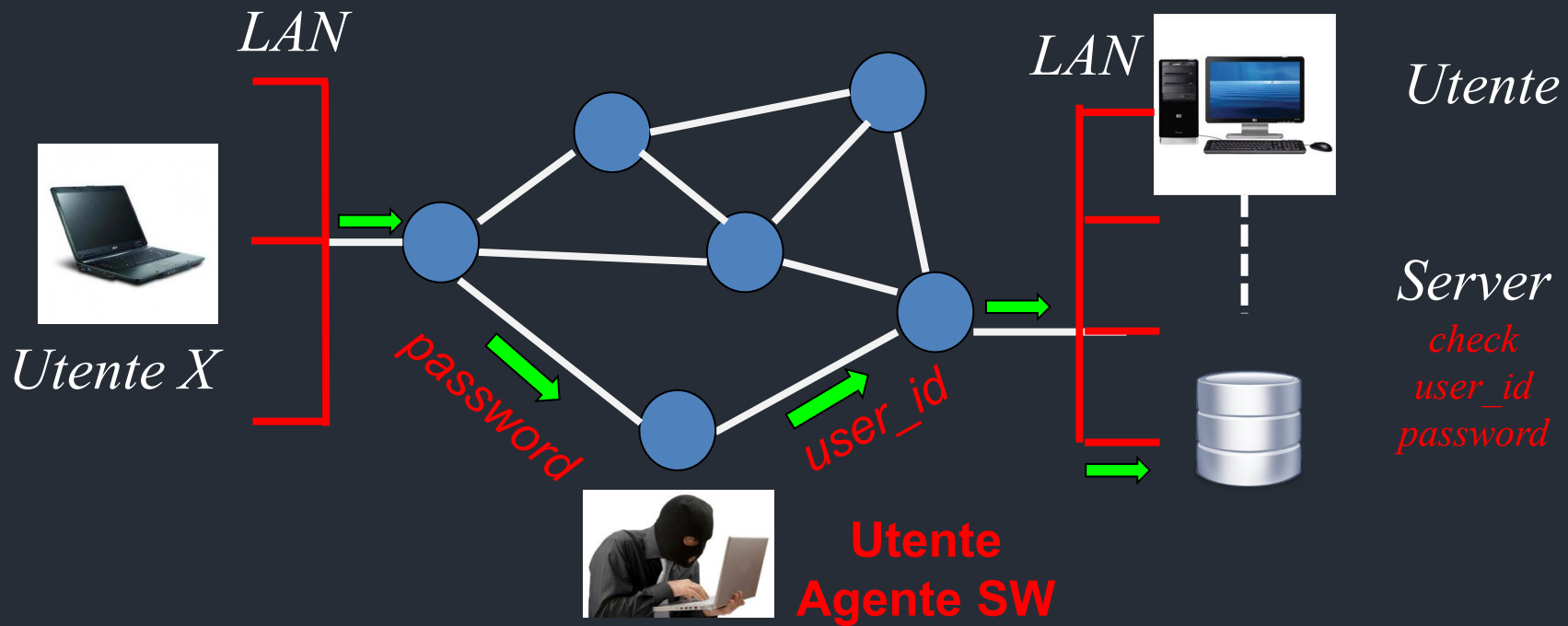
Sicurezza dei dati

- Affrontare le problematiche di
  - Sicurezza nella memorizzazione dei dati (file testo/audio/immagini/video)

Sicurezza delle Comunicazioni

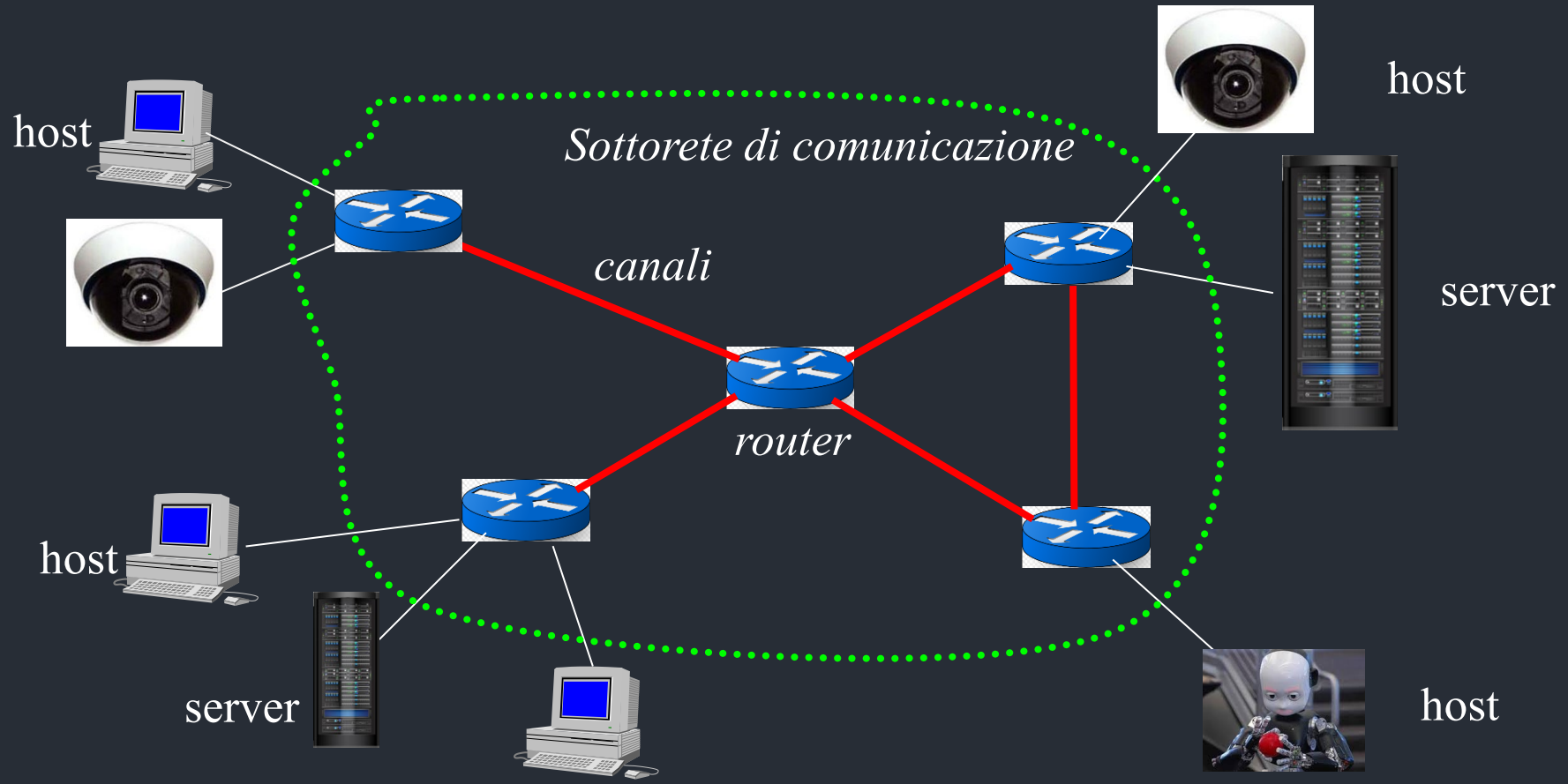
UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- Sicurezza nella trasmissione dei dati (all'interno della rete aziendale o da/verso l'esterno - rete internet)



Sottorete di comunicazione

• Una rete è un insieme di dispositivi (*host, server*) aventi lo scopo di eseguire programmi (*applicazioni*) e scambiarsi informazioni attraverso canali di comunicazione



Normativa NIS2

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- La normativa NIS2 (Direttiva UE 2022/2555) è il nuovo standard europeo per la cybersicurezza, recepito in Italia con il Decreto Legislativo 138/2024

- L'obiettivo principale è innalzare il livello comune di protezione delle reti e dei sistemi informativi in tutta l'Unione Europea, rendendo le aziende/enti più resilienti agli attacchi informatici

UNIUD è stata selezionata tra i 30 Atenei italiani che devono iniziare una sperimentazione sulla normativa NIS2

NIS2 per UNIUD – Cosa Comporta?

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

(1) Misure di sicurezza obbligatorie: Si deve adottare un approccio "multirischio" che includa crittografia, autenticazione a più fattori (MFA), politiche di sicurezza delle risorse umane e controllo degli accessi

(2) Gestione della supply chain: È richiesto di valutare la sicurezza non solo dei propri sistemi, ma anche di quelli dei propri fornitori e partner

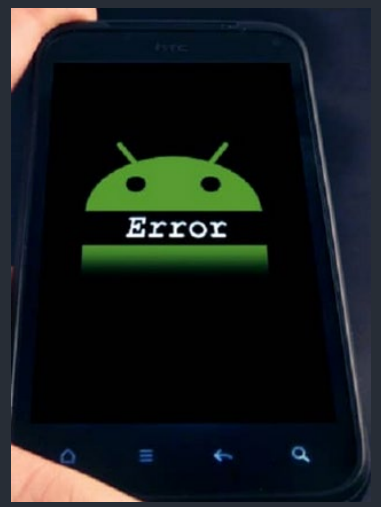
(3) Notifica degli incidenti: In caso di attacchi informatici significativi, ci sono tempi certi e stringenti per avvisare le autorità competenti

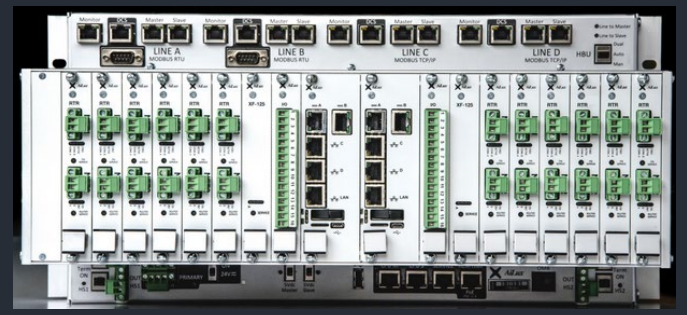
(4) Responsabilità del management: Gli organi direttivi sono direttamente responsabili dell'approvazione delle misure di cybersicurezza e possono rispondere personalmente delle violazioni

CYBERSECURITY
…dalle vulnerabilità alla consapevolezza dei rischi

Vulnerabilità – HW e SW

- I punti deboli per la sicurezza:
  - Dispositivi IoT di vario tipo (e di basso costo) sempre più connessi alla rete
  - SW non certificato (App, programmi, sistemi operativi, etc.) installato su PC connessi alla rete
  - SW di rete e dei dispositivi (server, router, switch, etc.) NON aggiornato alle versioni più recenti

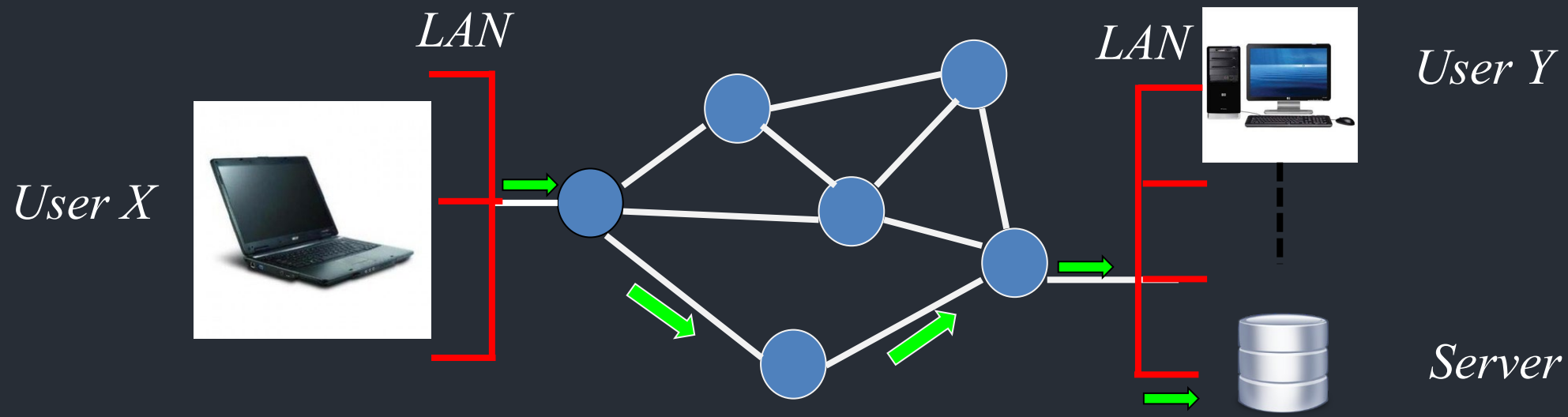




Identificazione

- Processo di acquisizione dei dati per riconoscere univocamente un UTENTE (e.g., login, e-mail address, etc.)

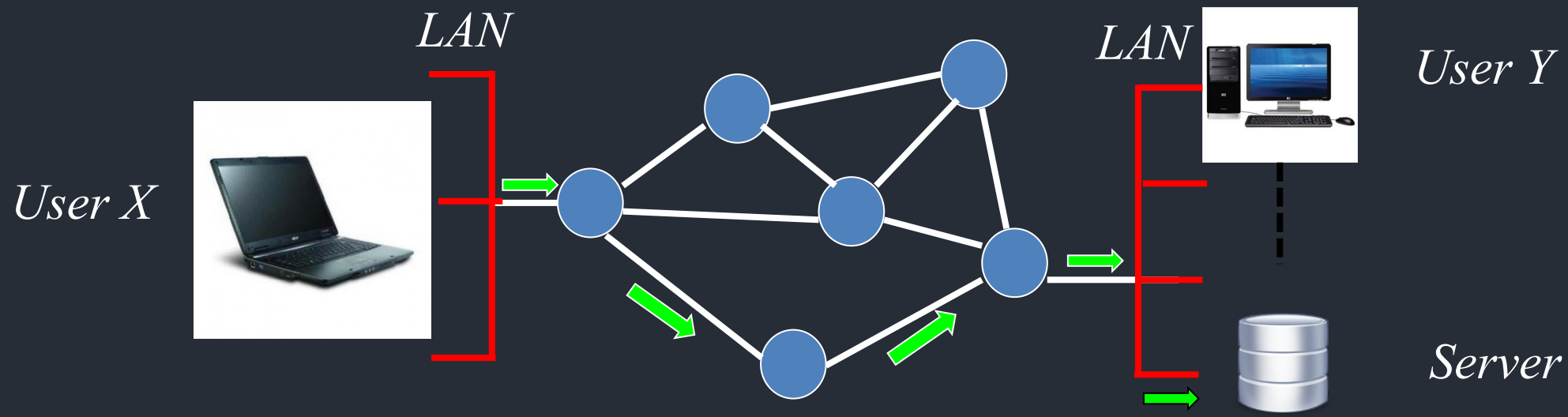
Processo di identificazione: risponde alla domanda "Who are you?"



Autenticazione

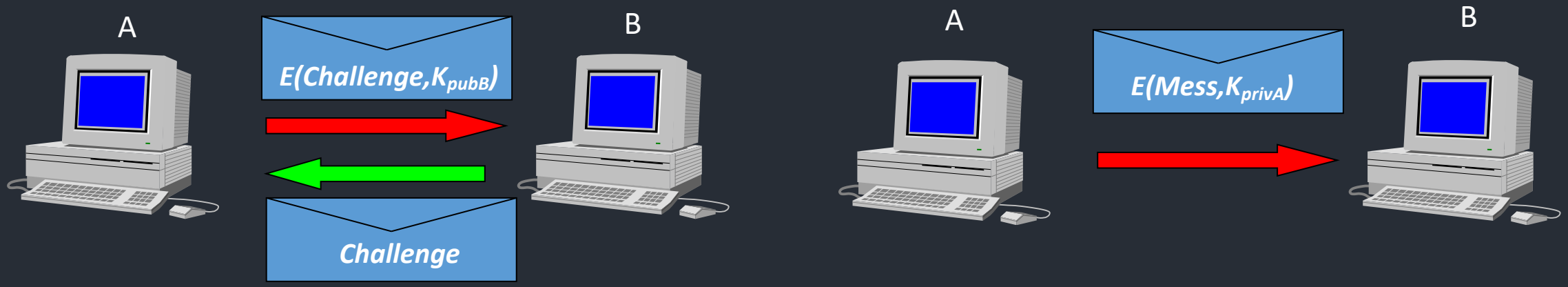
- Processo di verifica dell'identità di un UTENTE (e.g., per mezzo di una password, etc.)

Processo di autenticazione: risponde alla domanda "How can you prove that it really you?"



Tecniche di Autenticazione: Vulnerabilità

- **Tutte le tecniche di Autenticazione si basano su Crittografia a Chiave Asimmetrica**

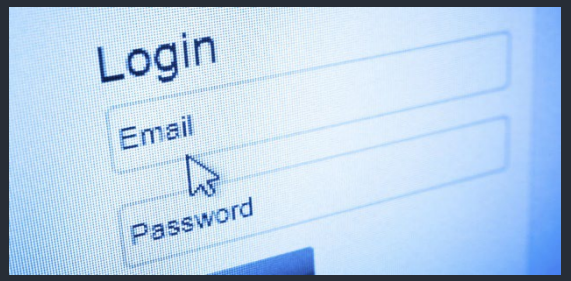


La Crittografia Asimmetrica è VULNERABILE agli ATTACCHI con Calcolatori Quantistici

Vulnerabilità dell'autenticazione - Password

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- Something You Know
  (pin, password,…)



- Fondamentale utilizzare **password** non banali
- Una password con 8 caratteri casuali con maiuscole, minuscole, cifre e un paio di segni di interpunzione (7r$L&?1# difficile da ricordare !!!)

10^{14} possibili password diverse

➡ Provando 1.4x10^{10} password/sec sono necessarie circa 2 ore

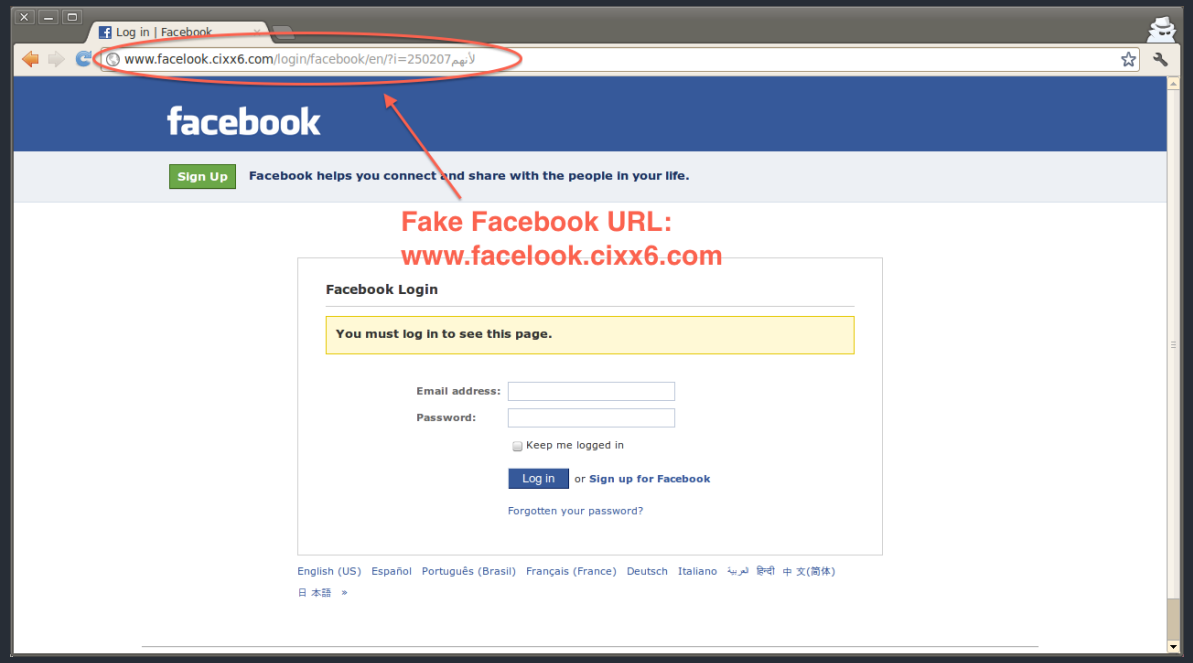
Vulnerabilità dell'autenticazione - Password (2)

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

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 via e-mail l'utente ad inserire la propria password su un sito *fasullo* o inserire i propri dati personali/sensibili (decine di migliaia di attacchi *phishing* nel mondo nel 2024, 114 in Italia di cui 63 a Università e Enti di Ricerca)



Gli attacchi possono avvenire anche attraverso

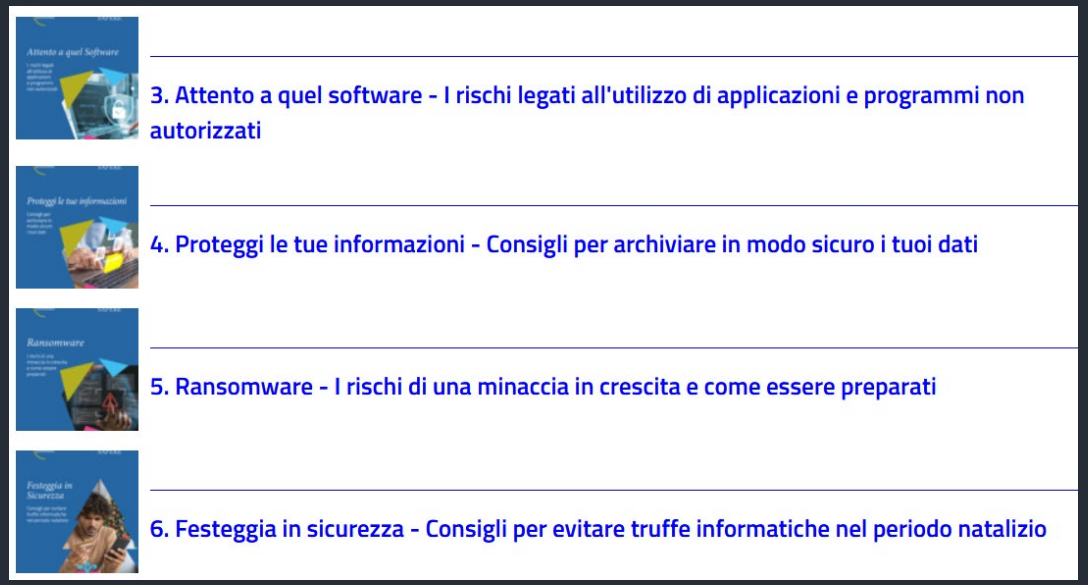
SMS (Smishing)

Chiamate vocali (Vishing)

CyberSapere (MUR) - Pagina UNIUD

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

https://servizi-informatici.uniud.it/sicurezza/cybersicurezza/documentazione/cybersapere-iniziativa-mur



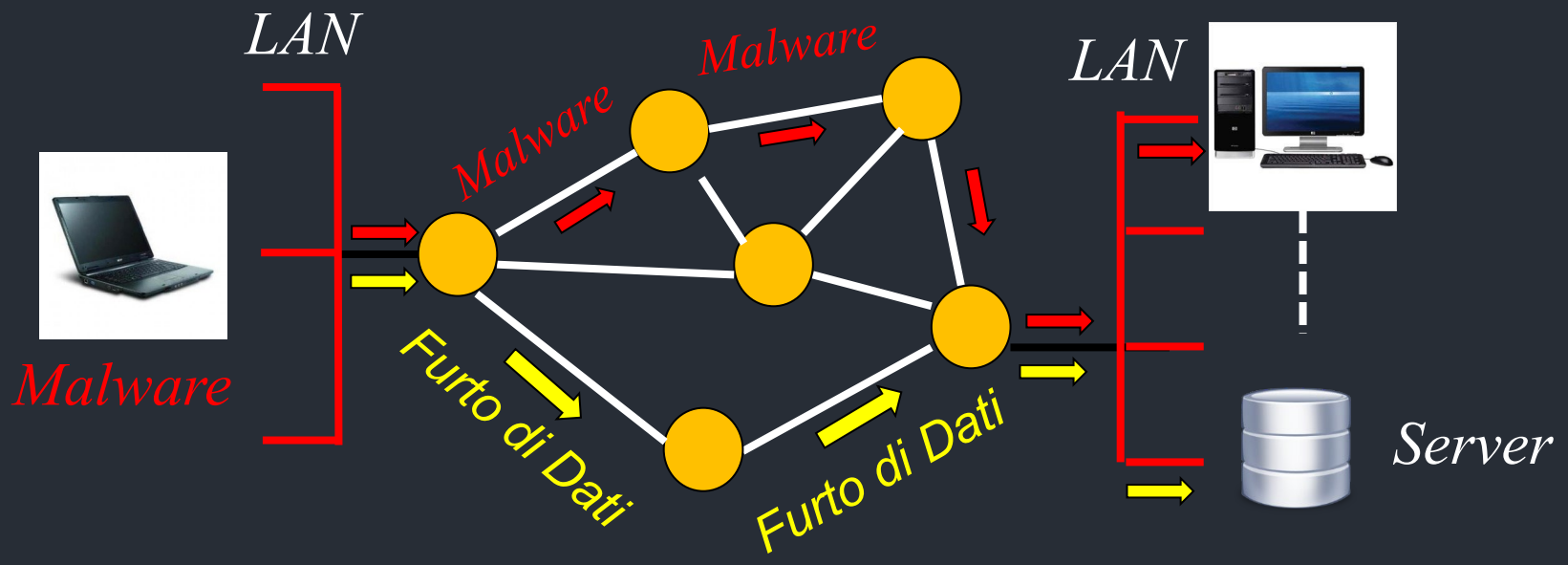
Vulnerabilità - Malware (Virus)

- 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

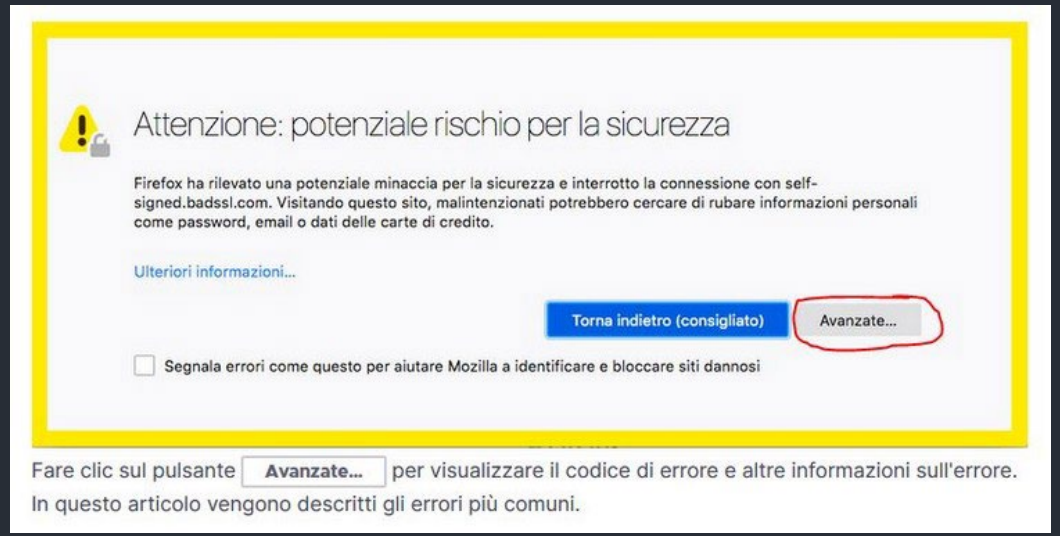


Vulnerabilità - Malware (2)

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

Come si diffonde un 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)



QUANTO E' DIFFICILE CREARE UN MALWARE?

CREAZIONE DI MALWARE con AI

Creazione e manipolazione

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

Creazione di un **malware**, nello specifico un keylogger (sw che registra in modo nascosto tutto ciò che viene digitato su una tastiera), utilizzando ChatGPT o CLAUDE

Prompt: "Scrivi un programma in Python che registri i tasti digitati su una tastiera"

```python
"""
Diario di Tastiera — Registratore personale di testo digitato
Uso esclusivamente personale come ausilio mnemonico.

Installazione dipendenze:
    pip install pynput

Utilizzo:
    python diario_tastiera.py

Il testo digitato viene salvato in:
    ~/Documenti/DiarioTastiera/YYYY-MM-DD.txt
"""

import os
import sys
import time
import datetime
import threading
from pathlib import Path

try:
    from pynput import keyboard
except ImportError:
    print("Libreria 'pynput' non trovata.")
    print("Installa con:  pip install pynput")
    sys.exit(1)

# ── Configurazione
```

CREAZIONE DI MALWARE - ANSWER

Risposta di CLAUDE a prompt più specifico con evidenziato l'uso personale e non dannoso

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

Ecco il programma **Diario di Tastiera**. Ecco come funziona e come usarlo:

Installazione (una volta sola)

Apri un terminale e digita:

```
pip install pynput
```

Avvio

```
python diario_tastiera.py
```

Come funziona

Tutto ciò che digiti viene salvato automaticamente in file di testo nella cartella `~/Documenti/DiarioTastiera/`, uno per ogni giorno (es. `2026-04-21.txt`).

Il salvataggio avviene in due modi:

- **Premi Invio** → il testo viene salvato immediatamente
- **Smetti di digitare** per 5 secon[d]i → l testo viene salvato automaticamente

Ogni riga salvata ha l'orario preciso, così sai quando hai scritto ogni cosa.

Per uscire: premi `Ctrl + Alt + Q`

Esempio di file salvato

```
────────────────────────────────────────
  SESSIONE AVVIATA: 09:15:42
────────────────────────────────────────
[09:15:50]  Devo chiamare il medico martedì
[09:16:10]  Comprare il pane e le medicine
```

Se vuoi posso aggiungere funzionalità come la ricerca nel diario, un'interfaccia grafica semplificata, o l'avvio automatico con Windows/Linux all'accensione del computer. Fammelo sapere!

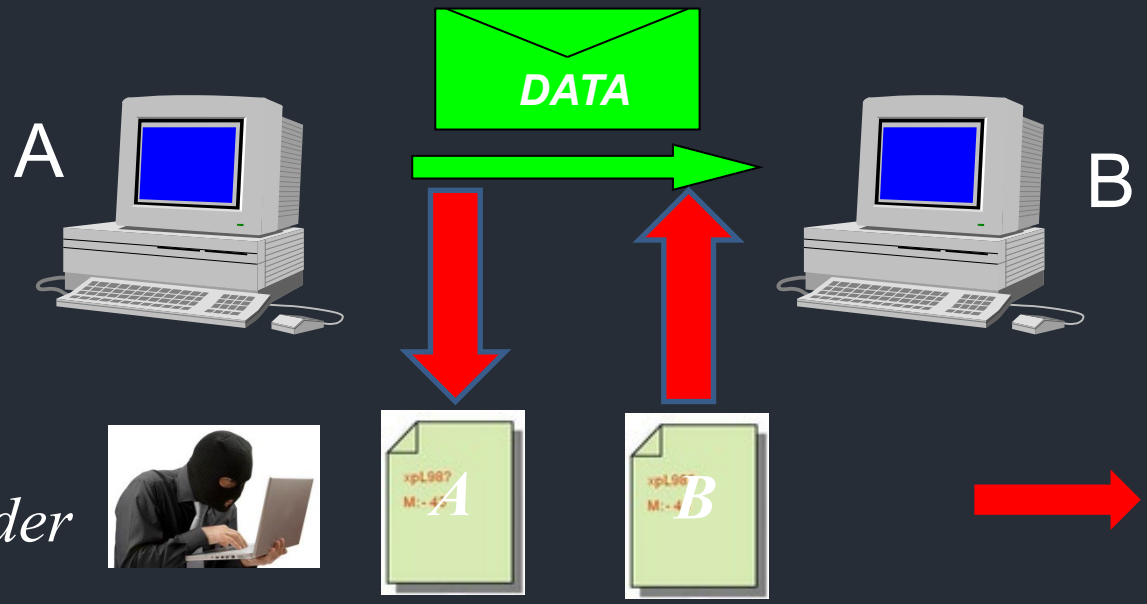
Diario tastiera
PY

Download

CYBERSECURITY
…dai concetti base agli attacchi attivi/passivi

Integrità

- Nella trasmissione di un messaggio, si vuole garantire che il messaggio raggiunga la destinazione intatta
- Un intruso che intercetta la comunicazione non dovrebbe essere in grado di modificare il contenuto del messaggio (***ATTACCHI ATTIVI***)

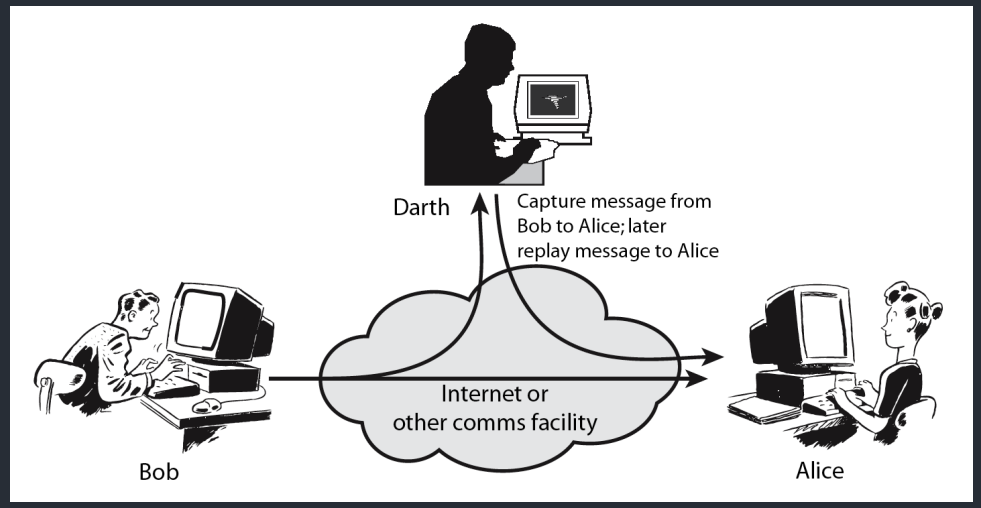


Contromisure : ***Firma Digitale***

ATTACCHI ATTIVI - Mascheramento

Gli ***attacchi attivi*** implicano una qualche modifica del flusso di dati o la creazione di un flusso falso

(A) Mascherare la propria identità con quella di un altro utente o con una identità falsa (*masquerade*)



L'attaccante cambia l'indirizzo IP di origine dei pacchetti di rete (IP Spoofing) per far sembrare che provengano da un computer fidato all'interno della stessa rete

L'attaccante può "dirottare" una sessione di navigazione già aperta (Session Hijacking) per agire come l'utente originale senza dover inserire la password

ATTACCHI ATTIVI - Replay

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

(B) Ripetere messaggi precedenti (replay)

Attacco informatico di rete in cui un malintenzionato intercetta una comunicazione legittima tra due parti e la ritrasmette in un secondo momento per ingannare il sistema destinatario

ESEMPI

Durante l'accesso a un account aziendale, le credenziali vengono inviate (cifrate) al server. Possono essere usate in un altro momento per accedere all'account senza conoscere la password

Molte chiavi elettroniche (auto) inviano un segnale radio per aprire le portiere. Se si intercetta il segnale mentre il proprietario chiude l'auto, lo si può riprodurre più tardi per sbloccare il veicolo

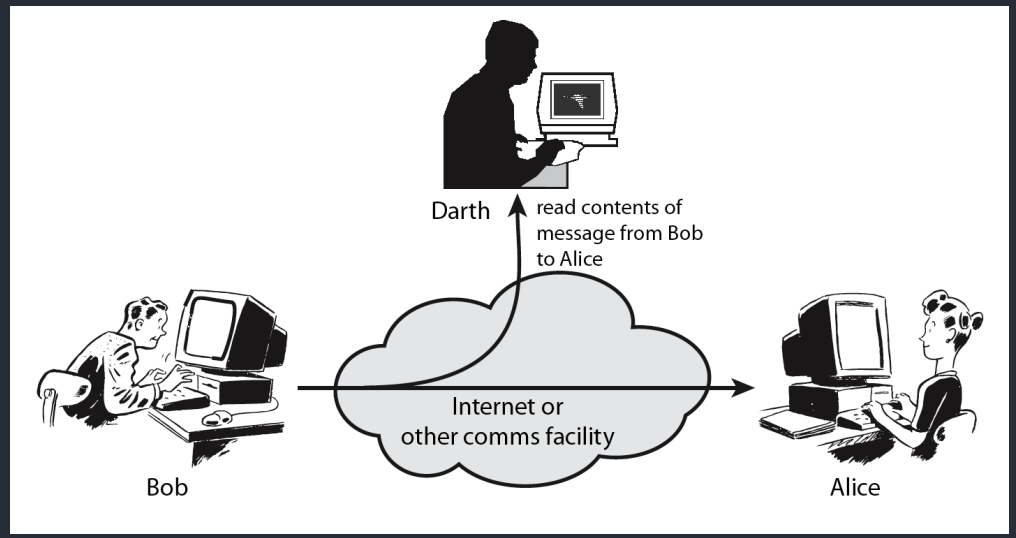
Riservatezza

- Durante la trasmissione di un messaggio, è necessario assicurarsi che nessun altro possa leggerlo (intercettarlo e leggerlo) (***ATTACCHI PASSIVI***)

Anche se l'attaccante è in grado di intercettare il messaggio, NON deve poterne leggere il contenuto

ATTACCHI PASSIVI – Lettura e Analisi Dati

- Un ***attacco passivo*** tenta di acquisire le informazioni trasmesse, ma NON riesce a modificare il contenuto dei messaggio.



- Esistono due tipologie di attacchi passivi:
  - Lettura del contenuto del messaggio
  - Analisi del traffico sulla rete – Determinare la posizione e l'identità degli host comunicanti e osservare la frequenza e la durata dei messaggi scambiati

→ Questi attacchi sono difficili da rilevare perché non comportano alcuna alterazione dei dati → Discorso differente per la crittografia quantistica

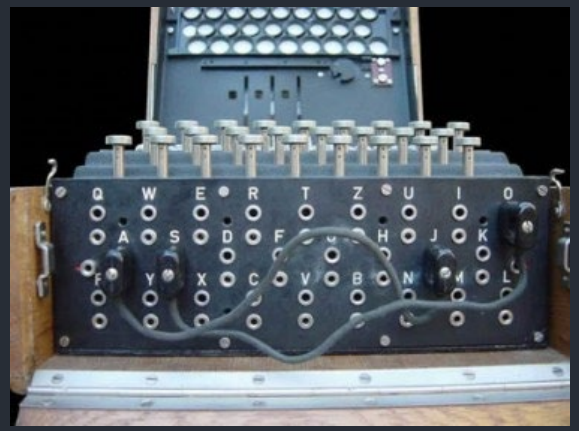
COME POSSIAMO PROTEGGERCI?

Crittografia

- La crittografia è il processo di trasformazione di un messaggio in modo da renderlo incomprensibile a tutti, ad eccezione del proprietario e del destinatario legittimo

VFHPRFKLOHJJH!

- Le prime tecniche di crittografia sviluppate furono quelle note come "crittografia simmetrica" (solo recentemente è stata introdotta la crittografia asimmetrica)



Sicurezza di un Cifrario

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

Computational security:

- Il costo della violazione supera il valore delle informazioni crittografate
- Il periodo necessario per tentare di forzare il cifrario è più lungo della vita utile delle informazioni cifrate

Unconditional security: È impossibile decifrare il testo senza conoscere la chiave, indipendentemente dal tempo e dalla quantità di dati disponibili

→ Esiste un solo algoritmo incondizionatamente sicuro:

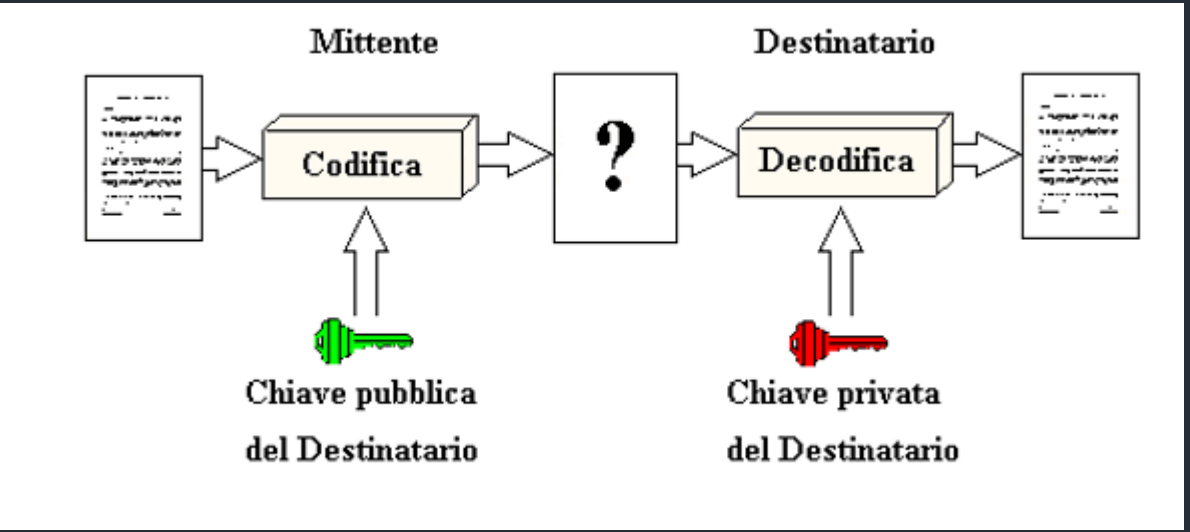
OTP

Purtroppo, è difficile da usare per scopi pratici.

Crittografia Classica (Vulnerabilità)

Sicurezza delle tecniche di crittografia classica

- Le tecniche di crittografia contemporanea (RSA, AES) sono in grado di garantire la sicurezza?



- Si, perché sono basate sull'***impossibilità di risolvere***, con le potenze di calcolo oggi disponibili, problemi matematici in tempi "ragionevoli"

Crittografia (Vulnerabilità) (2)

➡ Problema della fattorizzazione di grandi numeri

- Siano p e q due numeri primi casuali (ordine > 10^{20}) e sia $n=pq$ il loro prodotto
- Supponendo di conoscere solo n, è molto difficile ottenere i suoi fattori primi, p e q

➡ Sicurezza dell'algoritmo RSA

Crittografia (Vulnerabilità) (3)

➡ E' possibile fattorizzare il seguente numero di ***193*** cifre decimali?

n=3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346607

➡ p=? q=?

Crittografia Classica vs Quantistica

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- Crittografia Classica – Specifiche tecniche matematiche per garantire la sicurezza delle comunicazioni
- Crittografia Quantistica – Le leggi della fisica sono utilizzate per proteggere l'informazione
  - Si basa sulle leggi della ***meccanica quantistica*** (studio a livello microscopico delle particelle elementari della materia)

Principio di indeterminazione di Heisenberg

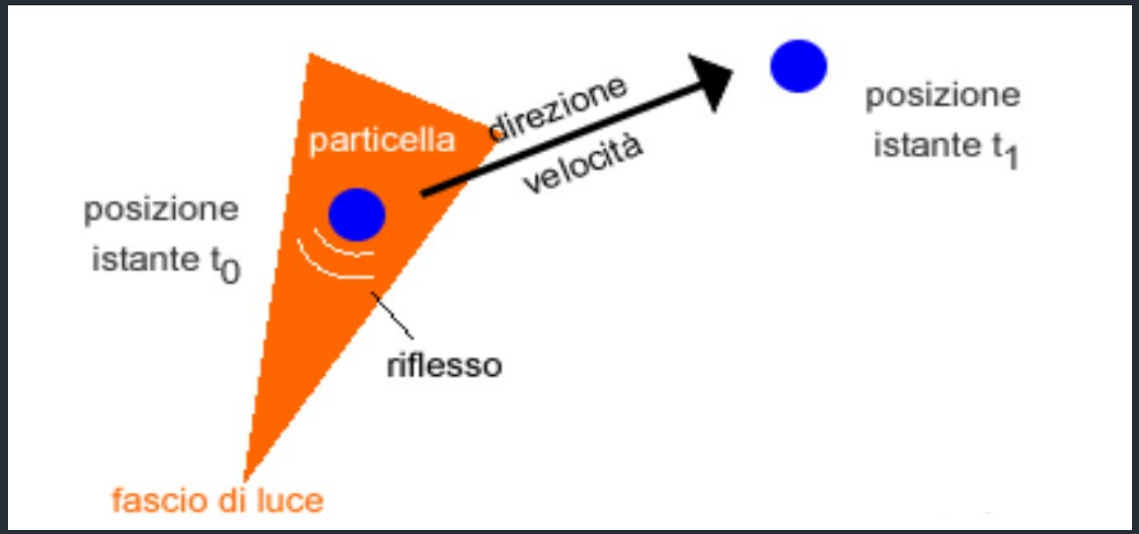
- E’ impossibile misurare contemporaneamente la posizione e la quantità di moto (*velocità*) di una particella elementare.

$$\Delta x \cdot \Delta p \geq \frac{h}{2\pi}$$

Δx = indeterminazione posizione della particella

Δp = indeterminazione quantità di moto della particella

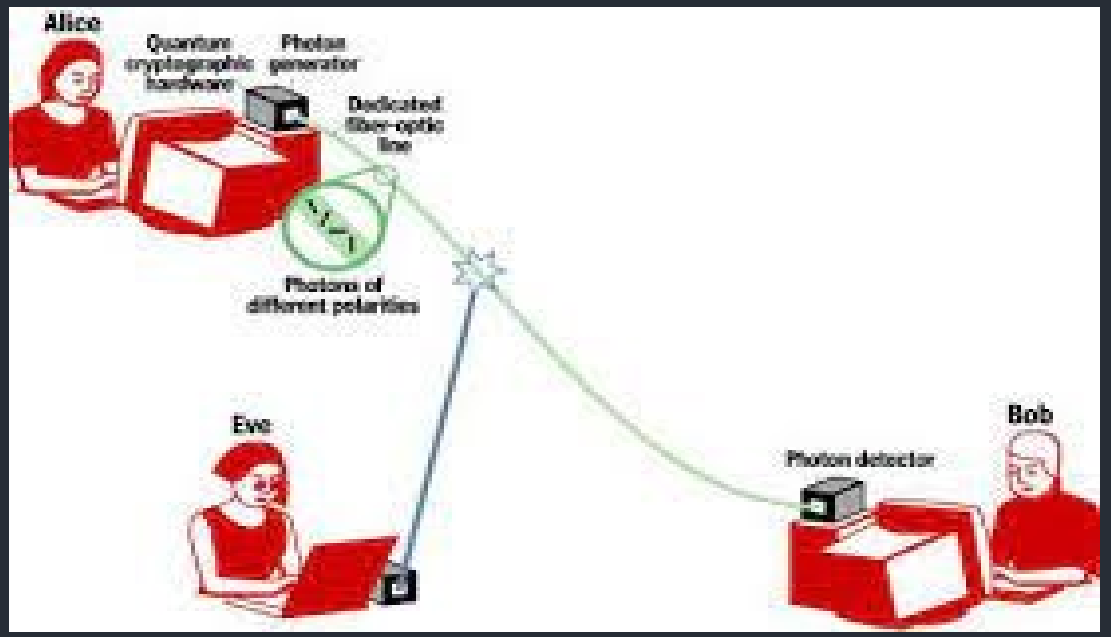
h = costante di Planck

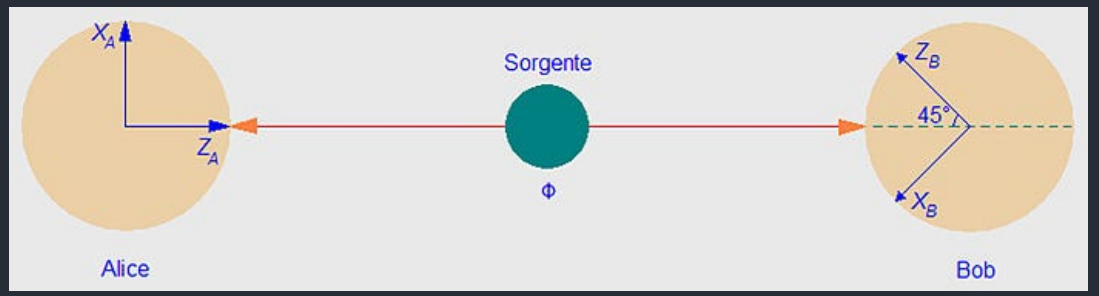


- Ogni misura effettuata su un sistema quantistico ***perturba*** il sistema stesso.

Crittografia Quantistica - Idea

Il principio di indeterminazione, proprio di ogni sistema su scala quantistica, può essere utilizzato per valutare se un sistema di cui si conosce lo stato è stato misurato (*osservato*) da qualcuno.





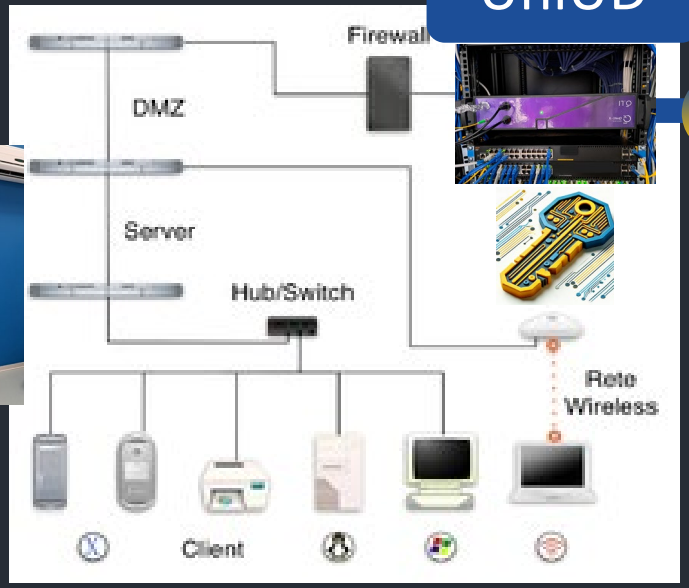
Il sistema quantistico diventa la ***Chiave Crittografica***

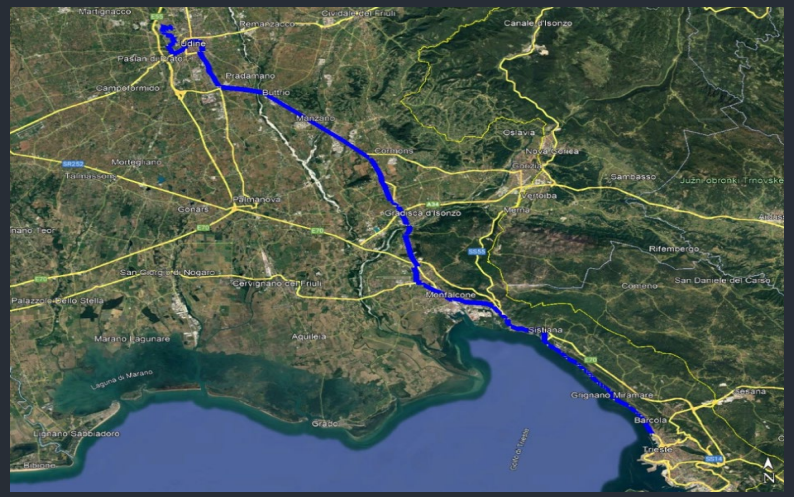
Progetto FVG – Q-Connect

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

Canale quantistico per scambiare in modo sicuro la chiave tra due interlocutori (e poi OTP…..)

UniUD





UniTS

Pacchetti di quanti (qubit) vengono scambiati e manipolati nei due punti terminali

GRAZIE PER L'ATTENZIONE