UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

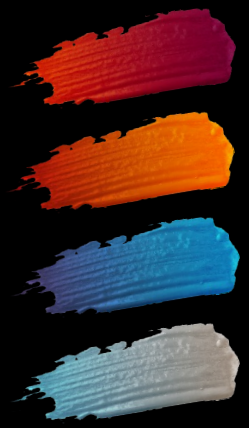
SERLAB
Software Engineering Research

Corso di laurea in
INFORMATICA

Cyber attack and defense simulation for a DRONE

Relatore:
Chiar.mo Prof. Danilo Caivano
Dott.ssa Vita Santa Barletta

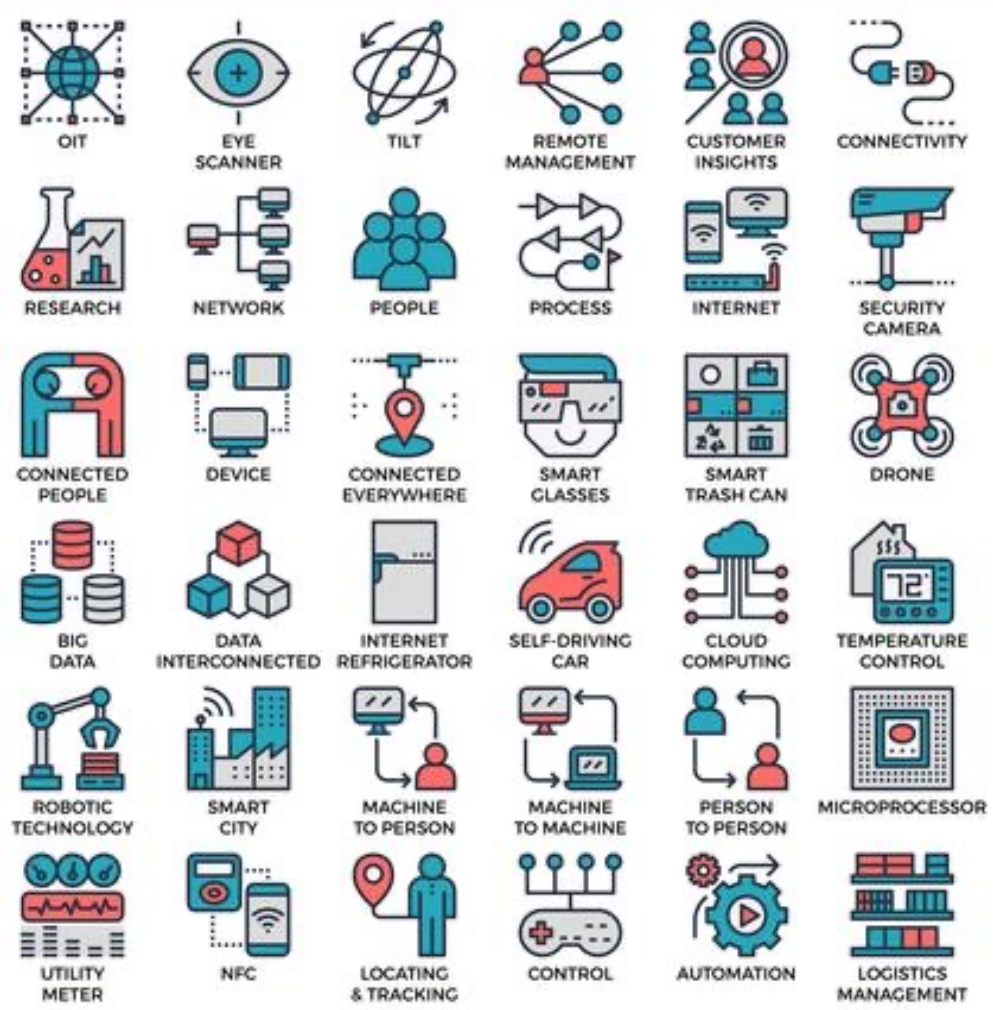
Laureando:
Arcangelo Saracino



Chi sono

- Classe ’98
- Esperienze lavorative:
  - Web Developer (Aryma)
  - Web Developer (Enterprise DS)
  - Security Analyst (Hacktive Security)

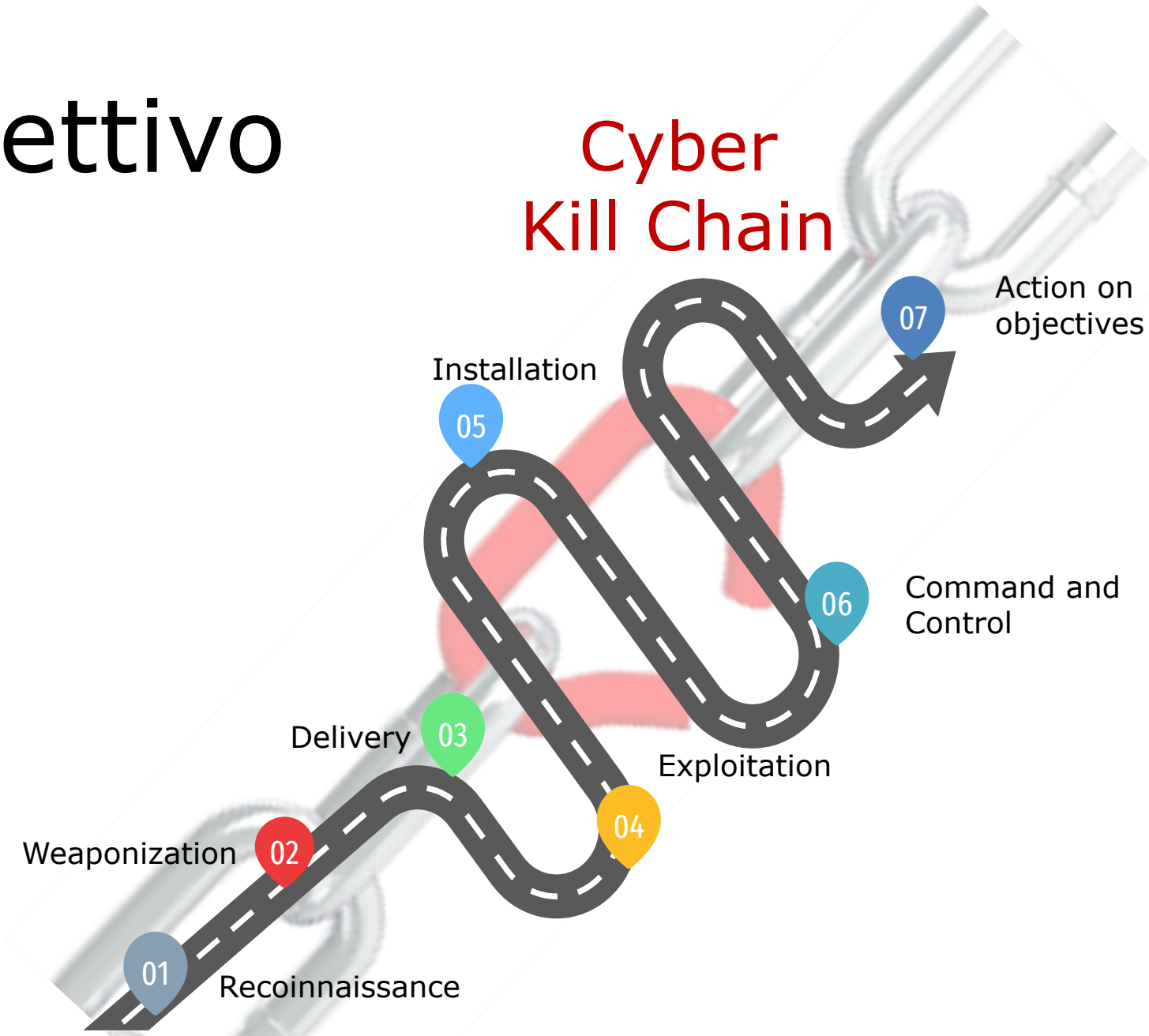
Contesto



IoT

Internet of Things

Obiettivo


Cyber
Kill Chain
01
Recoinnaissance
02
Weaponization
03
Delivery
04
Exploitation
05
Installation
06
Command and
Control
07
Action on
objectives

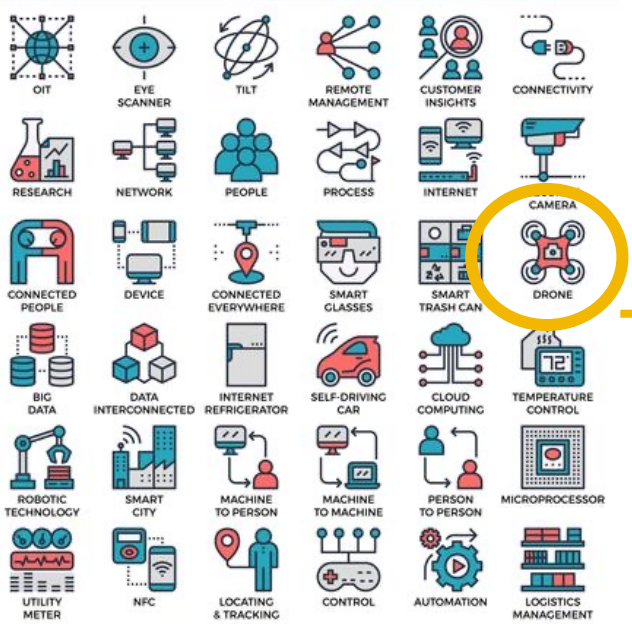
“IoT Cyber Kill Chain

IoT Cyber kill chain

Fasi della kill chain

- Capire lo scopo (Reconnaisance/Weaponization)
- Mappatura della superfice d’attacco (Delivery/Exploitation)
- Valutazione delle vulnerabilità ed exploitation (Installation/Command and Control/Action on objectives)
- Documentazione e report

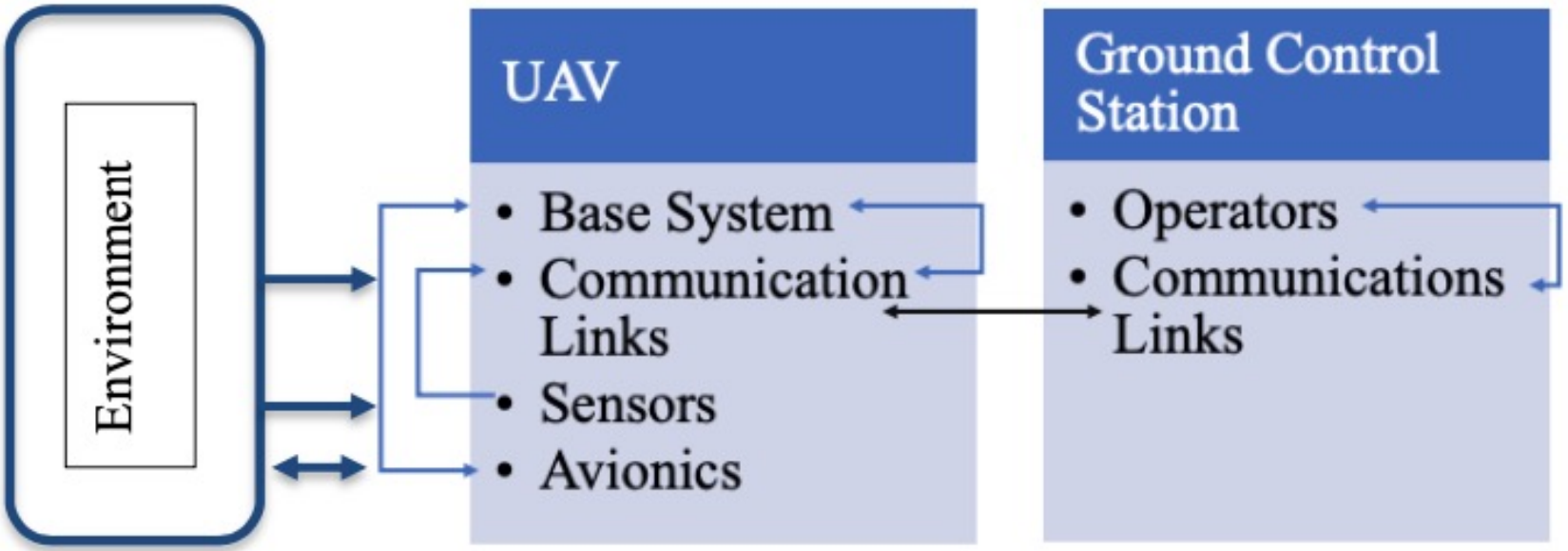
I droni



Drone

Drone

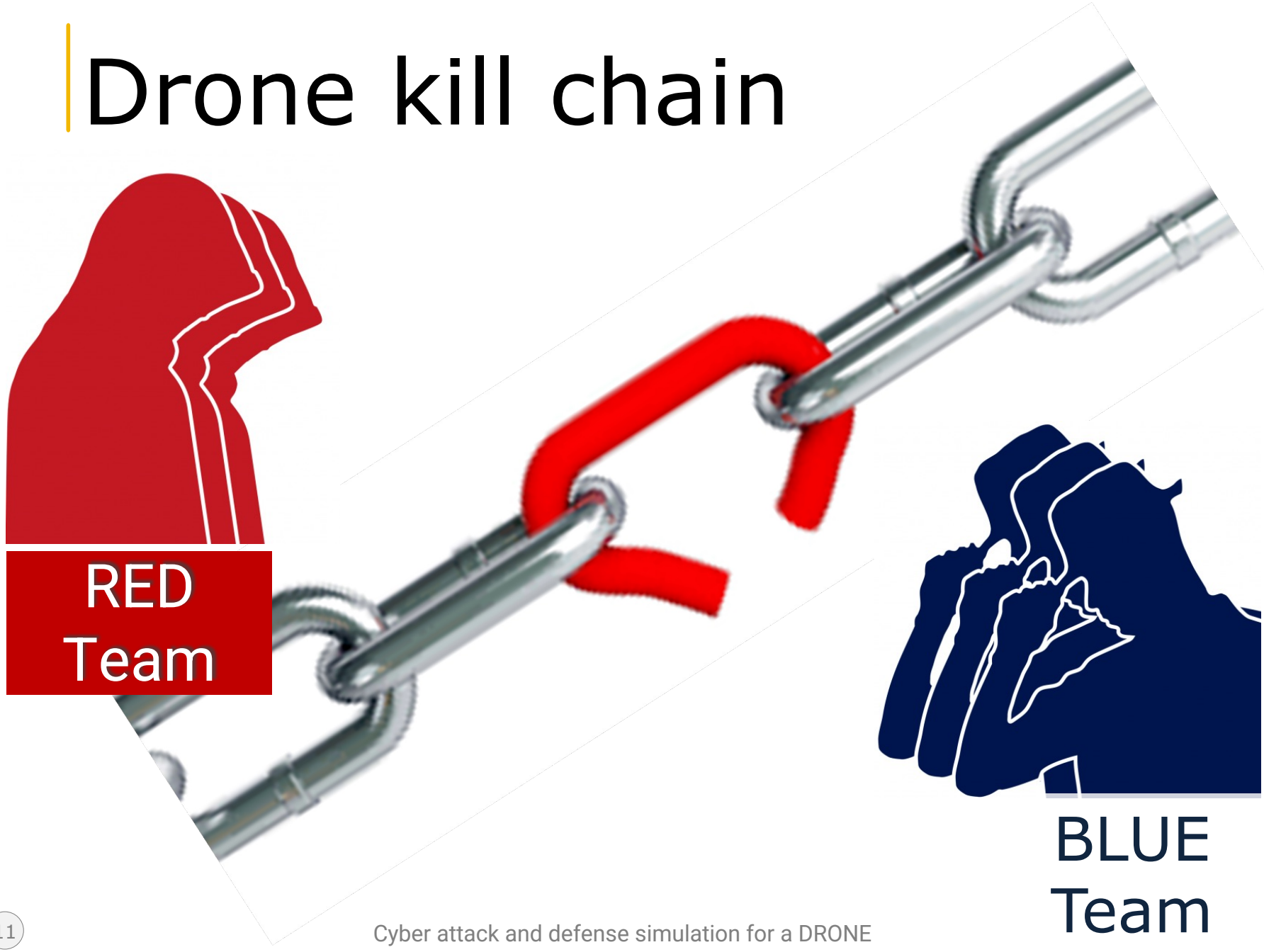
Macrocomponenti



Componenti comuni

- App Mobile
- Wifi Access Point
- Comunicazione Radio
- Servizi di rete
- Sensore di telemetria / GPS

Drone kill chain



Red vs Blue

App Mobile

- Insecure Data Storage

Librerie Standard per l’encryption (IOS,Adroid).

- Hardcoded credentials/appidentifier

Rendere l’applicazione resistente ai permessi di root.

Red vs Blue

Wifi Access Point

• Multiple connection	Limitare la banda e la connessione TCP/UDP, attraverso il tuning.
• No password	Utilizzare una password sicura
• Master/Slave identification	Identificare l'utente attraverso un certificato.

Red vs Blue

Comunicazione Radio

- Comunicazione non cifrata

Utilizzare un ecryption come AES, utilizzare il processo OTAR (Over the air rekeyring)

Red vs Blue

Servizi di rete

- Servizi non sicuri esposti

Non utilizzare porte di default, utilizzare servizi sicuri (SSH,FTPS) che non permettano attacchi di sniffing

Red vs Blue

Sensore di telemetria / GPS

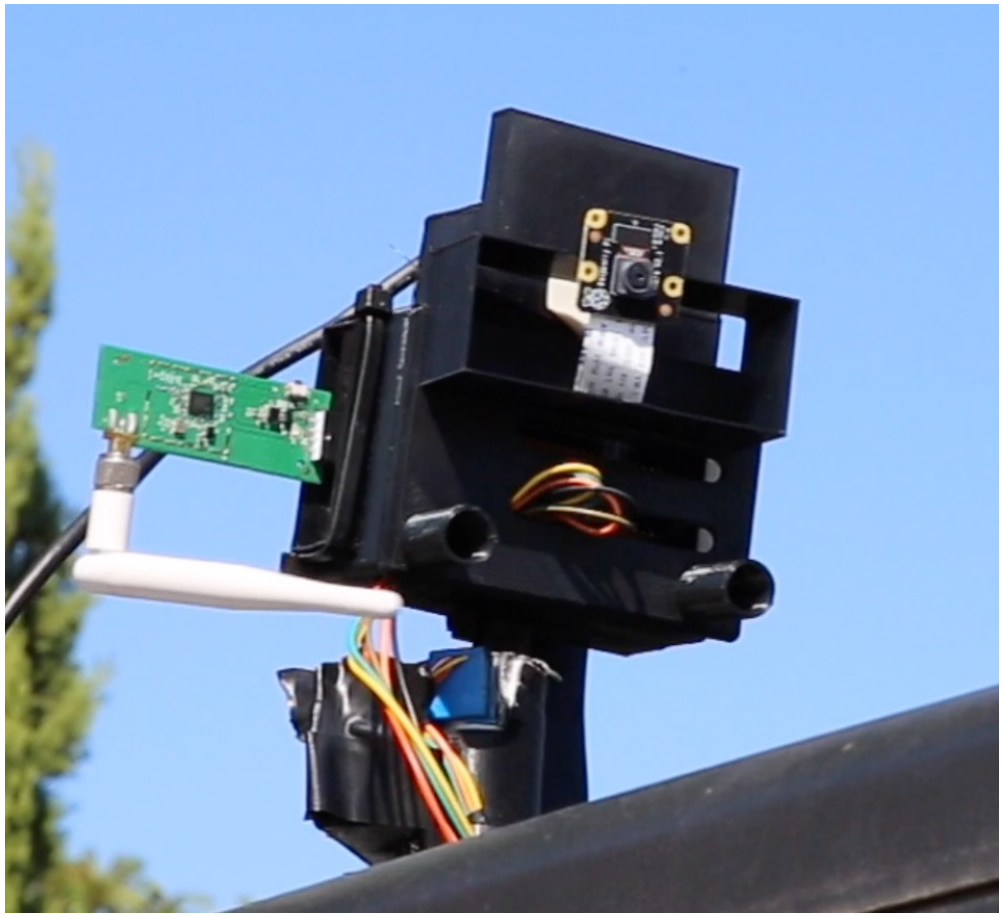
- Sensori non correttamente protetti

Rimedi simili alla comunicazione radio, ed inoltre implementare materiale che protegga il sensore da compromissioni esterne

Attacchi identificati

- Data exfiltration
- Man in the Middle (master substitution)
- Denial of Service (trasformatosi in battery draining)
- Wifi jamming/deauth
- Radio spoofing/jamming
- Gps spoofing
- Firmware update

Sperimentazione



Sperimentazione

Sviluppi futuri

Ringraziamenti

Si ringrazia il professor Danilo Caivano e la Dott.ssa Vita Santa Barletta.

Il dispositivo è stato sviluppato grazie al supporto economico e morale (☺) dell'azienda Hactive Security per la quale lavoro attualmente.