Introduction to cyber/physical vulnerabilities of medical devices

Ing. Francesca Maria Chiara Nanni
Contacts: frmach97@gmail.com

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Scenario

2010

At a Black Hat conference Barnaby Jack gave a presentation on **"jackpotting"** or causing automated teller machines to dispense cash without withdrawing it from a bank account using a bank card

2011

At the McAfee FOCUS 11 conference in October 2011 in Las Vegas, Jack first demonstrated the **wireless hacking of insulin pumps**

2012

Jack asserted that he could assassinate a victim by **hacking their pacemaker**

2018

Billy Rios and Jonathan Butts (Rapid7) demonstrated they've found vulnerabilities that **compromised the pacemaker's programmer**

Interactions
LOCAL

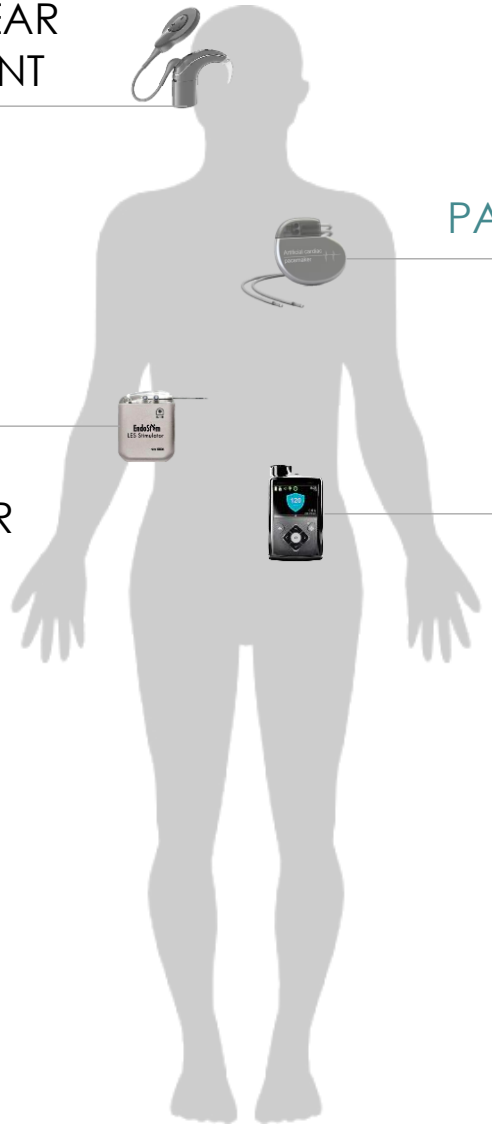
Telemetry

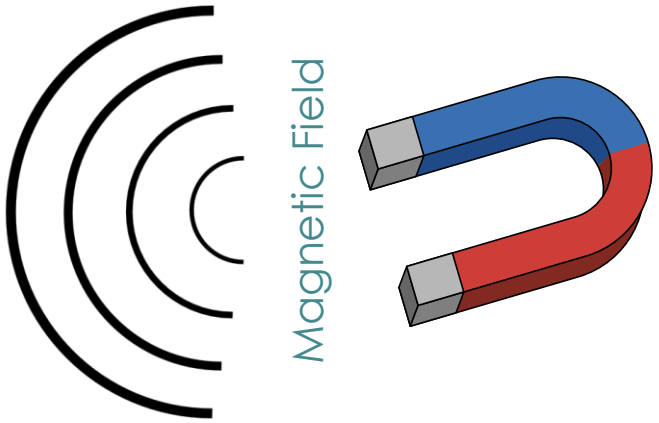
COCLEAR IMPLANT

PACEMAKER

GASTRIC STIMULATOR

INSULIN PUMP





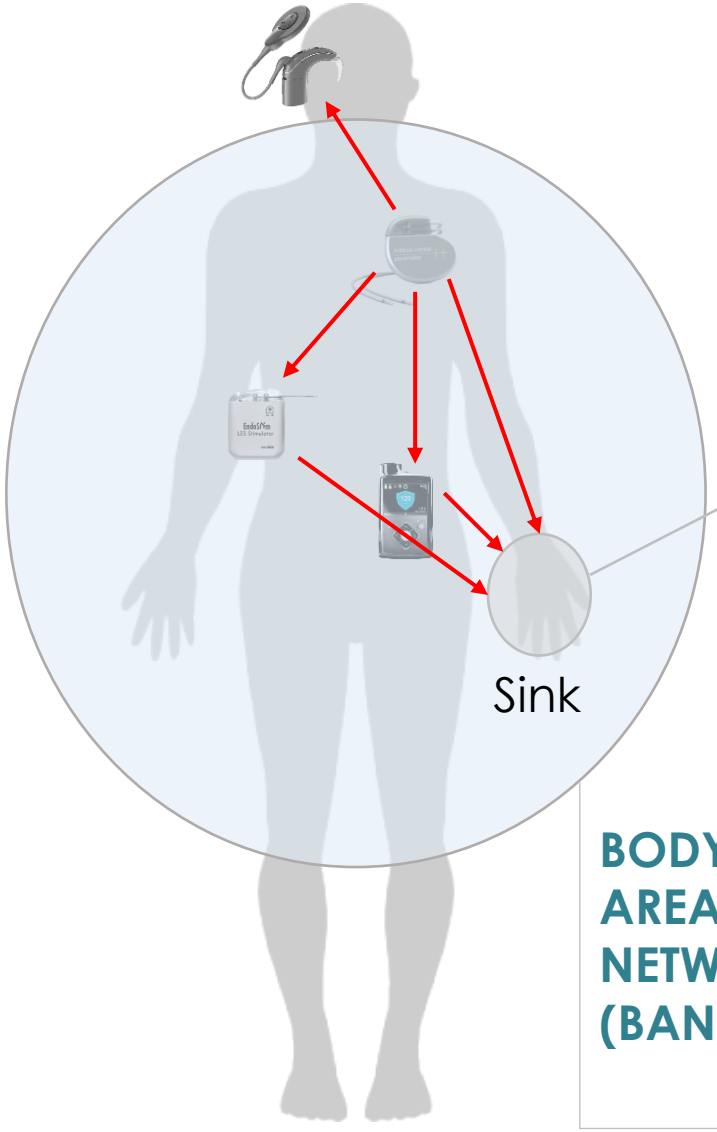
PROGRAMMER

Commands

External device with an interface for communicating wirelessly with an IMD and relaying data to a device used by clinicians or other health care providers

Interactions

GLOBAL



INTERNET

BODY AREA NETWORK (BAN)

Wireless network of heterogeneous computing devices that are wearable. This network enables continuous remote monitoring of patient physiological values in the medical setting.

Interactions

IDENTIFICATION

Authorized personnel must detect the presence of IMDs.

- Example- ICD* removal before heart surgery

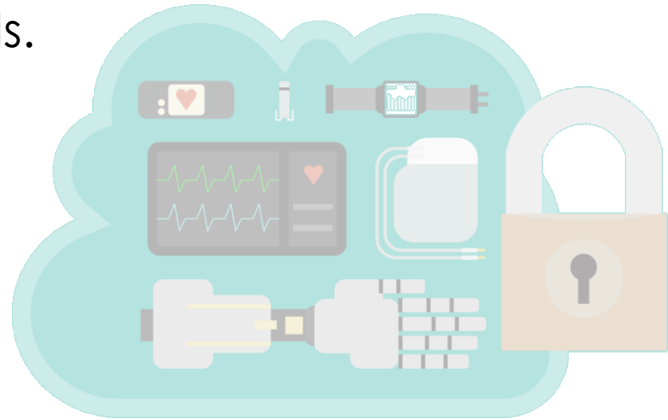
CONFIGURABILITY AND UPDATE

- Authorized personnel must be able to change IMD settings.
  - Appropriately engineered updates are necessary.
  - Updates need to come from authorized personnel.

AUDITABLE

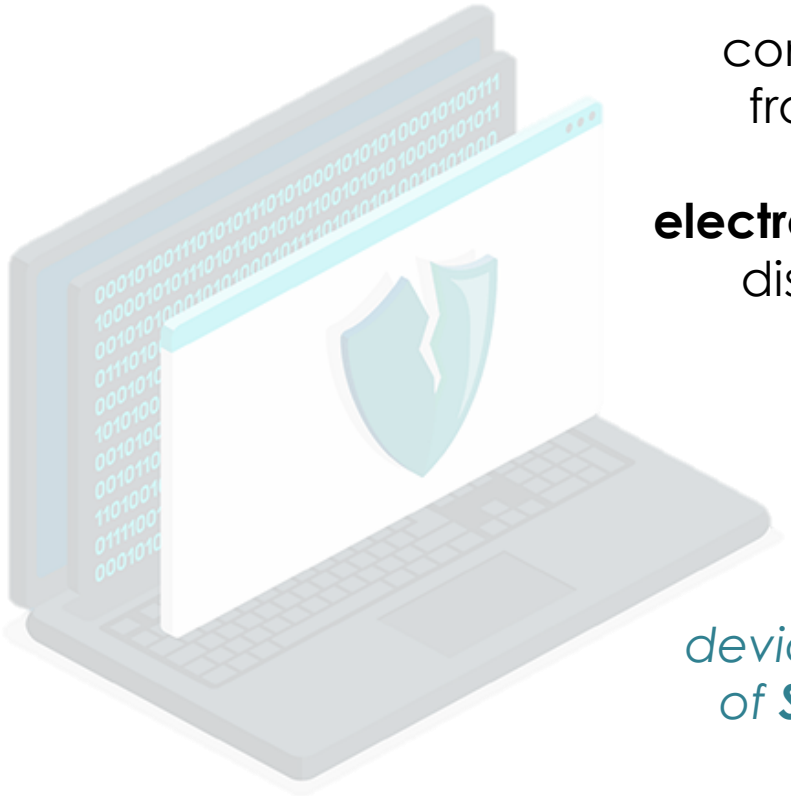
In case of failure:

- Device's operational history to manufacturers.
- Might differ from the data received by healthcare professionals.



SECURITY ISSUES

Cyber and Physical security



Cyber Security

Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems and networks from the theft of or damage to their hardware, **software, or electronic data**, as well as from the disruption or misdirection of the services they provide.

Physical Security

Physical security is the protection of personnel, hardware, software, networks and data **from physical actions** and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, theft, vandalism and terrorism.

(From Wikipedia)

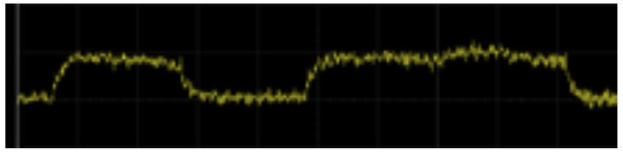
*Protection from attacks to devices/devices made by means of **Software Systems/procedures***

*Protection from attacks to devices made by means of **Hardware Systems/procedure***

Physical Attacks

SIDE CHANNEL ATTACKS

Any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself.



An attempt to decode RSA key bits using power analysis. The left peak represents the CPU power variations during the step of the algorithm without multiplication, the right (broader) peak – step with multiplication, allowing an attacker to read bits 0, 1.

An attacker will try to exploit weaknesses in the physical environment surrounding the system and extract sensitive information.

They are difficult to detect and prevent, as they do not rely on traditional software vulnerabilities or code weaknesses.

Physical Attacks

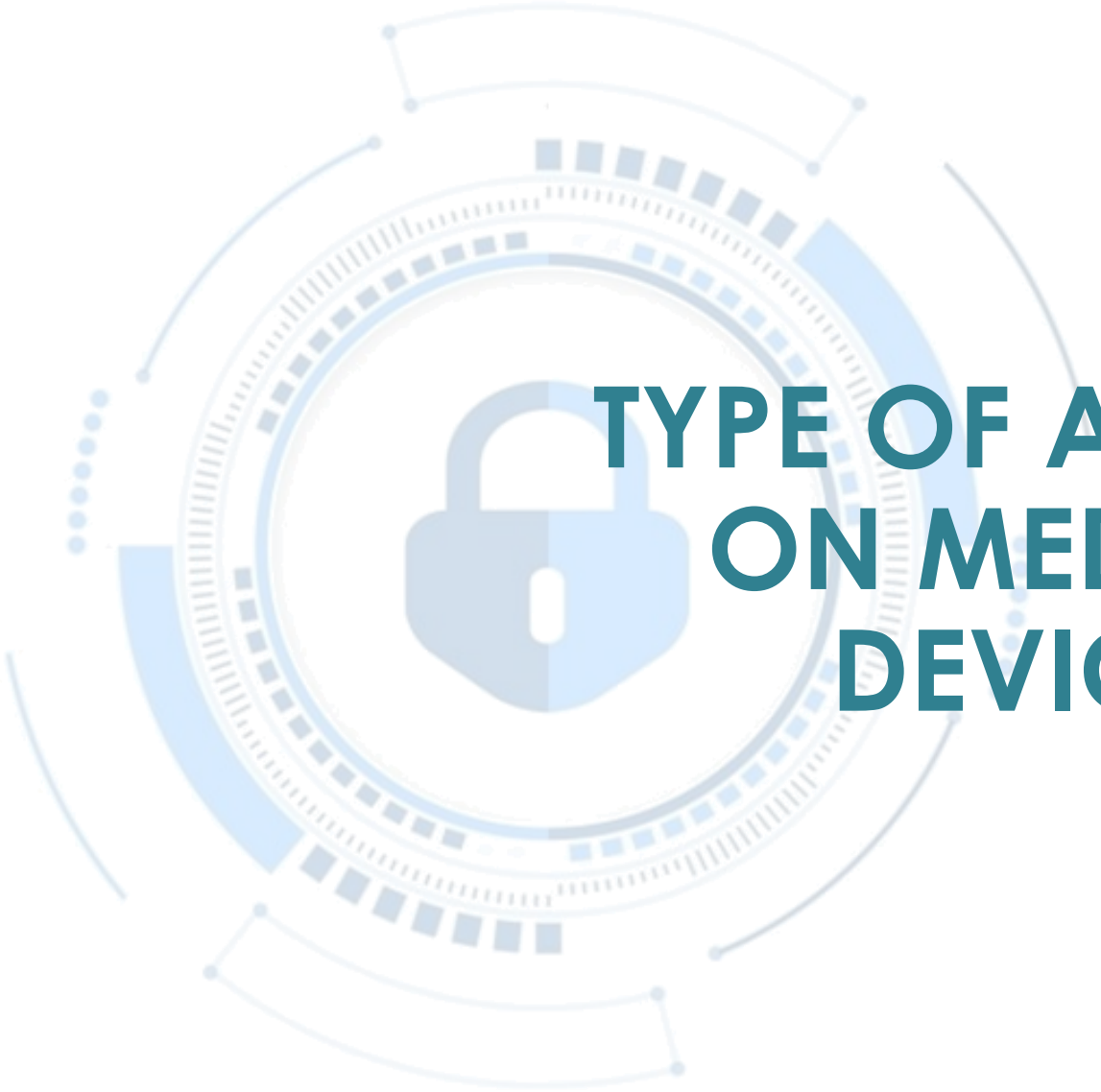
Non-invasive passive attacks **performed by measuring the electromagnetic radiation emitted from a device** and performing *signal analysis* on it.

ELECTROMAGNETIC ATTACKS

UNINTENTIONAL EMISSIONS

The fields emitted by devices can unintentionally reveal information about their operation **if not properly designed**.

Reveal encryption keys



TYPE OF ATTACKS ON MEDICAL DEVICES

Security attacks

Patient diagnosis,
vital signs

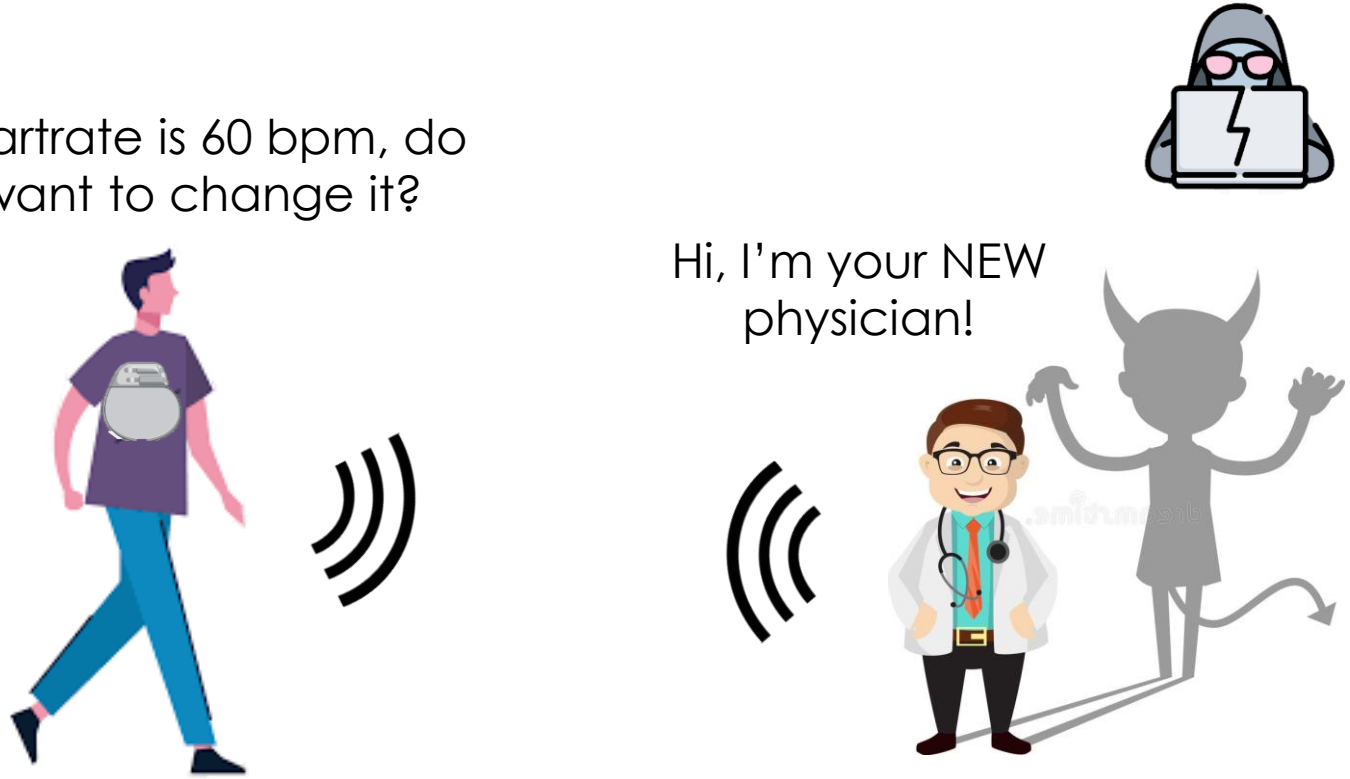
The attacker listens on the medium.
Whenever the implant transmits, the attacker snoops on these transmission to obtain the patient's private data.

Such a snooping is a significant **violation of the patient's privacy.**

PASSIVE ATTACK:
Eavesdropping on private data

Security attacks

IMPERSONIFICATION



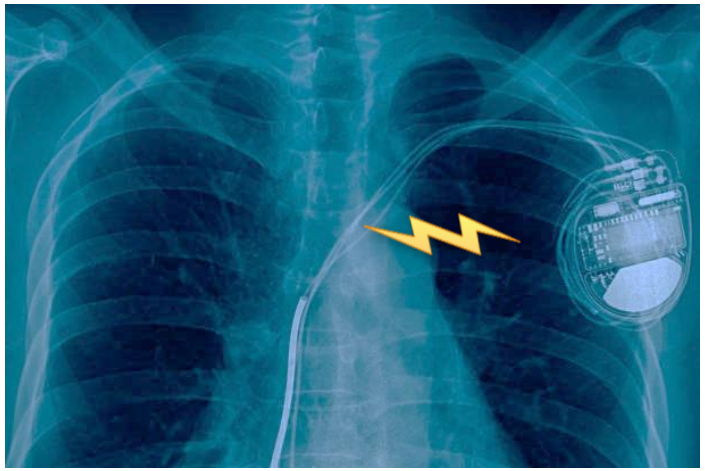
If the attacker somehow discovered the device's cryptographic key or its authentication protocol, he could take control of it and even change its settings or, in the worst case, disable it.

Security attacks

RESOURCE DEPLETION

An attacker initiates communication with the device, fail in the authentication process, and tries again.
During each authentication, the device consumes power, so it only needs to be repeated numerous times to drain it completely.

Security attacks



An-authorized command

Inoculation of digital virus

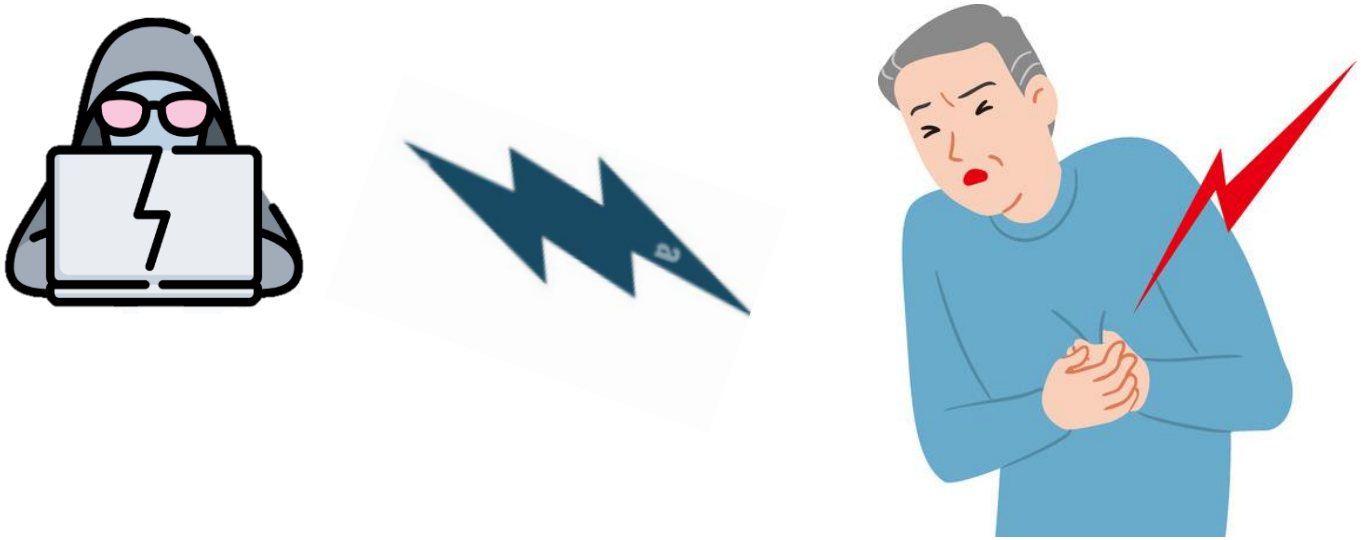
ACTIVE ATTACK:
Send unauthorized commands

The attacker sends unauthorized commands to the implant.
For example, the attacker can send wireless commands which turn off therapies on the implant.

Researchers have showed that an attacker can make a cardiac defibrillators **deliver an electric shock** to the patient's heart.

Security attacks

FAULT INDUCTION ATTACK



The most dangerous attack is the one in which you induce failures in the device. In this case, you do not even need to initiate communication, but you are going to damage the analogic components of it by illuminating it with a high-intensity electromagnetic field.

Targets

The patient

The adversary may wish to obtain private information concerning the patient (e.g., where-abouts, diagnosis, or blackmail-worthy material), or cause physical or psychological harm to the patient.

The device or system manufacturer

The adversary may wish to engage in corporate espionage or fraud.

System resources

The adversary may wish to utilize system resources and may be unaware of the type of device or network compromised. That is, the adversary does not knowingly target an IMD/BAN.

PRIVACY ISSUES

What about privacy?

PRIVACY

- **Define/enforce boundary & policy for personal data**
  - **Give patients the control over the collection and use of personal data**

Patients should know who owns and manipulates their health records, and IoT devices' locations, patients' identities, must stay hidden.

IMD-specific Privacy Levels

1 **Device-existence privacy**
Unauthorized entities should not be able to determine that a patient has an IMD/BAN.

2 **Device-type privacy**
Unauthorized entities should not be able to determine what type of IMD/BAN is in use.

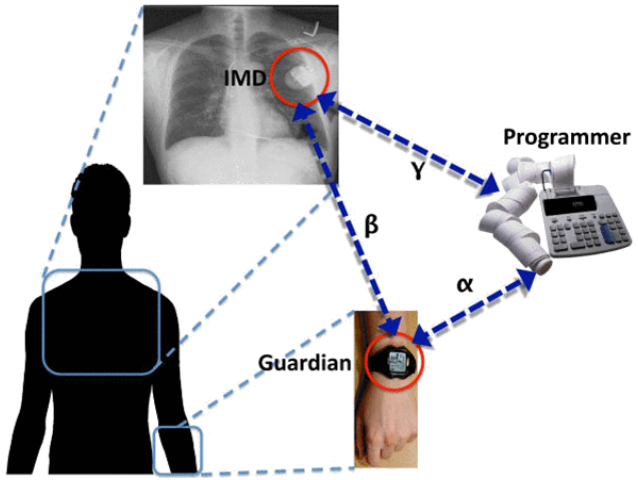
3 **Specific-device ID privacy**
Unauthorized entities should not be able to determine the unique ID of an IMD/BAN sensor.

4 **Measurement and log privacy**
Unauthorized entities should not be able to determine private telemetry or access stored data.

5 **Bearer privacy**
Unauthorized entities should not be able to exploit IMD/BAN properties to identify the patient.

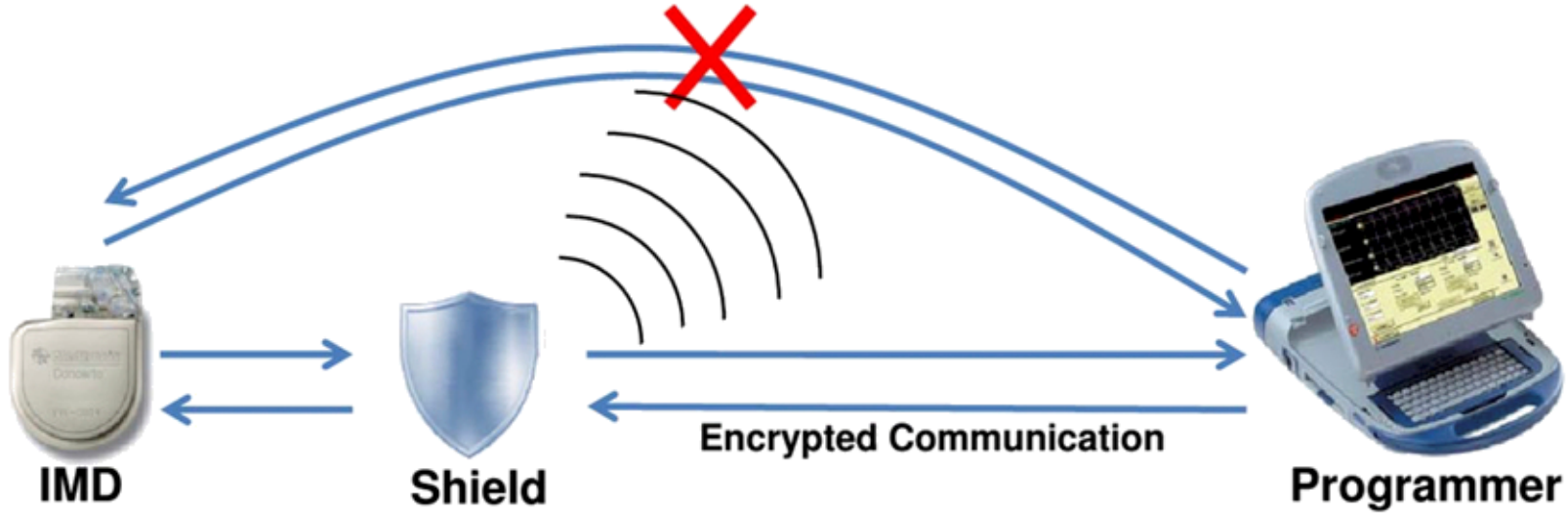
6 **Tracking**
Unauthorized entities should not be able to leverage the physical layer (e.g., by monitoring analog sensors or matching a radio fingerprint to track or locate a patient).

Countermeasures



EXTERNAL WEARABLE DEVICE

An external device **mediates communication with the IMD**, thereby providing both confidentiality for transmitted data and protection against unauthenticated communication.



Security & Privacy by design

Balancing **security, privacy, safety, and utility** is a necessity in the health care domain.

SECURITY BY DESIGN

Thanks for the attention!

Francesca Maria Chiara Nanni

Contacts:
Pervasive Electromagnetic Lab,
Roma, Via del Politecnico 1

frmach97@gmail.com
francesca.nanni@alumni.uniroma2.eu

Pervasive Electromagnetics Lab

Your opinion matters!