PIEMONTE
FONDI STRUTTURALI E DI INVESTIMENTO EUROPEI 2014/2020
fondo sociale europeo
ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Cybersecurity

Sicurezza informatica

v. 3.2.1 ~ apr 2022

Prof. Marco Farina

marco.farina@its-ictpiemonte.it

t.me/marcofarina

in collaborazione con:
ISTITUTI TECNICI SUPERIORI
Ministero dell'Istruzione
UNIONE EUROPEA
REGIONE PIEMONTE
per una crescita intelligente, sostenibile ed inclusiva
www.regione.piemonte.it/europa2020
INIZIATIVA CO-FINANZIATA CON FSE

Public Service Announcement

Who am I?	Marco Farina, insegno informatica e reti al Maxwell di Nichelino.
Cybersec?	Non lavoro nel campo, ma sono appassionato di *cybersec* e *AI*.
Topics?	Cybersecurity, crittografia, sicurezza web/cloud/database, laboratorio.
Handout?	Slide a fine lezione, **appunti** e **attenzione**.
Exam?	Sulla teoria, una parte a risposta chiusa, una parte aperta.
Questions?	Meglio una domanda in più adesso che un esame a settembre.

POR Piemonte
FSE 2014-2020

ITS
TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

1

Introduzione alla cybersecurity

Cos'è la sicurezza?

Valutazione del rischio

Il rischio è la probabilità che accada un certo evento capace di causare un danno.

È implicata l'esistenza di una sorgente di pericolo, detta minaccia, e delle possibilità che essa si trasformi in un danno.

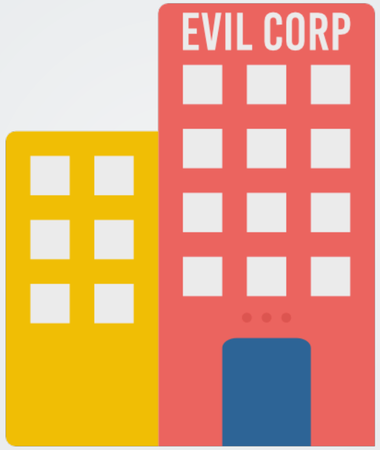
$$r = p \cdot d$$

Il rischio è uguale alla probabilità che si verifichi l'evento moltiplicata per la gravità del danno.

Cos'è la sicurezza informatica?

Protezione dei dati, dei dispositivi e dei sistemi interconnessi.

Livello personale



Livello aziendale

Livello nazionale

[POR Piemonte FSE 2014-2020]

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Cos'è la sicurezza informatica?

Protezione dei dati, dei dispositivi e dei sistemi interconnessi.

Livello personale

Cosa vogliamo proteggere?

Finanze

Sanità

Identità

Social

Lavoro

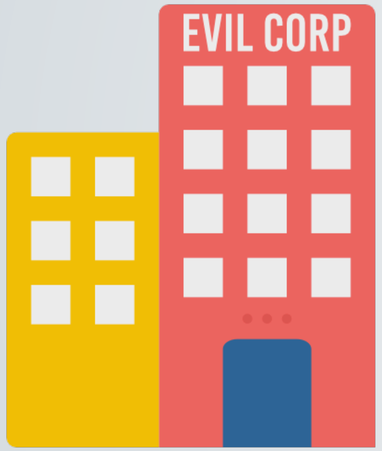
Dispositivi

[POR Piemonte FSE 2014-2020]

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Cos'è la sicurezza informatica?

Protezione dei dati, dei dispositivi e dei sistemi interconnessi.

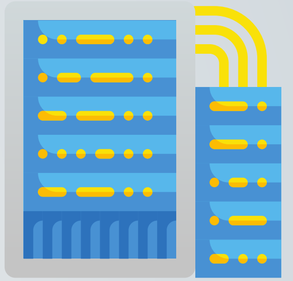


Livello aziendale

Cosa vogliamo proteggere?

Idee e brevetti

Finanze



Hardware
Software

Dipendenti

Clienti

Dati

POR Piemonte
FSE 2014-2020

ITS
TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Cos'è la sicurezza informatica?

Protezione dei dati, dei dispositivi e dei sistemi interconnessi.

Livello nazionale

Cosa vogliamo proteggere?

Cittadini

Energia

Comunicazione

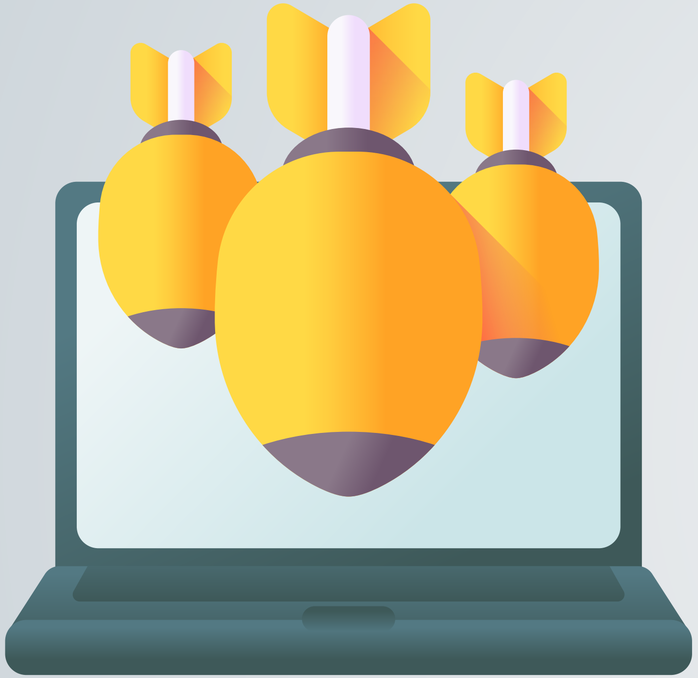
Segreti

Intelligence

Cyberwarfare


The future of cyberwarfare
Cracking Stuxnet
TED
Uploading.

Cyberwarfare



Uso di arsenali digitali per attaccare una nazione, causando danni comparabili alla guerra tradizionale.

- Spionaggio internazionale
- Sabotaggio delle infrastrutture
- Propaganda
- Shock economico

Entry level

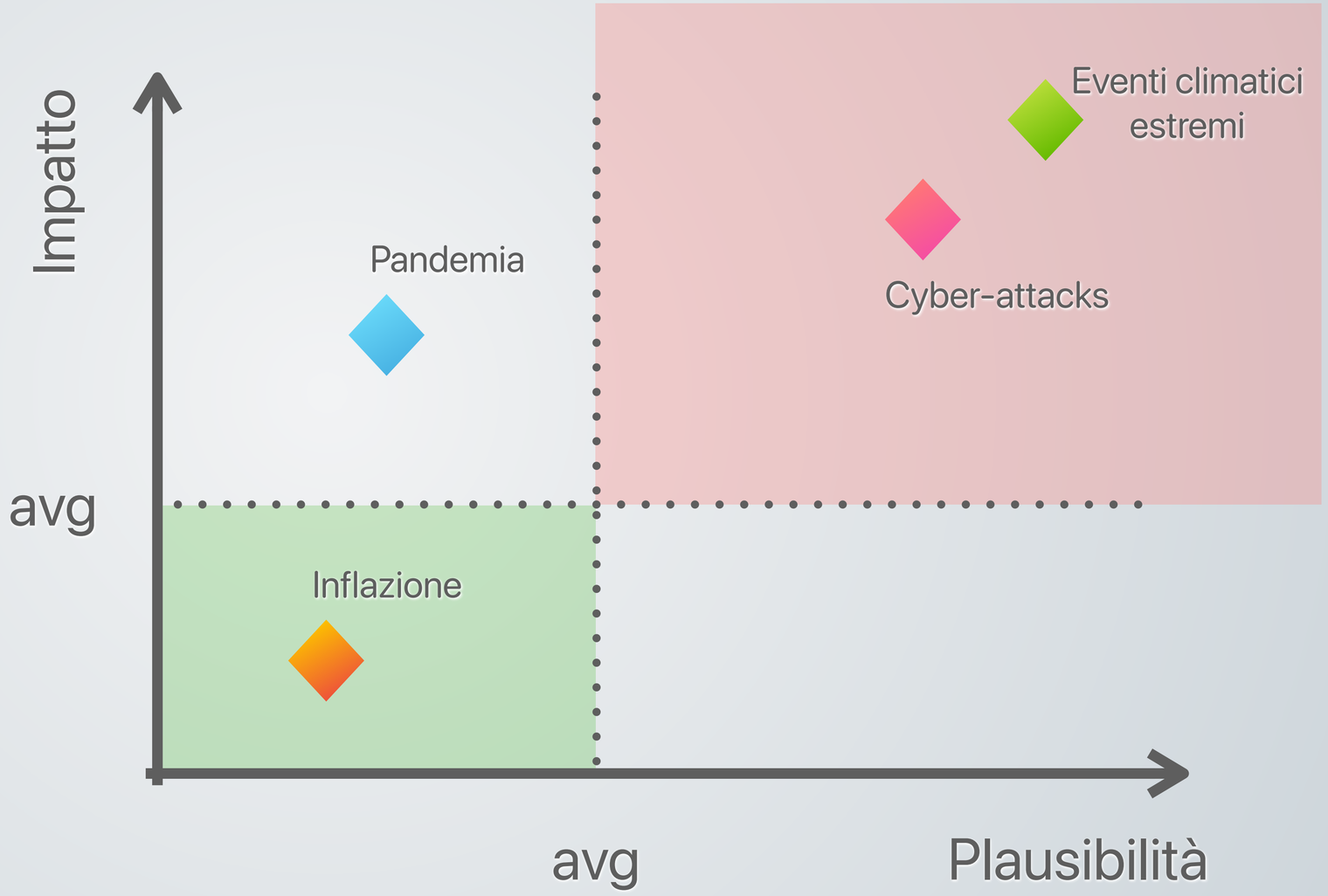
estremamente basso

Danni

potenzialmente devastanti

Cyberwarfare

The Global risk landscape, 2019
World Economic Forum



La triade C.I.A.

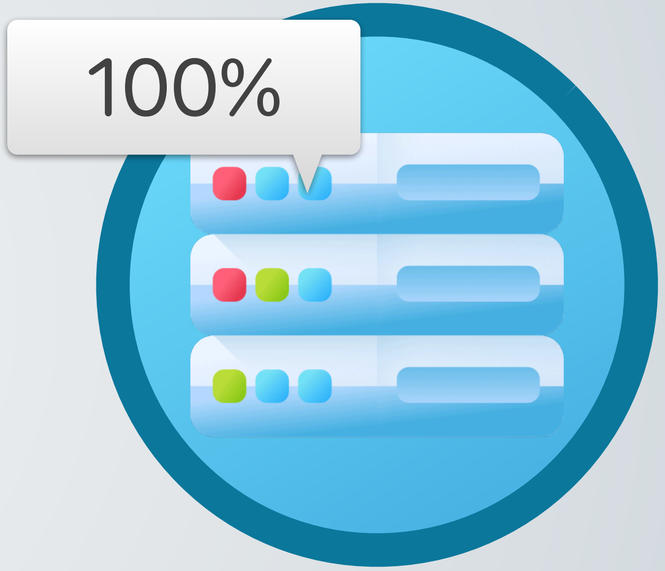
Indipendentemente dal livello, la triade C.I.A. è il concetto fondamentale.

Confidentiality

Confidenzialità

Integrity

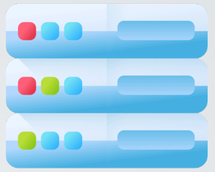
Integrità



Availability

Disponibilità

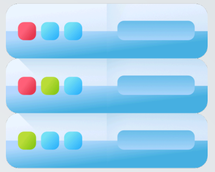
Confidenzialità



È la proprietà che indica che le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.

Il concetto non è strettamente sinonimo di privacy, ma un componente della privacy implementato per proteggere i dati da visualizzazioni non autorizzate.

Integrità

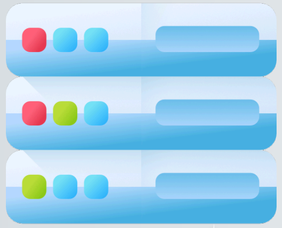


Assicura che la completezza e l'accuratezza dei dati venga mantenuta durante il loro intero ciclo di vita.

Il concetto non è strettamente sinonimo di integrità referenziale dei database, anche se può essere vista come un caso speciale di consistenza.

La crittografia è lo strumento più utilizzato perché assieme all'integrità fornisce anche la confidenzialità.

Disponibilità



100%

Affinché i sistemi informativi assolvano la propria funzione, le informazioni devono essere disponibili quando richieste.

I sistemi di memorizzazione e calcolo, i controlli di sicurezza e i canali di comunicazione devono essere sempre funzionanti.

Uno dei più grandi sforzi è compiuto nel prevenire gli attacchi di tipo **Denial of Service**.

POR Piemonte
FSE 2014-2020

ITS
TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

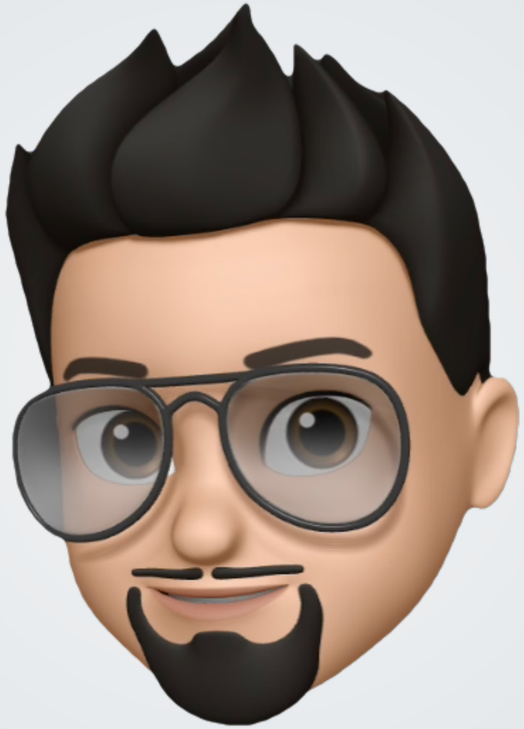
2

Attacks & attackers

Meet Alice, Bob & Eve

Alice

il mittente



Bob

il destinatario

Eve

l'attaccante

Tipologie di attacchi

Attivi

Mascheramento
(*spoofing*)

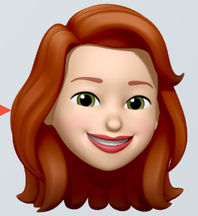
Ripetizione
(*replay*)

Modifica

Ripudio

Denial of Service

Il sistema o le risorse vengono alterate dall'attaccante.



Tipologie di attacchi

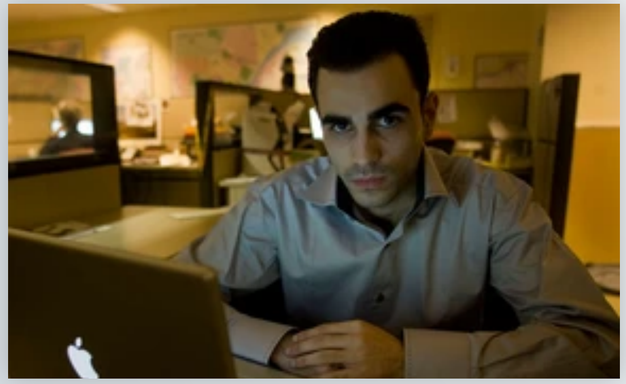
Passivi

Lettura dei messaggi

Analisi e statistiche

Cyber attackers

"Script kiddies"



- Abilità limitate
- Uso di tool professionali
- Danni potenzialmente devastanti
- Tracce spesso non coperte

Mafiaboy (2000): 15 anni, denial of service causa 1,7$ miliardi di danni.

Cyber attackers

White hat
Classe

Legale buono
Allineamento

Comunemente conosciuto come hacker etico, è uno dei lavori più ricercati negli ultimi anni.

- Usa le sue abilità per scopi leciti e legali.
- Conduce penetration-test per scoprire vulnerabilità delle reti o dei sistemi informatici.
- Agisce con autorizzazione scritta, sotto contratto e nei limiti definiti dall'azienda committente.
- Al termine dell'attività stila un report per aiutare l'azienda a risolvere i problemi di sicurezza.

Cyber attackers

Gray hat
Classe

Caotico buono
Allineamento

Spinto dalla curiosità si aggira nel meandri del web alla ricerca di vulnerabilità zero-day.

- Compiono atti illegali, ma non per scopo di lucro.
- Sono spesso guidati dalla curiosità e dal mettere alla prova le proprie abilità di hacking.
- Le vulnerabilità vengono scoperte illegalmente o con metodi non etici.
- Risolvono le vulnerabilità scoperte sotto compenso oppure divulgano le informazioni nel web senza venderle.

Cyber attackers

Black hat
Classe

Caotico malvagio
Allineamento

Il dark web è l'habitat naturale in cui mietono vittime senza pietà.

- È un attaccante malintenzionato con intenti criminali. Lavora per causare un danno, o per prelevare informazioni private e confidenziali, con o senza vantaggio personale (profitto economico o politico).
- Mantiene segrete vulnerabilità ed exploit per sfruttarli attivamente.
- Può vendere i propri servizi sul dark web.

Cyber attackers

Organized hackers

Organizzazioni criminali

Hacktivist

State-sponsored

Cyber attackers

Minacce interne

Malicious insider	Impiegati o partner che usano i loro accessi legittimi per accedere ai dati confidenziali per un vantaggio personale.
Inside agent	Dipendenti malintenzionati neoassunti, ma alle reali dipendenze di una parte esterna che ruba, altera o cancella dati riservati.
Emotional employees	Dipendenti emotivi che causano danno all'azienda per vendetta in seguito ad un torto subito (a ragione o meno).
Reckless employees	Dipendenti o terze parti che non accettano le regole delle policy di sicurezza dell'azienda.
Third-party users	Un collaboratore che si avvantaggia dell'accesso ai dati per compromettere la sicurezza delle informazioni.

POR Piemonte FSE 2014-2020

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

3

Vulnerabilità e malware

Vulnerabilità

È un punto debole del sistema in cui le misure di sicurezza sono assenti, ridotte o compromesse.

Zero Day

Una qualunque vulnerabilità non nota agli sviluppatori. Costituiscono una grave minaccia alla sicurezza.

Exploit

Un attacco che sfrutta una vulnerabilità per eseguire un rootkit o per creare comportamenti imprevisti nel sistema.

Rootkit

Un software malevolo in grado di mascherare la propria presenza ideato per abilitare l'accesso ad un sistema.

Backdoor

Un metodo alternativo all'autenticazione per superare le difese informatiche di un sistema.

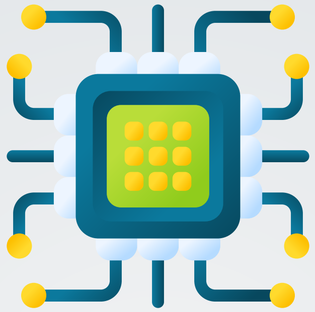
POR Piemonte
FSE 2014-2020

ITS
TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Vulnerabilità

Software

- Buffer overflow
- Injection
- Broken authentication
- Broken access control
- Security misconfiguration
- ...



Hardware

- Spectre & Meltdown
- Rowhammer
- Directory trasversal
- Secure Enclave
- ...

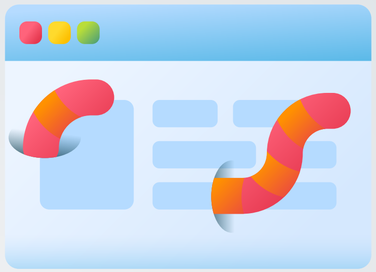
Protocolli

- Procedure di sicurezza
- Controllo degli accessi
- Componenti obsoleti
- Sicurezza fisica
- ...

Malware

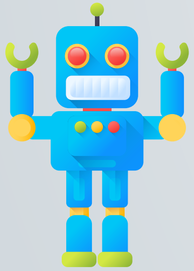
Virus

Trojan



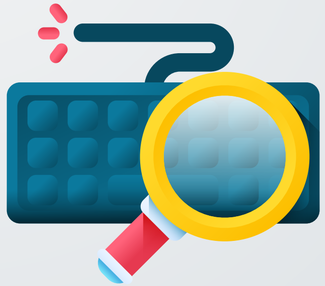
Worm

Ransomware



Botnet

Spyware



Keylogger

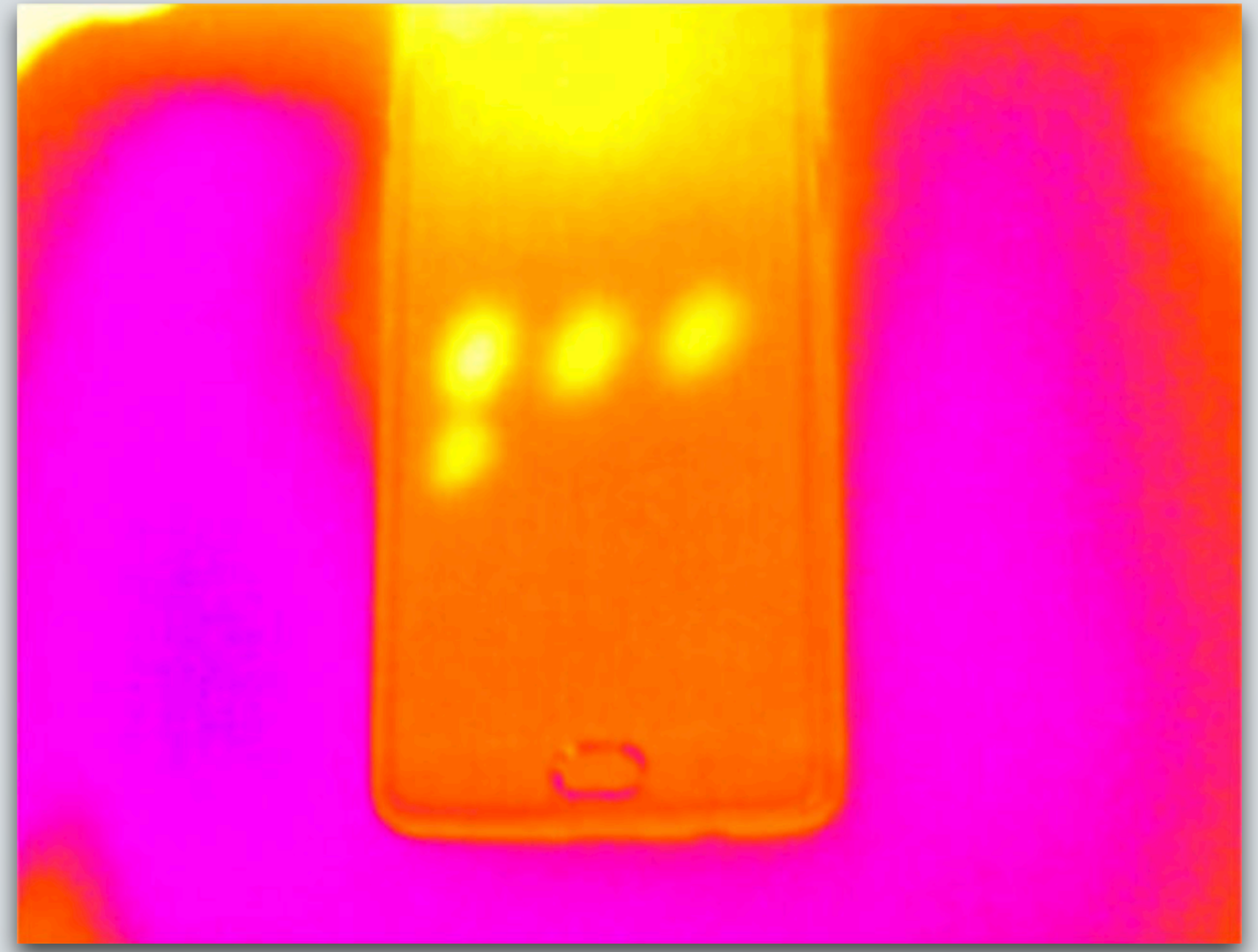
Scareware / Rogueware

Le vulnerabilità sono ovunque.

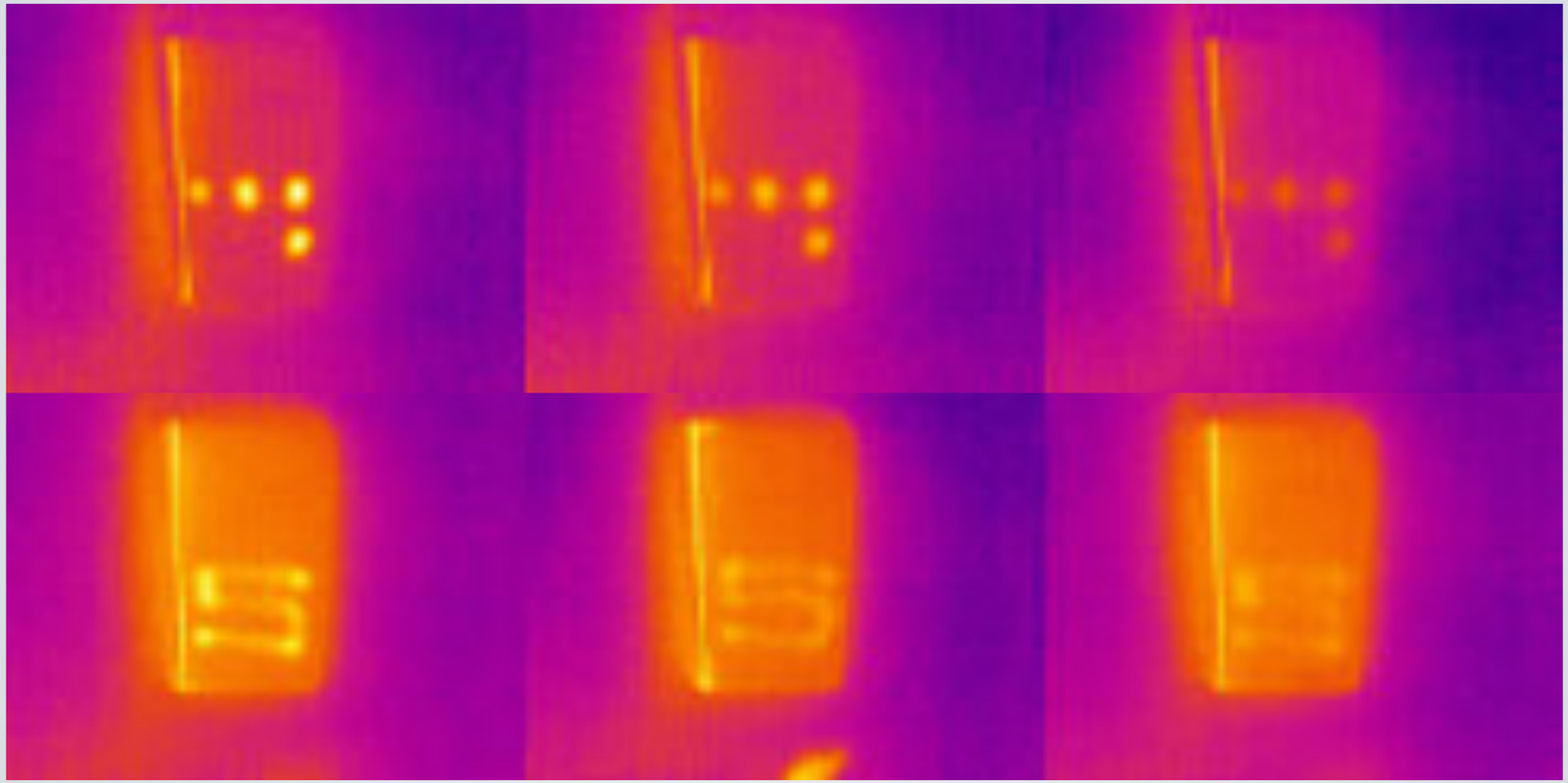
Un attaccante si appiglierà a qualunque cosa.

Cosa sta succedendo secondo voi?

Thermal attacks



Thermal attacks



0 secondi 30 secondi 60 secondi

Keystroke attack

Behavioral Acoustic Emanations: Attack and Verification of PIN Entry Using Keypress Sounds

by **Sourav Panda** [1], **Yuanzhen Liu** [2], **Gerhard Petrus Hancke** [2,*] and **Umair Mujtaba Qureshi** [2,3]

[1] Department of Computer Science and Engineering, University of California, Riverside, CA 92521, USA
[2] Department of Computer Science, City University of Hong Kong, Hong Kong, China
[3] Department of Telecommunication Engineering, Mehran University of Engineering and Technology, Jamshoro 76062, Sindh, Pakistan
* Author to whom correspondence should be addressed.

Sensors **2020**, *20*(11), 3015; https://doi.org/10.3390/s20113015

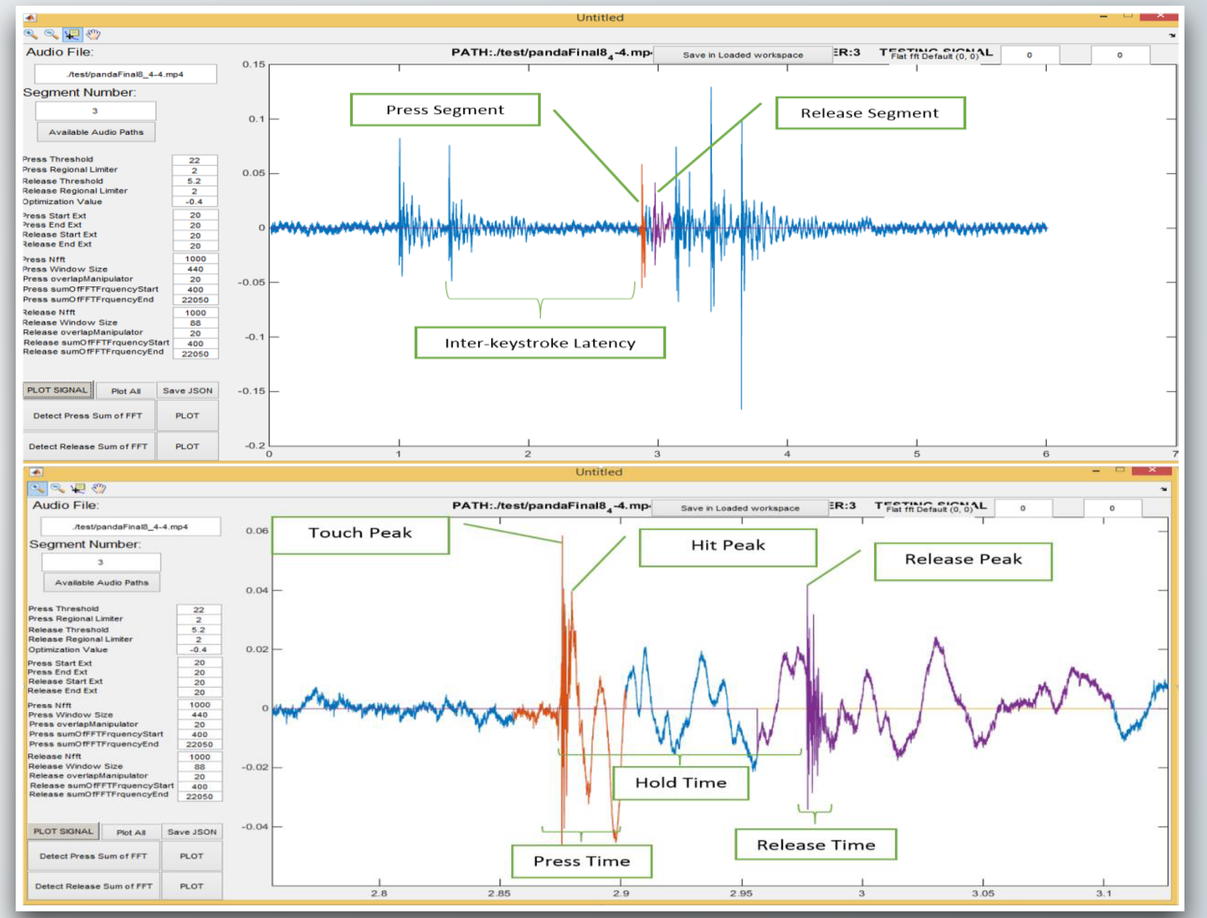
Received: 29 April 2020 / Revised: 20 May 2020 / Accepted: 22 May 2020 / Published: 26 May 2020

RESEARCH-ARTICLE

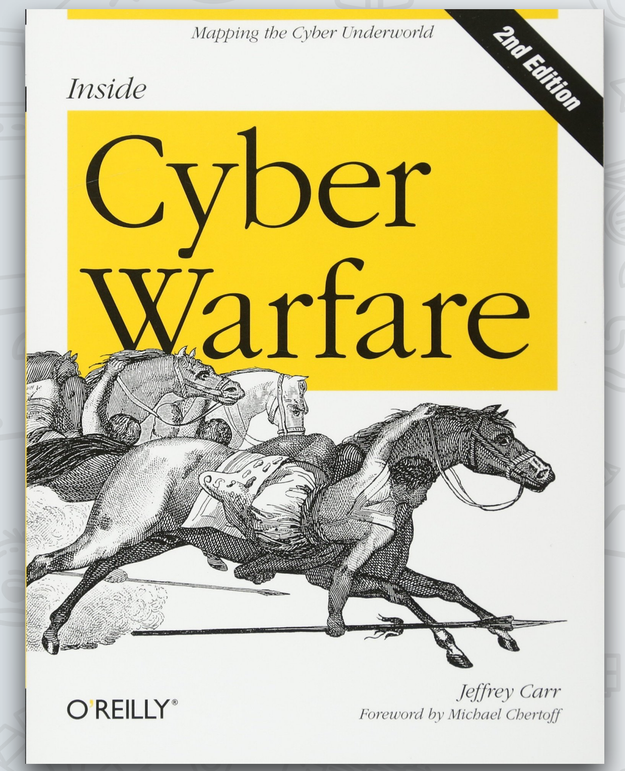
(sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers

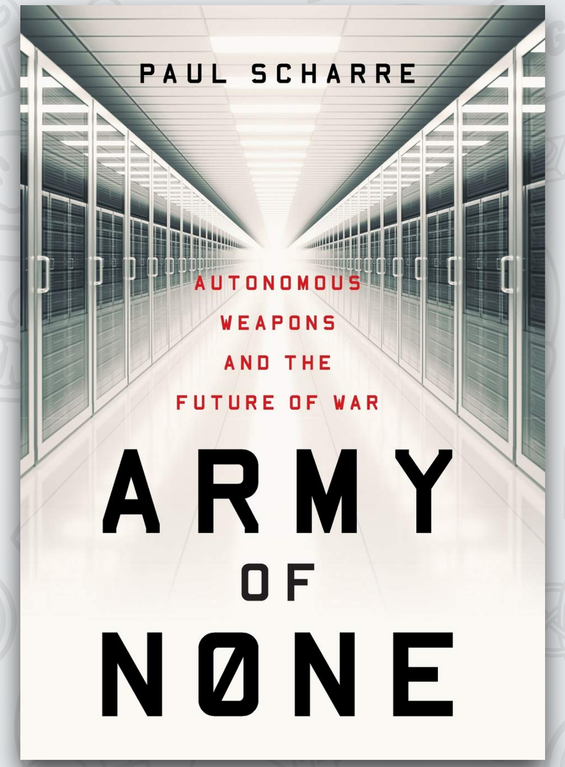
Authors: Philip Marquardt, Arunabh Verma, Henry Carter, Patrick Traynor Authors Info & Affiliations

Publication: CCS '11: Proceedings of the 18th ACM conference on Computer and communications security • Oc
• Pages 551–562 • https://doi.org/10.1145/2046707.2046771



Approfondimenti e bibliografia





CISCO
Networking Academy

Introduction to cyber security