CYBER AND PHYSICAL VULNERABILITIES OF MEDICAL DEVICES - OBSERVATORY

Scientific advisor:
Prof. Gaetano Marrocco

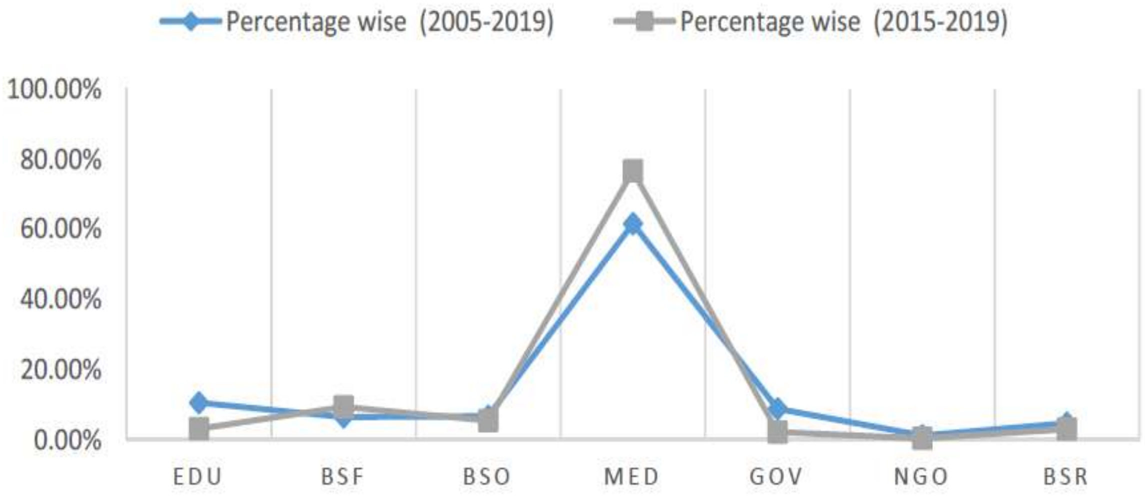
Collab.
Prof. Pierpaolo Loreti
Prof. Giuseppe Bianchi
Emanuele Raso

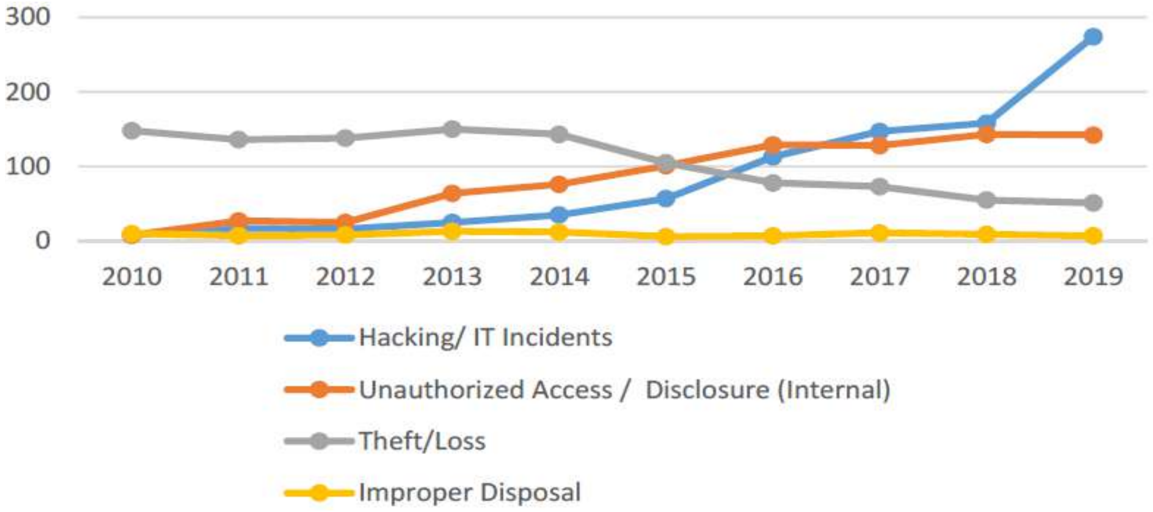
CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Francesco Lestini
Francesca Nanni

Motivation

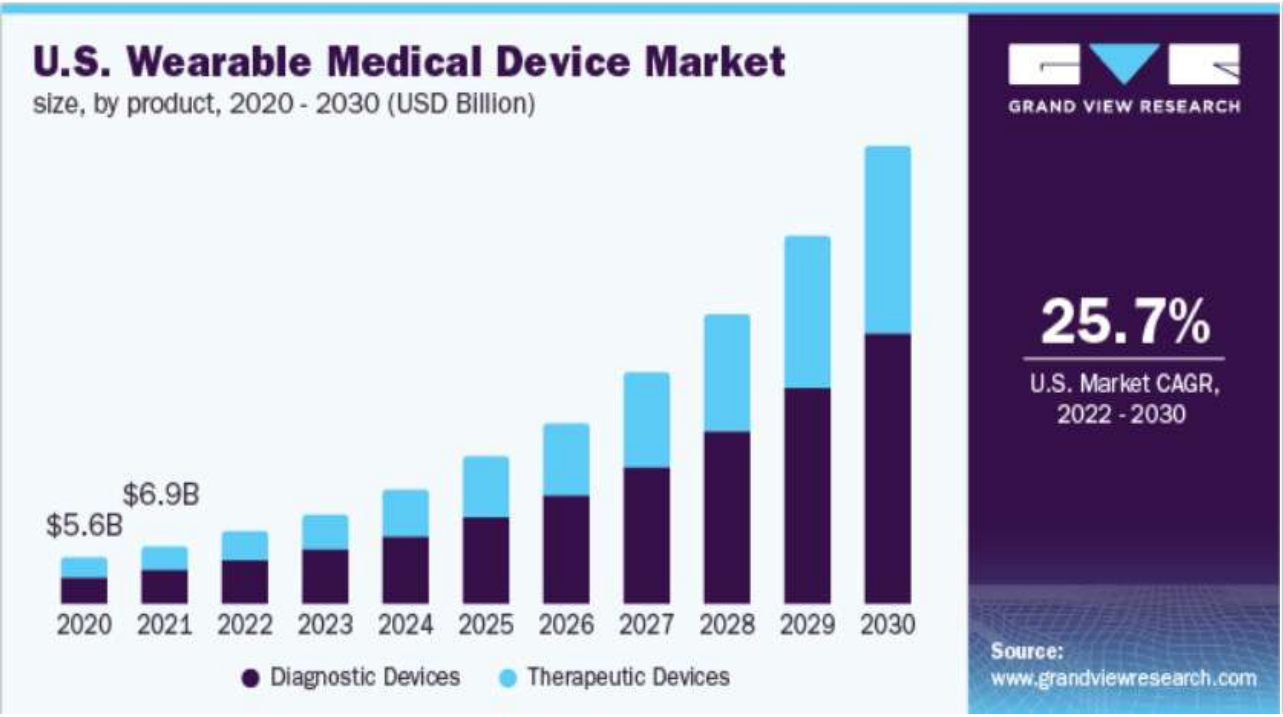
Some statistics





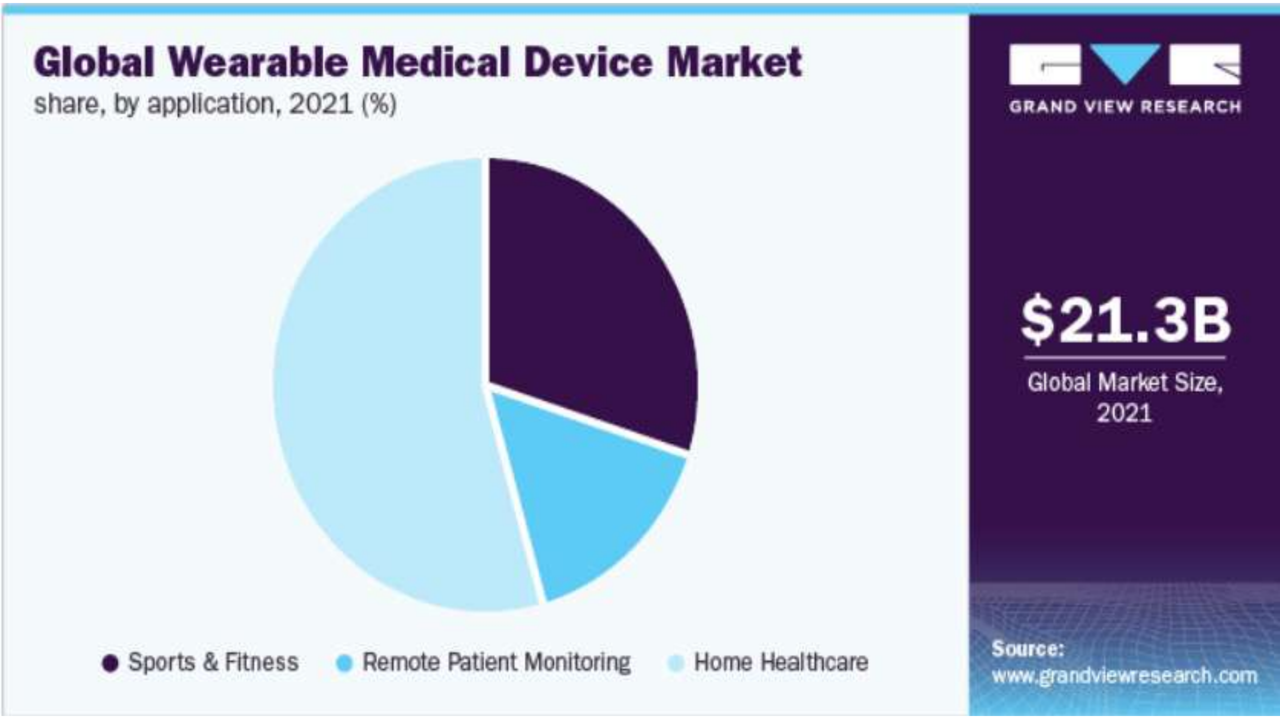
- The **healthcare industry is the preferred target of attackers** because of the high commercial value of EHRs.
- Theft/loss and improper disposal incidents have decreased in frequency, but **hacking/IT incidents and unauthorized access incidents have increased**

Motivation



U.S. Wearable Medical Device Market
size, by product, 2020 - 2030 (USD Billion)

Source:
www.grandviewresearch.com

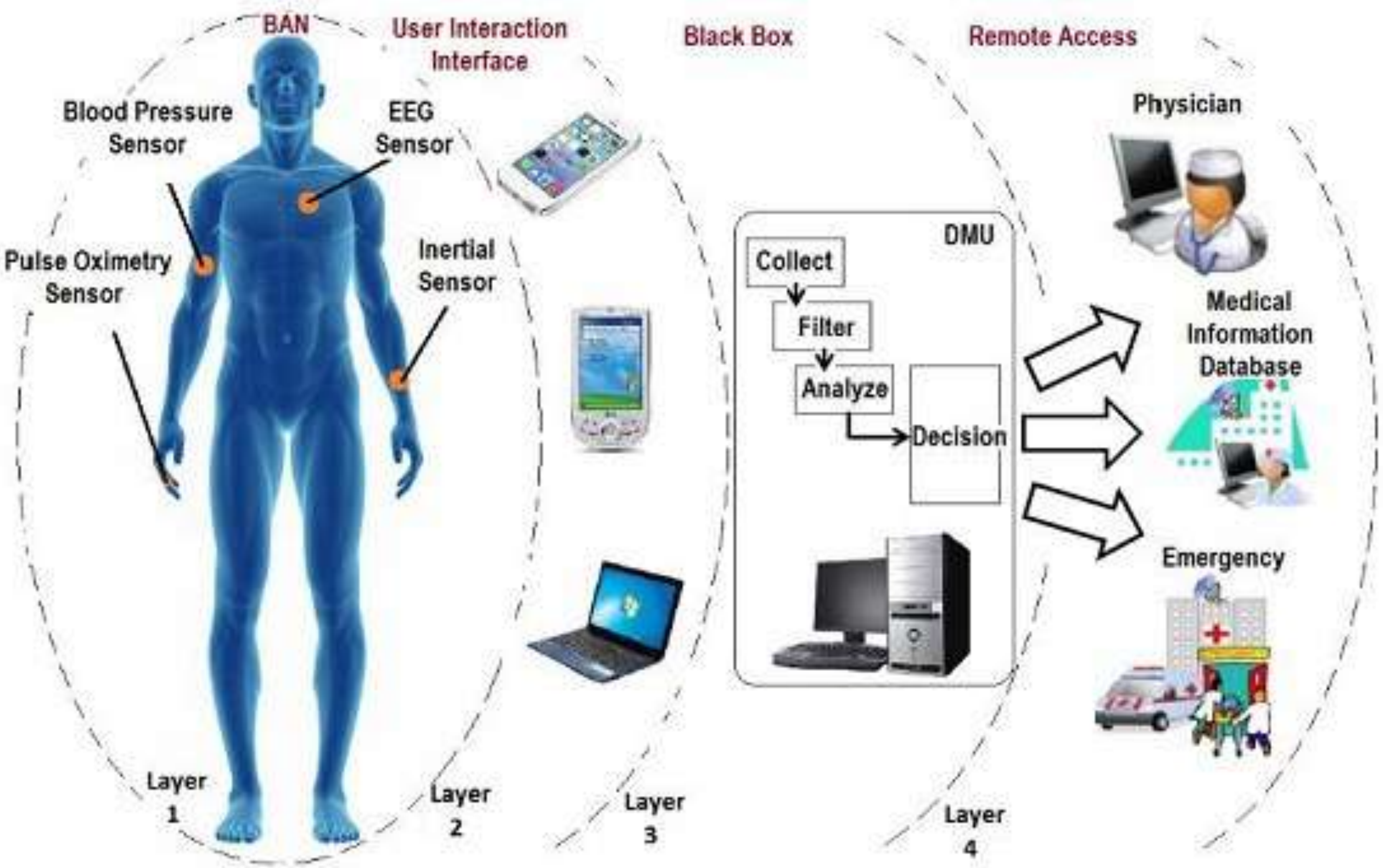


Global Wearable Medical Device Market
share, by application, 2021 (%)

Source:
www.grandviewresearch.com

Implanted and Medical Devices (IMD)

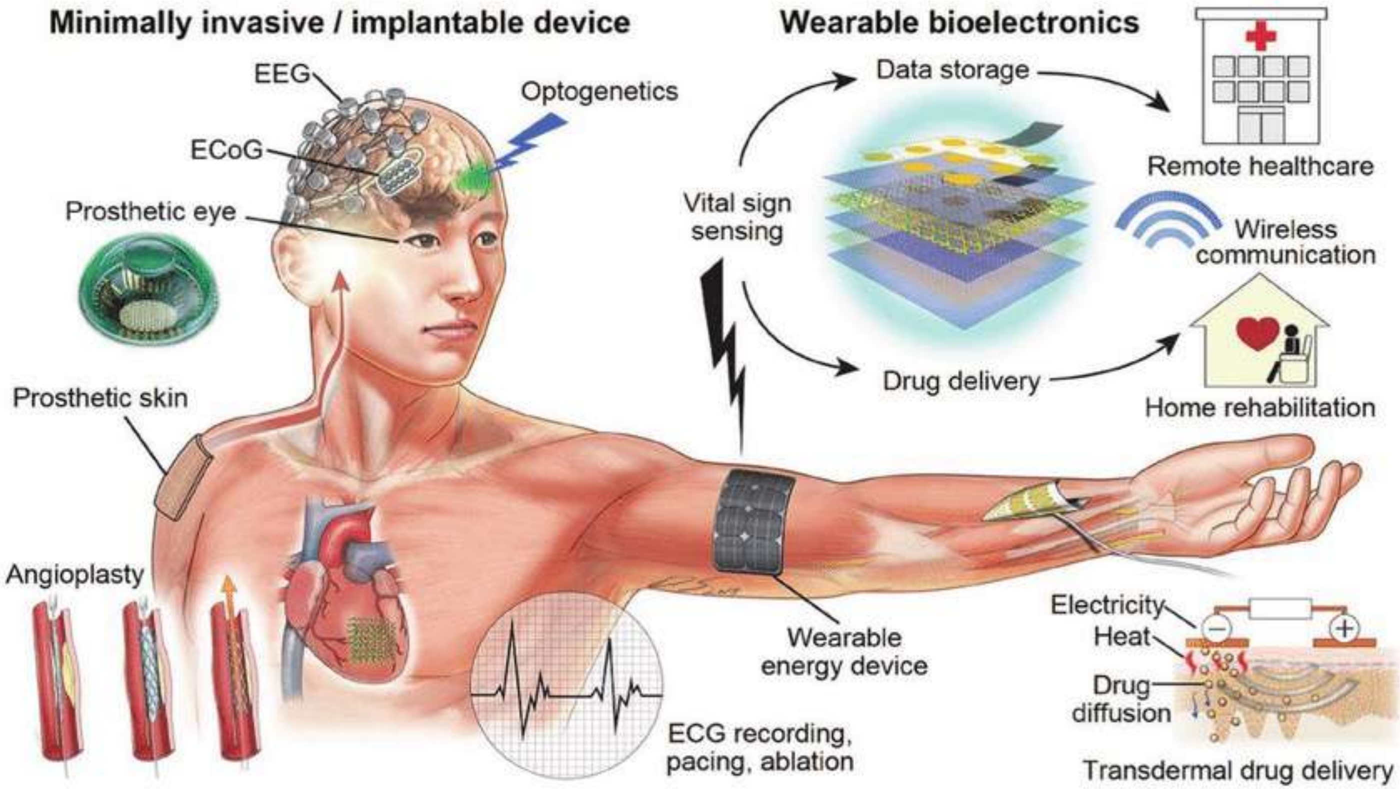
Body Area Network (BAN)



A ***body area network (BAN)*** is a wireless network of heterogeneous computing devices that are wearable.

This network enables ***continuous remote monitoring*** of patient physiological values in the medical setting.

IMD Connectivity



WIRELESS CONNECTIVITY:

- Enable remote monitoring over long-range
- Communicate with other interoperating IMDs

BENEFITS:

1. It makes it easier to communicate with the implant itself
2. It enables *remote monitoring* of the patient’s status, ***reducing hospital visits***
3. The patient can be ***in his home*** to monitor his vital signals.

IMD vulnerabilities

- **2011.** Barnaby Jack first demonstrated the **wireless hacking of insulin pumps.**

Abbott

- **2017.** Almost half a million pacemakers have been recalled by the **US FDA**, for ***lax of cybersecurity***.

Medtronic

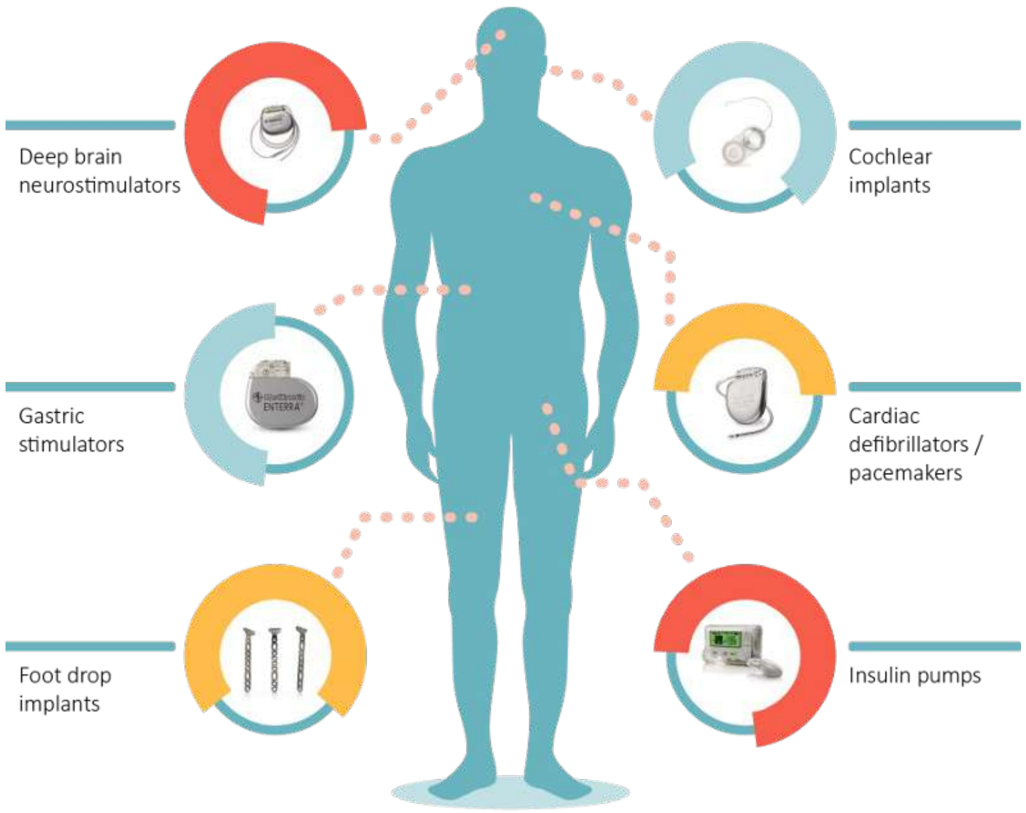
- ***2018.*** ***Billy Rios*** and ***Jonathan Butts*** demonstrated they've found vulnerabilities that compromise pacemaker's programmer.

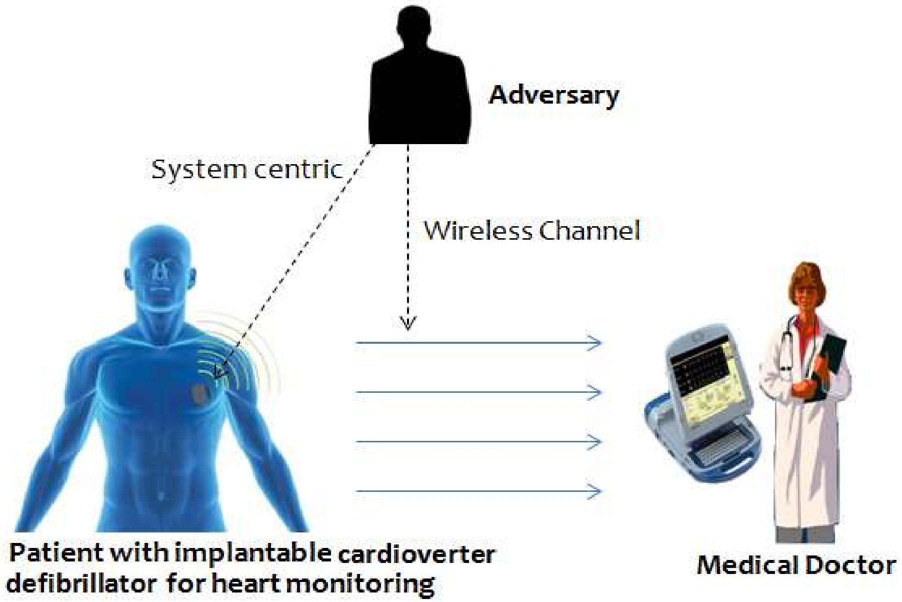
Fundamental Security Services and Attacks

Authentication	**Fabrication attack (SPOOFING)**
Confidentiality	**Interception attack (EVESDROPPING)**
Integrity	**Modification attack**
Availability	**Interruption attack (DoS)**

Cyber Threats Scenario

- So far, there has been no documentation of a patient ***dying*** from hacking, but the researchers admit that this possibility is real.



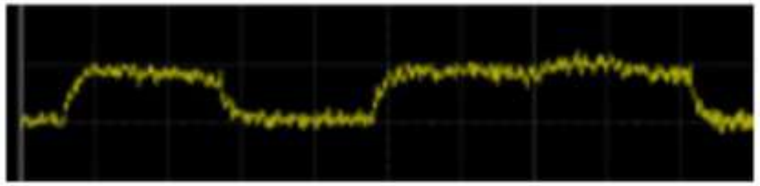

Adversary
System centric
Wireless Channel
Patient with implantable cardioverter defibrillator for heart monitoring
Medical Doctor

- System centric attack
- Wireless channel attack

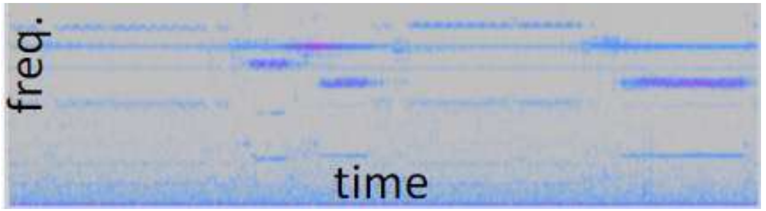
Side Channel Attacks

In computer security, a **side-channel attack** is any attack based on ***information gained from the implementation of a computer system***, rather than weaknesses in the implemented algorithm itself (e.g., cryptanalysis)

- **Timing attack** — attacks based on measuring **how much time various computations take to perform**.
- **Power-monitoring attack** — attacks that make use of **varying power consumption by the hardware** during computation.



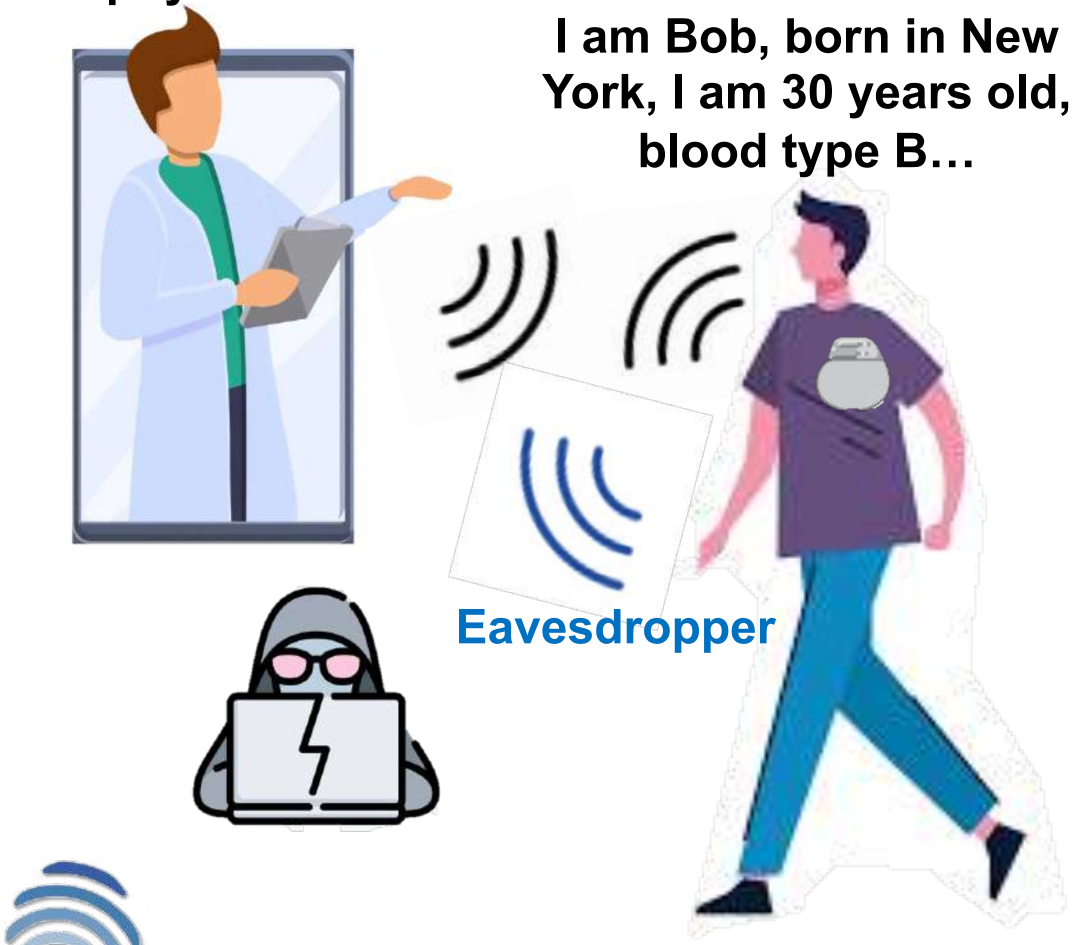
- **Differential fault analysis** — in which secrets are discovered **by introducing faults in a computation**.
- **Electromagnetic attack** — attacks based on **leaked electromagnetic radiation**, which can directly provide plaintexts and other information.



Side Channel Attacks

Data stealing/Access control

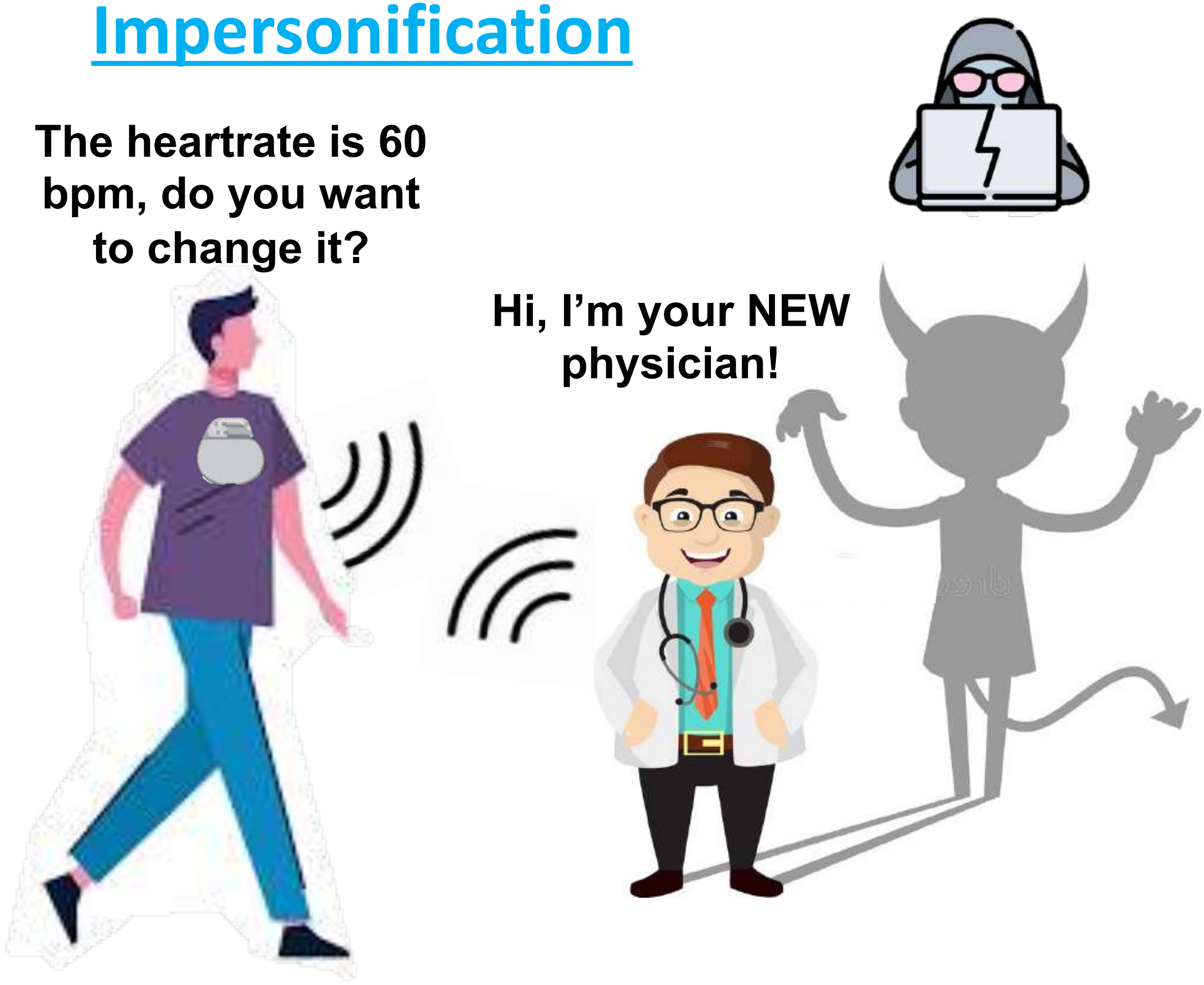
Eavesdropping



Hi, I'm your physician

I am Bob, born in New York, I am 30 years old, blood type B…

Impersonification



The heartrate is 60 bpm, do you want to change it?

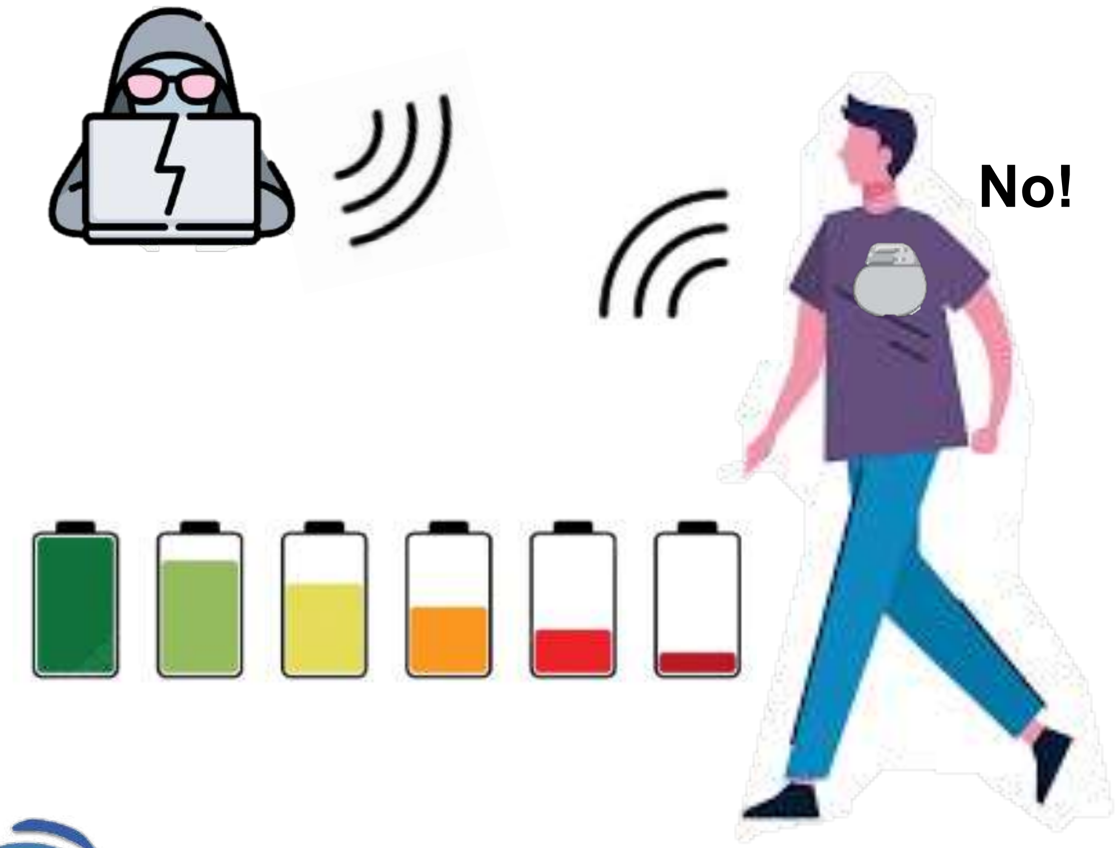
Hi, I'm your NEW physician!

Side Channel Attacks

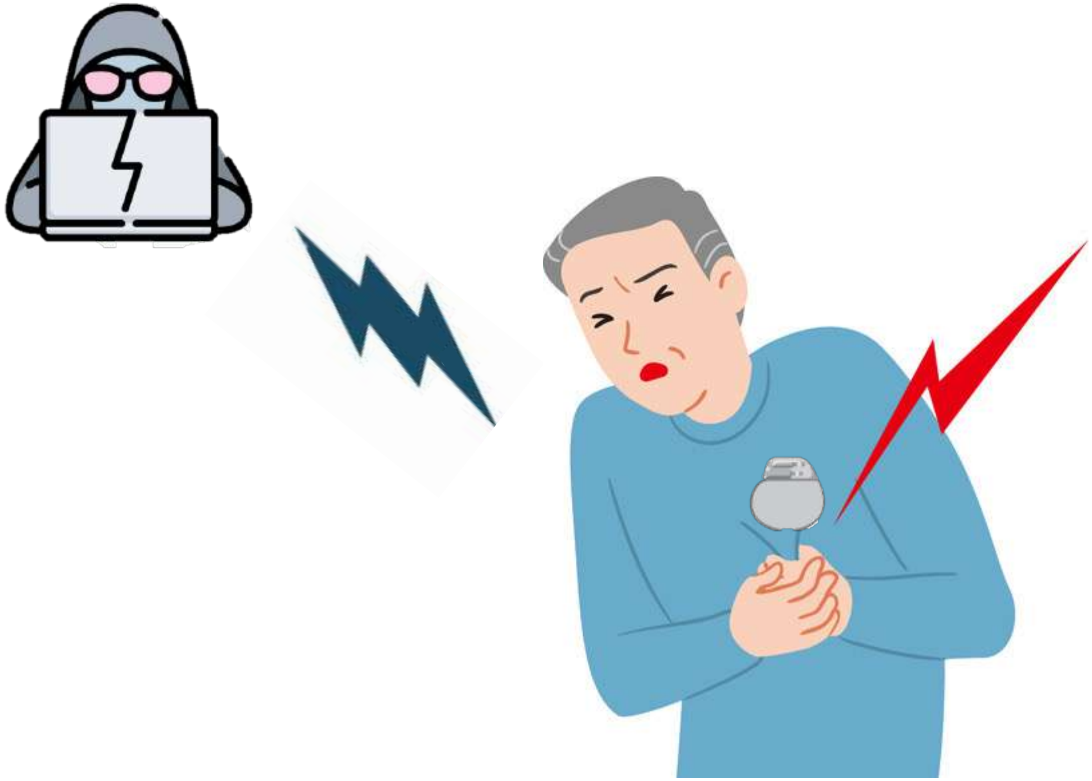
Battery draining/Fault induction

Resource Depletion

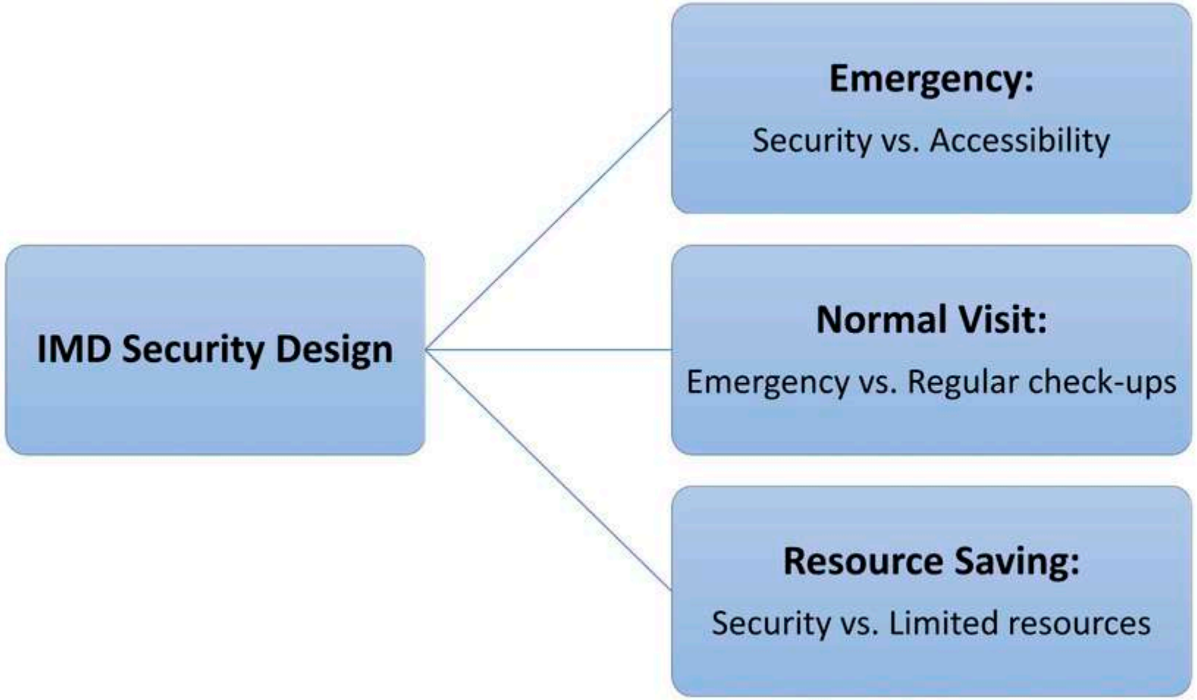
Are you sleeping?



Fault induction attack



IMD Security constrains



IMD Security Design

Emergency:
Security vs. Accessibility

Normal Visit:
Emergency vs. Regular check-ups

Resource Saving:
Security vs. Limited resources

There are ***three important aspects*** when designing an IMD security scheme:

1. ***IMD Modifications***
2. ***IMD Resource Consumption***
3. ***Patient’s Values***

MDs SECURITY

Overview

RECOMMENDED BEST PRACTICES

FDA
Regulations for Medical Devices

enisa
THE EU CYBERSECURITY AGENCY

- **MD security** refers to practices and techniques that can prevent attacks against MDs:

→ ***unauthorized access or control*** of MDs
→ ***exposure of the sensitive data*** they generate.

IoT devices are different ***from MDs***:

- Attackers gaining control of MDs may be ***life-threatening***
- Information on MDs is ***extremely sensitive***
- Medical devices are **long-lived**

CYBER4 OBSERVATORY

GOALS

- Literature scouting and classification (scientific paper, journal article)
- Classification of ***MD attacks/vulnerabilities***
- **AWARENESS**

→ User-friendly **information sharing** platform

Who will benefit?

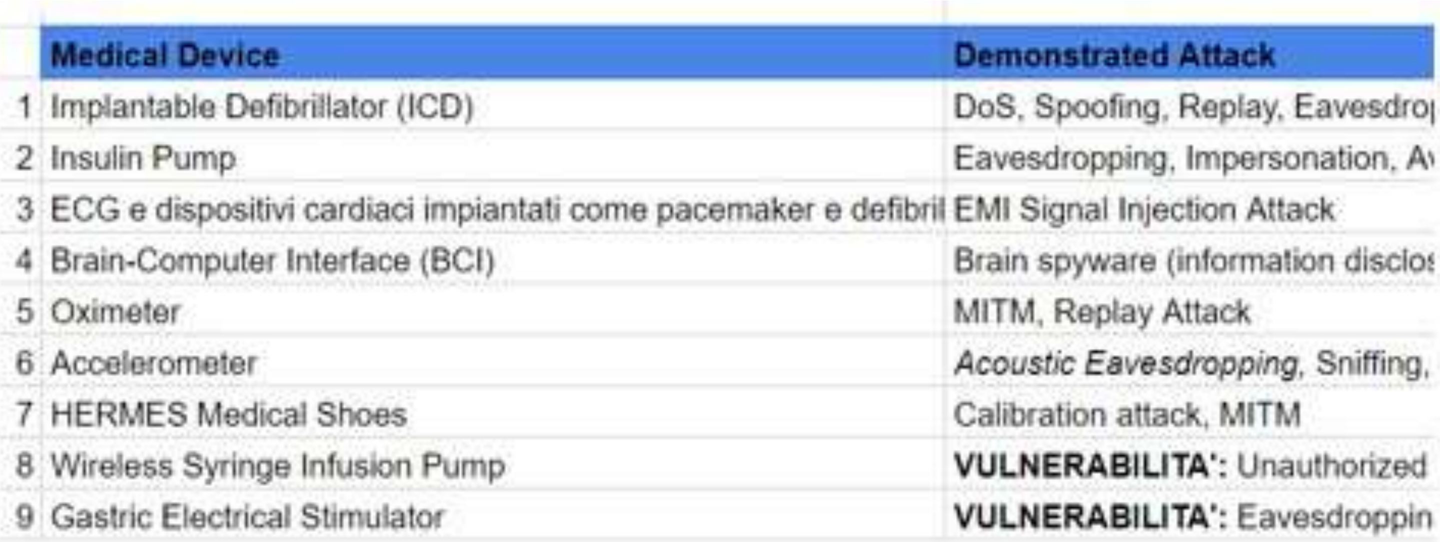
- Hospitals
- Laboratories of analysis
- MD manufacturers
- ASL
- Healthcare organizations

MISP
Threat Sharing

CYBER4 OBSERVATORY

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Università di Roma
Tor Vergata



	Medical Device	Demonstrated Attack
1	Implantable Defibrillator (ICD)	DoS, Spoofing, Replay, Eavesdro
2	Insulin Pump	Eavesdropping, Impersonation, A
3	ECG e dispositivi cardiaci impiantati come pacemaker e defibril	EMI Signal Injection Attack
4	Brain-Computer Interface (BCI)	Brain spyware (information disclos
5	Oximeter	MITM, Replay Attack
6	Accelerometer	*Acoustic Eavesdropping*, Sniffing,
7	HERMES Medical Shoes	Calibration attack, MITM
8	Wireless Syringe Infusion Pump	**VULNERABILITA'**: Unauthorized
9	Gastric Electrical Stimulator	**VULNERABILITA'**: Eavesdroppin

H-ISAC™
HEALTH - ISAC

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

RAPID7