Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino 1859
Telsy A TIM ENTERPRISE BRAND
DISMA

life.augmented

La Sicurezza dei Dispositivi Embedded

Matteo BOCCHI

Senior Advanced Research Engineer
System Research & Applications (SRA)
STMicroelectronics

CrypTO Conference
22 Maggio 2025
Torino

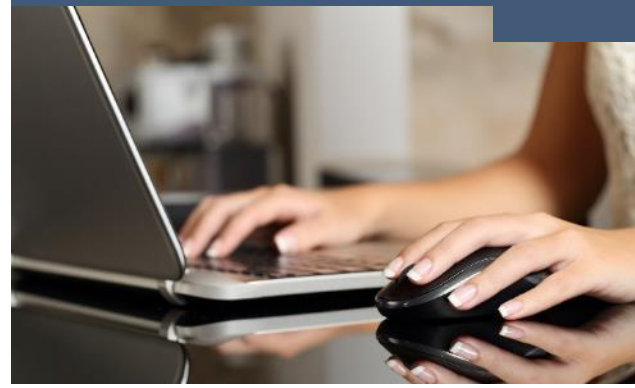
Sicurezza & applicazioni/mercati di riferimento per i dispositivi embedded

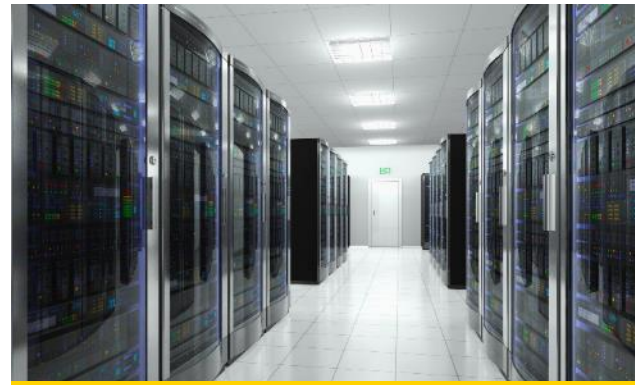
Automotive

Elettronica per l'industria e la domotica

Dispositivi indossabili

Computer, periferiche, telecomunicazioni



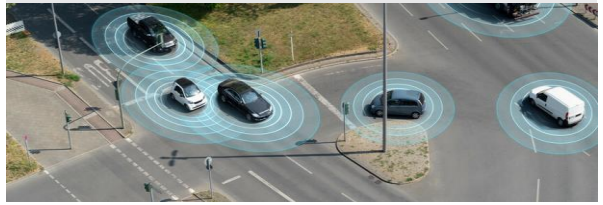


life.augmented

Esempi

Sicurezza e integrità dei dati dell'auto

Sicurezza sistemi ADAS e V2X

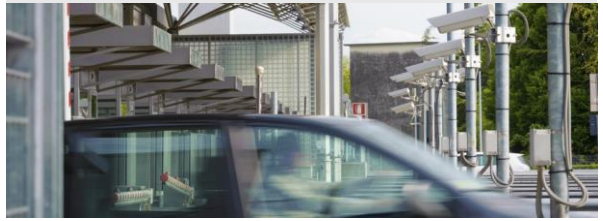


Sistemi digitali per l'accesso

Sicurezza della ricarica delle auto elettriche

Industria 4.0 e cybersecurity

Sistemi elettronici di pedaggio



Contatori smart

Apparecchi connessi

Protezione del brand

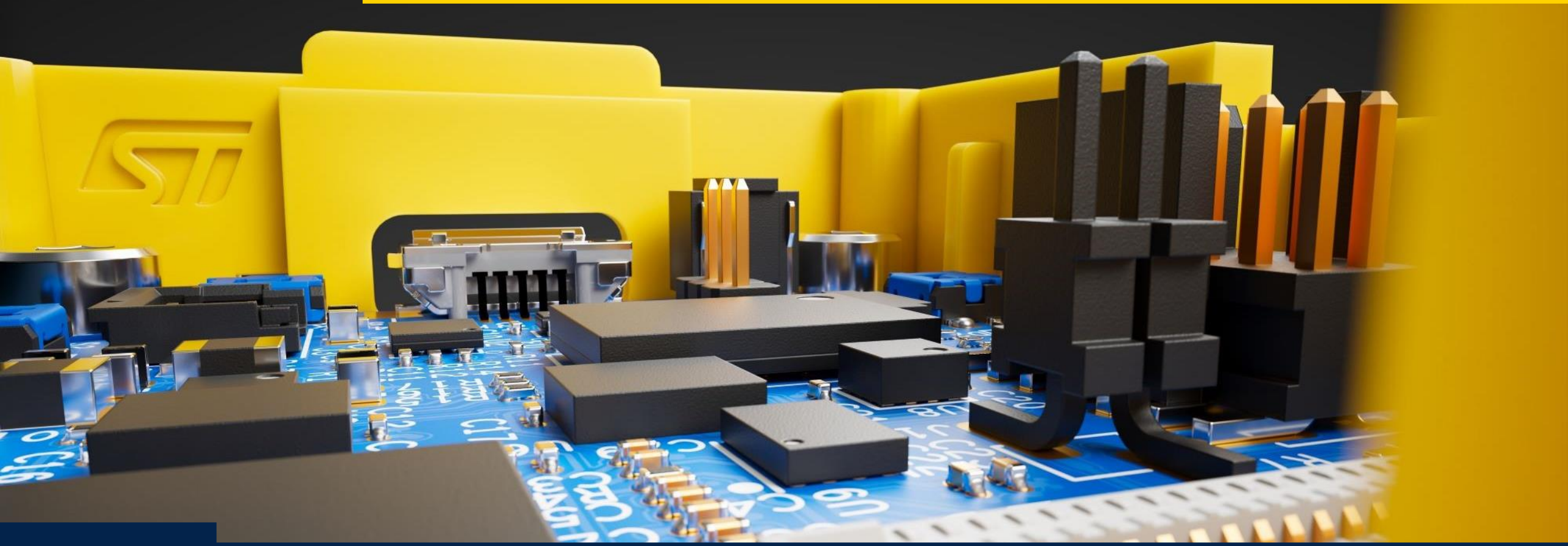
Identità digitale

Transazioni da dispositivi mobili

Pagamenti elettronici

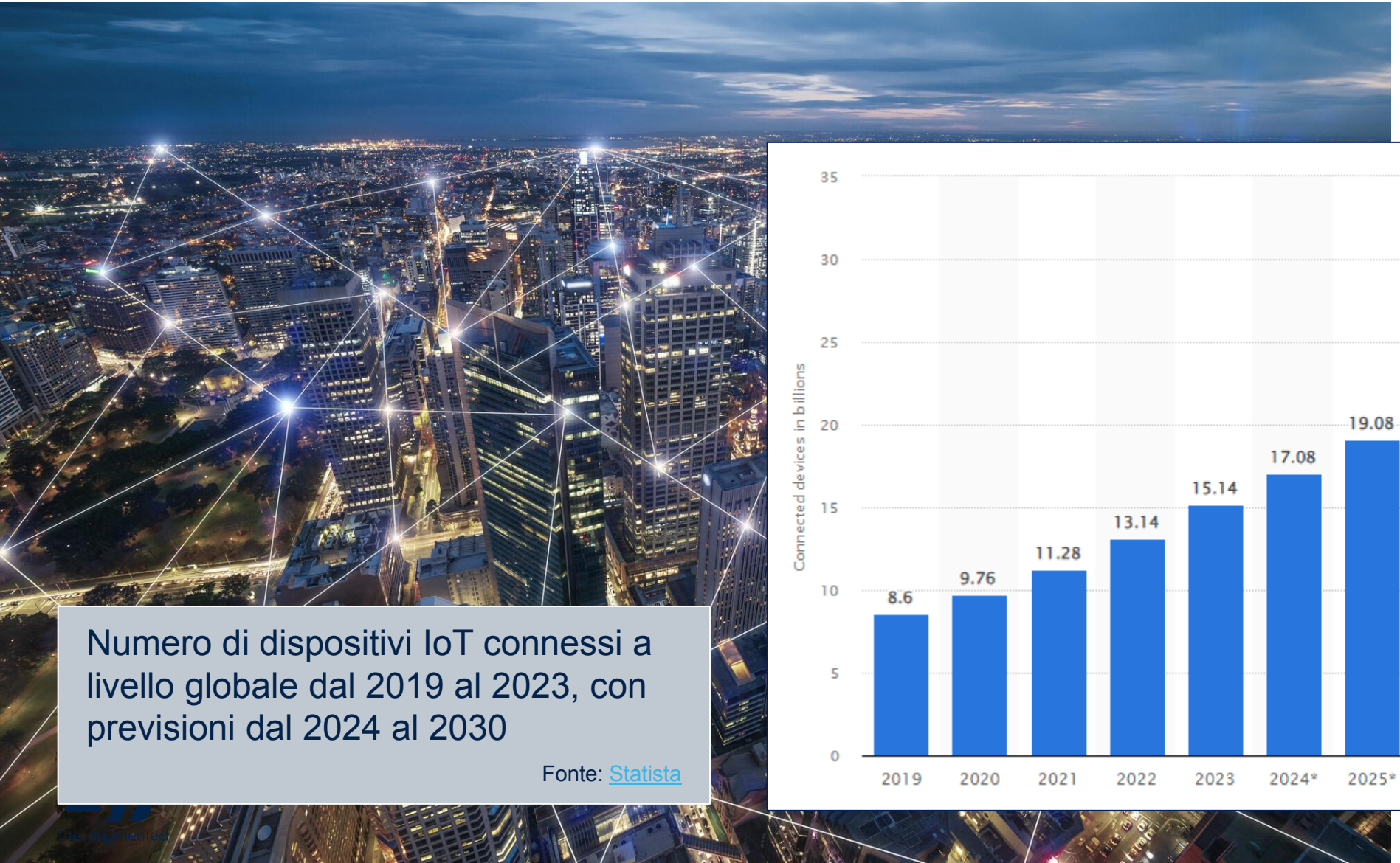
life.augmented

Dispositivi embedded e limitazioni



life.augmented

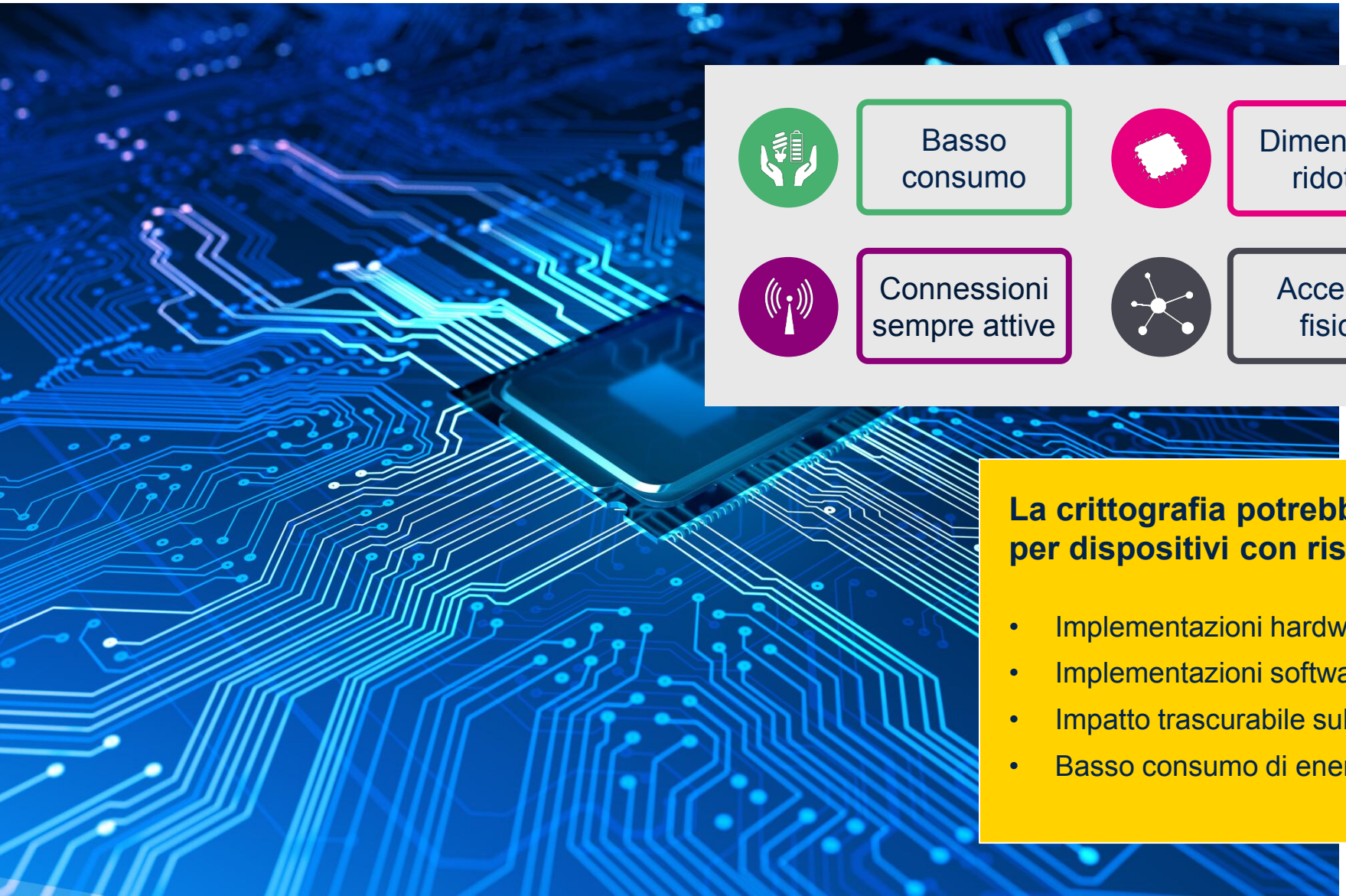
Dispositivi IoT connessi



Numero di dispositivi IoT connessi a livello globale dal 2019 al 2023, con previsioni dal 2024 al 2030

Fonte: Statista

Le sfide della sicurezza per dispositivi embedded



- Basso consumo
- Dimensioni ridotte
- Memoria limitata
- Connessioni sempre attive
- Accesso fisico
- Costo ridotto

La crittografia potrebbe essere costosa per dispositivi con risorse limitate

- Implementazioni hardware compatte
- Implementazioni software con basso utilizzo di RAM e ROM
- Impatto trascurabile sulle prestazioni complessive
- Basso consumo di energia/potenza

Sicurezza di sistema

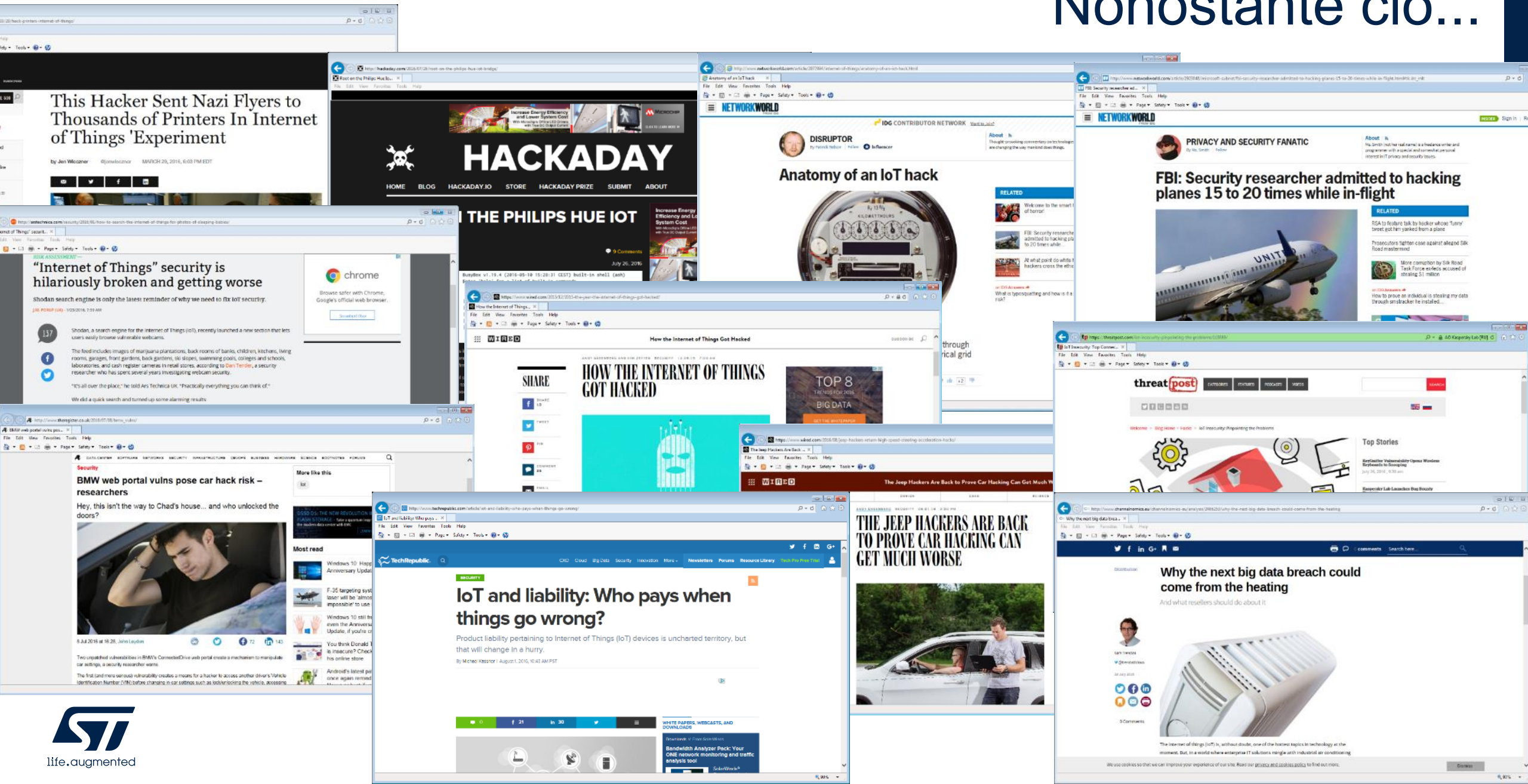
life.augmented

Principi di Secure Design (1974)

- ***economy of mechanism***: mantenere il design il più semplice e piccolo possibile.
- ***fail-safe defaults***: basare le decisioni di accesso sul permesso piuttosto che sull'esclusione.
- ***complete mediation***: di ogni accesso ad ogni oggetto deve esserne controllata l'autorizzazione.
- ***open design***: un design non dovrebbe essere segreto. I meccanismi non dovrebbero dipendere dall'ignoranza dei potenziali attaccanti, ma piuttosto dal possesso di chiavi o password specifiche, più facilmente protette.
- ***separation of privilege***: dove possibile, un meccanismo di protezione che richiede due chiavi per l'accesso è più robusto e flessibile di uno che consente l'accesso al possessore di una sola chiave.
- ***least privilege***: ogni programma e ogni utente del sistema dovrebbe operare utilizzando il minimo insieme di privilegi necessari per completare il lavoro.
- ***least common mechanism***: minimizzare la quantità di meccanismi comuni a più di un utente e da cui dipendono tutti gli utenti.
- ***psychological acceptability***: è essenziale che l'interfaccia utente sia progettata per essere facile da usare, in modo che gli utenti applichino correttamente e automaticamente i meccanismi di protezione.

Jerome H. Saltzer and Michael D. Schroeder
The Protection of Information in Computer Systems
Manuscript received October 11, **1974**.
Fourth ACM Symposium on Operating System Principles
http://www.cs.virginia.edu/~evans/cs551/saltzer/

Nonostante ciò...



life.augmented

Perchè?

- Sicurezza e affidabilità sono costose e complesse, difficili da dimostrare
- È impegnativo garantire qualità lungo tutta la catena del valore

  → Sforzi per stabilire linee guida e standard (ENISA, SESIP, IIC for industrial, ARM PSA, ISO-21434 cybersecurity for automotive, ecc.)
- Mancanza di incentivi finanziari per coloro che "fanno le cose per bene"
  Mancanza di sanzioni per chi prende scorciatoie sulla sicurezza

  → Questo sta cambiando: spinta politica (EU GDPR, EU Cybersecurity Act, EU DA RED on cybersecurity for radio equipment, US Cyber Trust Mark, UN R155 cybersecurity for road transportation, ecc.)
- Errori di progettazione della sicurezza del sistema
  - Alcuni produttori mancano delle competenze, dell'esperienza o della guida necessaria
- Alcune sfide tecniche sono veramente difficili

Side-Channel Attacks (SCA)

life.augmented

Crittanalisi, o come attaccare gli algoritmi crittografici

- È l'arte e la scienza di analizzare i sistemi crittografici al fine di studiarne gli aspetti nascosti
  - Analisi matematica degli algoritmi crittografici
  - Side-Channel Attacks
    - Basato su informazioni ottenute dall'implementazione fisica di un crittosistema
    - *NESSUNA* debolezza teorica nell'algoritmo
    - *NESSUNA* forza bruta per provare tutte le possibili combinazioni/chiavi

Esempio

life.augmented

Esempio

Dutch police catch cannabis growers after spotting snow-free roof

Police in the Netherlands have been identifying cannabis growers from the lack of snow on the roofs of their houses

By Harriet Alexander
10 February 2015 • 11:44 am

The house in Haarlem with no snow on its roof

Tipi di “side channel”

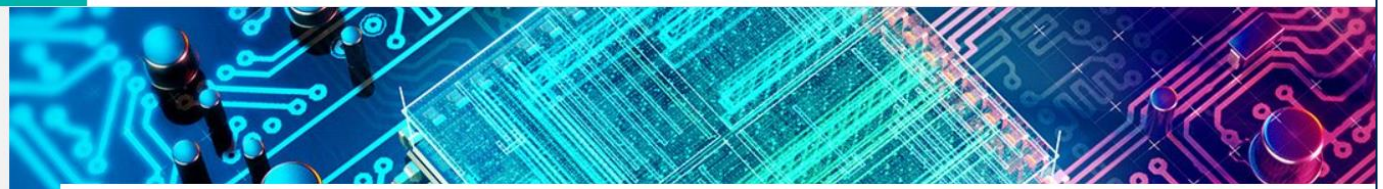
- Tempo
  - I crittosistemi spesso impiegano tempi leggermente diversi per elaborare diversi input segreti (proprio a causa del dato segreto)
  - Questo attacco potrebbe essere eseguito da remoto
- Consumo di energia
  - Il consumo istantaneo di energia di un dispositivo dipende dai dati che elabora e dalle operazioni che esegue
- Emissioni elettromagnetiche
  - Il flusso di corrente attraverso un dispositivo elettronico induce emanazioni elettromagnetiche
  - Questo canale può portare ad attacchi più efficaci di quelli basati sul consumo di energia

Ma davvero funzionano nel mondo reale?

TechTarget | Security

News Features Tips Webinars 2023 IT Salary Survey Results More

Analytics & Automation | Application & Platform Security | Cloud Security | Compliance | Data Security & Privacy | More Topics



NEWS

'GoFetch' attack spells trouble for Apple M-series chips

Academic researchers discovered a hardware optimization feature called 'data memory-dependent prefetcher' could be abused to extract secret encryption keys from vulnerable systems.

HACKADAY

HOME BLOG HACKADAY.IO TINDIE HACKADAY PRIZE SUBMIT

YOUR NOISY FINGERPRINTS VULNERABLE TO NEW SIDE-CHANNEL ATTACK

by: Dan Maloney 28 Comments

February 23, 2024

SECURITYWEEK

CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Malware & Threats | Security Operations | Security Architecture | Risk Management | CISO Strategy | ICS/OT | Funding/M&A

VULNERABILITIES

New Attack Shows Risks of Browsers Giving Websites Access to GPU

Researchers demonstrate remote GPU cache side-channel attack from within browsers against AMD and NVIDIA graphics cards.

hackster.io

AN AVNET COMMUNITY

Search

Projects | Channels | News

Kévin Courdesses Breaks the ESP32-V3, ESP32-C3, and ESP32-C6 Wide Open with a Side-Channel Attack

"There is no software [or] hardware fix available," Espressif warns of vulnerabilities allowing for encrypted flash data exfiltration.

life.augmented

Edge-AI & sicurezza

life.augmented

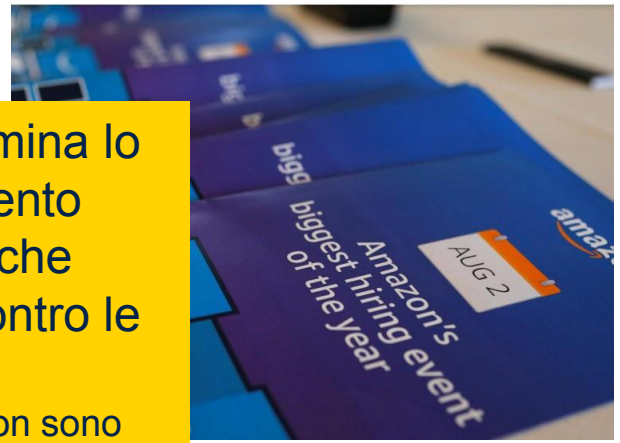
AI, AI, AI…

- Tutti vogliono l’intelligenza artificiale ovunque
- Ma chi pensa alla sua sicurezza?

“Hook – Capitan Uncino”, 1991

life.augmented

Problemi legati all’AI



Ott. 2018: Amazon elimina lo strumento di reclutamento segreto basato sull'IA che mostrava pregiudizi contro le donne.

I modelli informatici di Amazon sono stati addestrati a valutare i candidati osservando i curriculum inviati all'azienda, senza attenta analisi sulla base di dati

2015: Uno sviluppatore software ha caricato una foto di due persone di colore su Google Foto, e il sistema di riconoscimento facciale ha etichettato la fotografia come "gorilla".

Nov. 2019: La carta di credito di Apple è stata sotto indagine per discriminazione nei confronti delle donne.

I clienti affermavano che la carta offrisse meno credito alle donne rispetto che agli uomini.

Mar. 2018: Auto Uber a guida autonoma uccide pedone in Arizona

Woman’s Death in Arizona Casts A Pall on Driverless Car Testing

By DAISUKE WAKABAYASHI

SAN FRANCISCO — Arizona officials saw opportunity when Uber and other companies began testing driverless cars a few years ago. Promising to keep oversight

their self-driving vehicles in cities around the country. The companies say the cars will be safer than regular cars simply because they take easily distracted humans out

life.augmented

Abusi e casi sensibili legati all'AI

Deepfake: possono distruggere la credibilità di un individuo, perpetrare frodi, manipolare l'opinione pubblica.

2019: PassGAN utilizza una GAN (Generative Adversarial Network) per apprendere la distribuzione statistica delle password e generare ipotesi di password di alta qualità.

Mar. 2016: un utente ha trasformato Tay, il bot AI di Microsoft, in un maniaco genocida in meno di 24h.

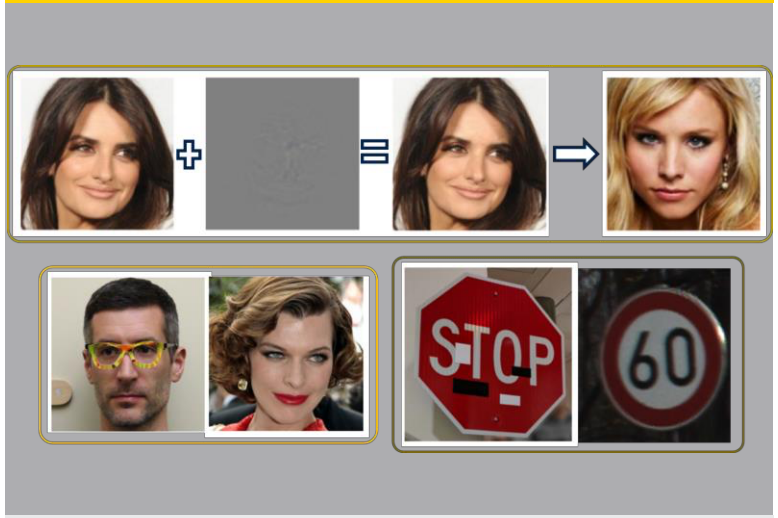
Armi letali autonome

Minacce all'AI sui sistemi embedded

Data poisoning

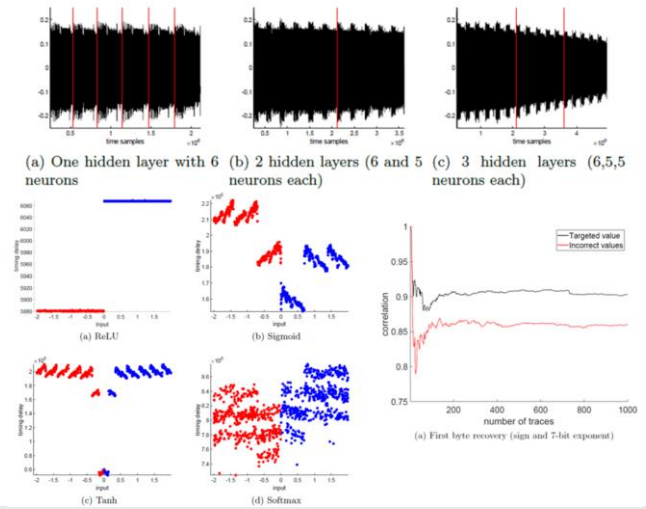
- I dati per l'addestramento vengono intenzionalmente modificati al fine di far funzionare diversamente il sistema

Adversarial examples



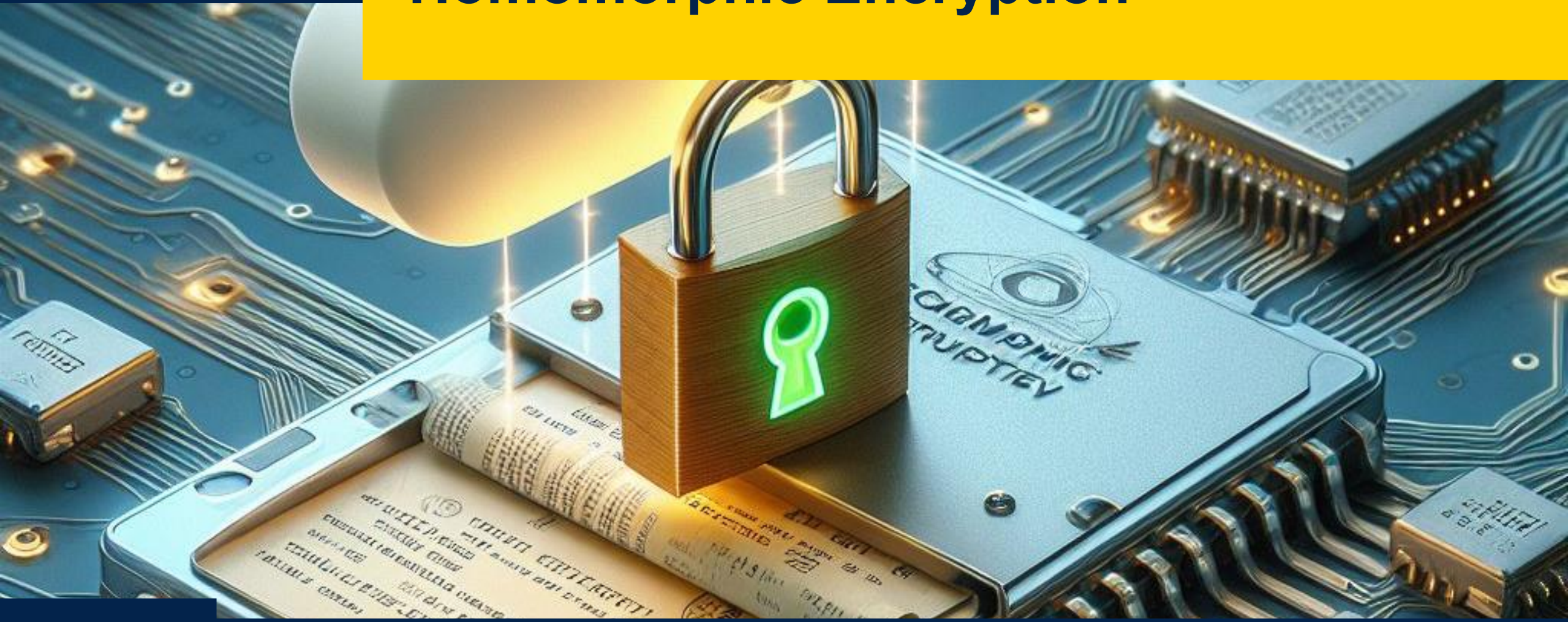
- Gli input hanno impercettibili modifiche che causano un errato funzionamento del sistema

Side-channel attacks



- Permettono di estrarre informazioni quali modello e parametri della rete neurale, e in alcuni casi anche gli input forniti al sistema

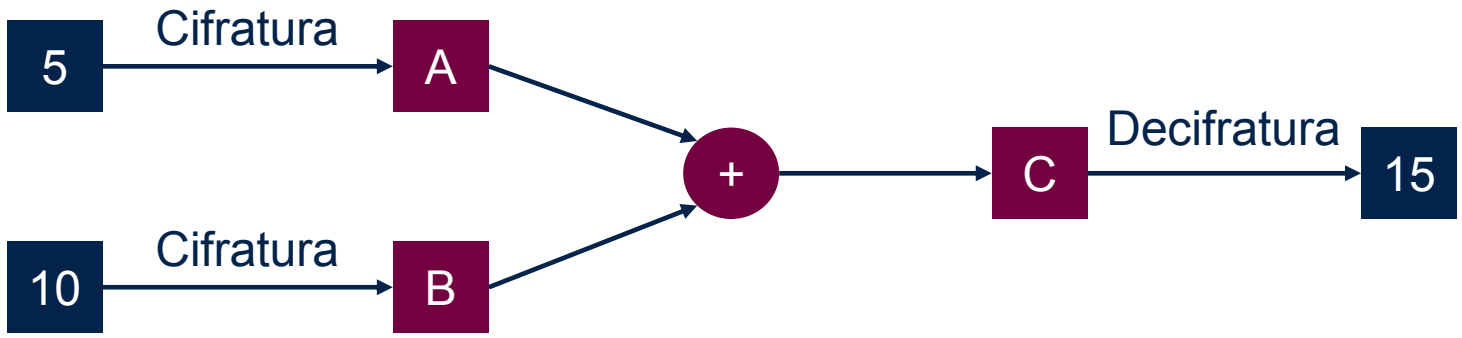
Homomorphic Encryption



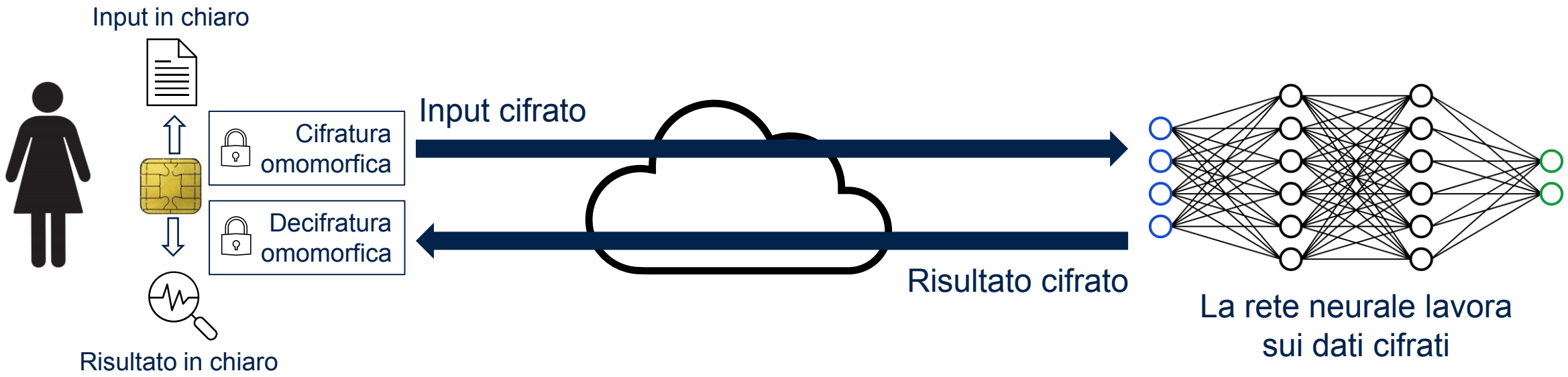
life.augmented

Homomorphic Encryption (HE)

- La crittografia omomorfica consente di eseguire calcoli direttamente sui dati cifrati, senza la necessità che siano decifrati
- Questo garantisce la segretezza dei dati durante tutto il processo
- I risultati decifrati sono identici a quelli che si sarebbero ottenuti se le operazioni fossero state eseguite sui dati originali.



Un caso d'uso reale: secure element + HE + AI



Combinando la privacy di nuovi paradigmi di sicurezza…

…con la flessibilità del machine learning

Chiave (protetta in un secure element) ~ 80 B

Dati cifrati ~ 300 B

Chiavi di bootstrapping ~ 15.5 MB

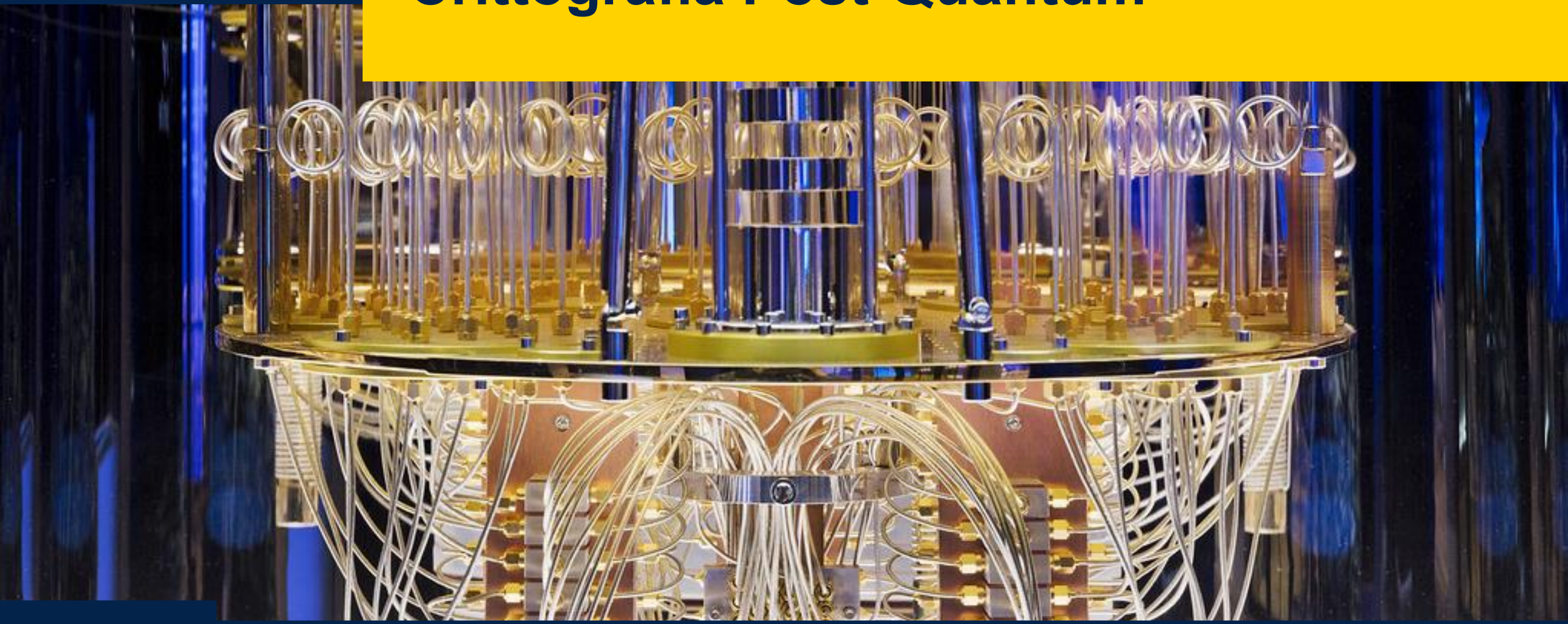
✓ Key storage

✓ Cifratura / Decifratura

✗ Chiavi di bootstrapping → *Le chiavi di bootstrapping possono essere generate in anticipo, e consegnate al cloud in modo indipendente*

life.augmented

Crittografia Post-Quantum



life.augmented

Computer quantistici e crittografia

- La sicurezza della crittografia si basa sull'intrattabilità di certi problemi per i computer moderni.
  - Esempi: RSA e fattorizzazione di interi; ECC e il problema del logaritmo discreto.
- I computer quantistici offrirebbero un significativo aumento di velocità, rispetto ai computer classici, sulla risoluzione di tali problemi

Crittografia Post-Quantum (PQC)

- Anche conosciuta come “quantum-safe” o “quantum-resistant”
- Algoritmi che funzionano su dispositivi classici, e sono considerati sicuri da attacchi fatti grazie a computer quantistici
- Si basano su diversi paradigmi:
  - Reticoli (es. ML-KEM. ML-DSA)
  - Codici (es. Classic McEliece)
  - Funzioni di Hash (es. SLH-DSA, LMS, XMSS)
  - e altri ancora…

Svantaggi degli algoritmi PQC

- Alto consumo di memoria RAM
- Dimensioni maggiori per gli elementi in uso (chiavi, firme digitali, ecc.)
  - Es. diversi kB, rispetto alle decine di byte per gli attuali algoritmi basati su ECC
- Nuovi paradigmi
  - Non tutti ben conosciuti, nuovi attacchi/vulnerabilità emergono
  - Minor conoscenza su come proteggerli da attacchi fisici (es. contromisure contro SCA)

Grazie per l’ascolto! Domande?

life.augmented

Contact: matteo.bocchi@st.com