

# 29- Usable Privacy and Security for Safety-Critical Devices

Lujo Bauer, Nicolas Christin,  
and Abby Marsh

April 27, 2016

05-436 / 05-836 / 08-534 / 08-734

*Usable Privacy and Security*

Carnegie  
Mellon  
University

CyLab



Engineering &  
Public Policy



# Today!

- Clarify expectations for project report and presentation
- UPS for cars
- UPS for medical devices
- UPS for medical records

# Project

# Cars

<https://www.youtube.com/watch?v=oqe6S6m73Zw>

# Meta-issues with car privacy/security

- Why are our cars run by computers?
- Why are we connecting our cars to the Internet?

# Meta-issues with car privacy/security

- Why are our cars run by computers?
- Why are we connecting our cars to the Internet?
  - Rich media content
  - Real-time traffic and safety info
  - OTA updates
  - Self-driving cars
  - (Surveillance)

# Meta-issues with car privacy/security

- Why are our cars run by computers?
- Why are we connecting our cars to the Internet?
  - Rich media content
  - Real-time traffic and safety info
  - OTA updates
  - Self-driving cars
  - (Surveillance)
- Are privacy/security issues the same?

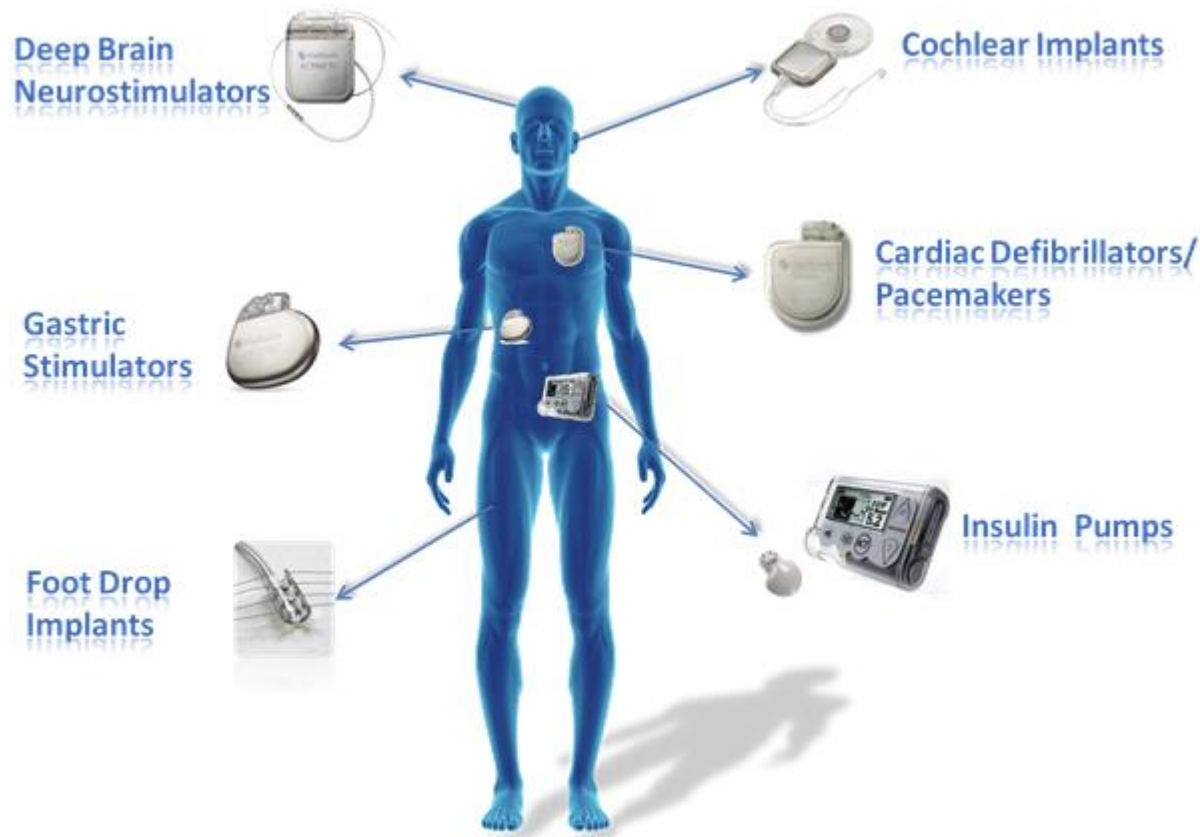
# Meta-issues with privacy/security

- Let's answer the same questions for medical devices



# Implantable Medical Devices (IMD)

- Embedded computers
- 6M Pacemakers & 173K Cardiac Defibrillators in 2006



# Operational Requirements/Goals

# Operational Requirements

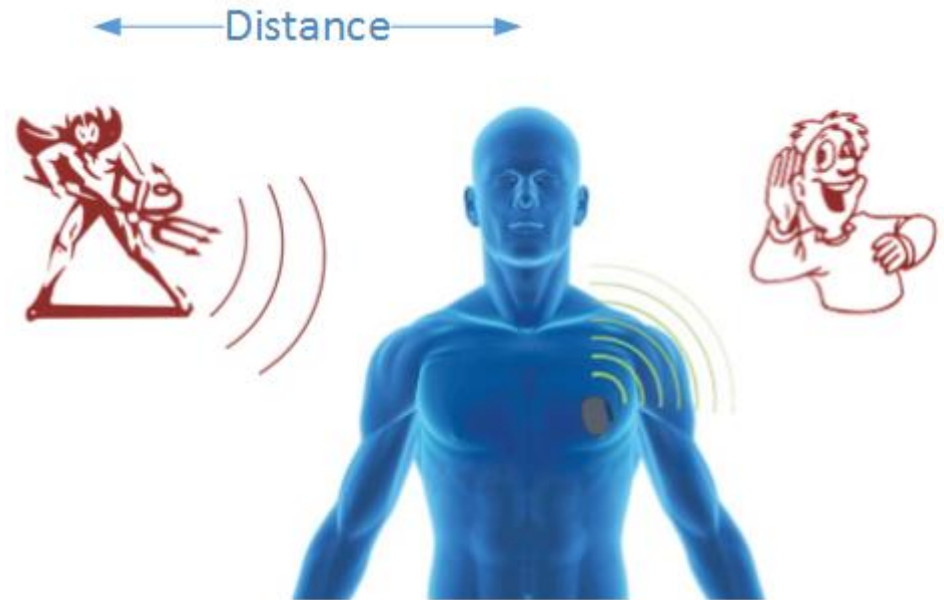
- Possible goals
  - Collect information (diagnostics)
  - Provide information (medical history)
  - Perform medical function
- Disable IMD before conducting surgeries
- Access in emergency situations

# Operational Requirements

- Possible goals
  - Collect information (diagnostics)
  - Provide information (medical history)
  - Perform medical function
- Disable IMD before conducting surgeries
- Access in emergency situations
- Constraints
  - Limited capacity of battery (replacement = surgery)

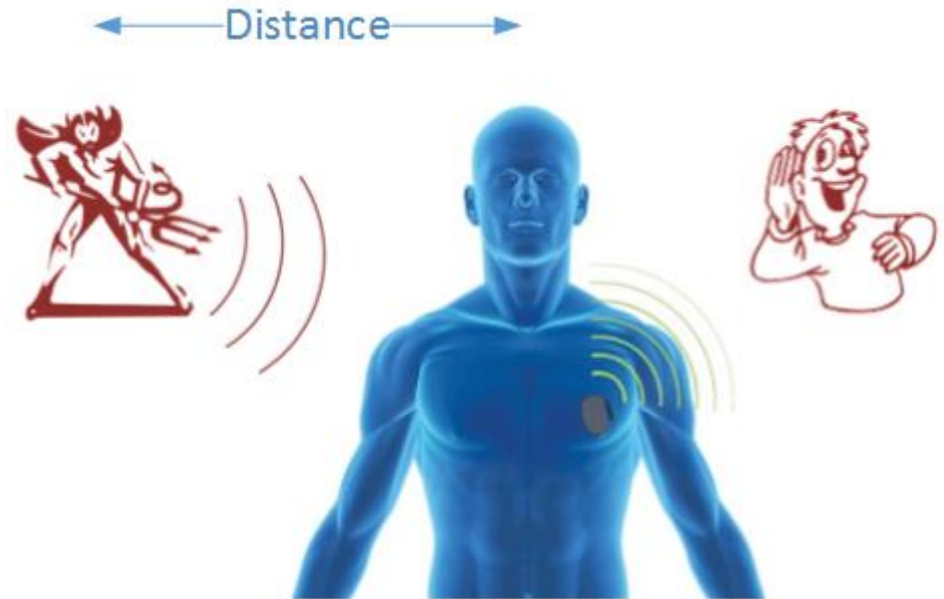
# Risks in Medical Devices

- Vulnerabilities
  - Authentication
- Attack Vectors
  - Passive
  - Active
- Risks / threats

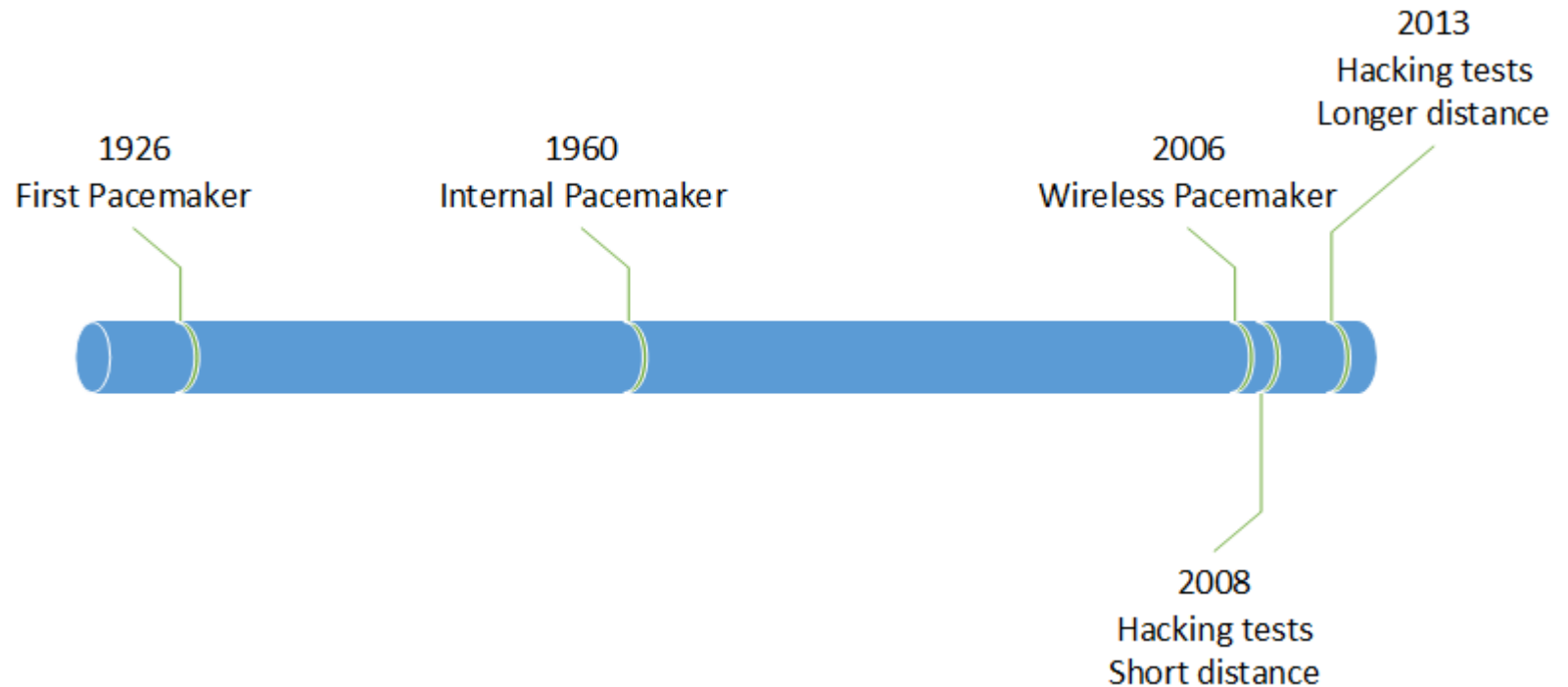


# Risks in Medical Devices

- Vulnerabilities
  - Authentication
- Attack Vectors
  - Passive
  - Active
- Risks / threats
  - DoS
  - Changes in configuration
  - Replace medical records -- someone having a different operation
  - Injuries, death



# Pacemakers



Networking changes the treat model

# Hacking Tests (1)

- **2008:** wireless access to a combination heart defibrillator and pacemaker (within two inches of the test gear)
- Disclose personal patient data
- Reprogram IMD to shut down and to deliver jolts of electricity that would potentially be fatal



# Hacking Tests (2)

2011-2012-2013

- **Hacking Insulin Pumps**



-- insulinpump.com

2013 -- Black Hat /Defcon:

- **“Implantable medical devices: hacking humans”**
  - At 30 feet by compromising their pacemaker
  - Transmitter to scan for and interrogate individual medical implants
  - Security techniques for manufacturers

-- ioactive.com

# Defense Approaches

- How do we achieve resistance to attacks?
  - What are the classes of attacks?
- What can go wrong?
- How do we balance utility and security/privacy?

# Authentication Methods

- Passwords: how to make them available?

# Authentication Methods

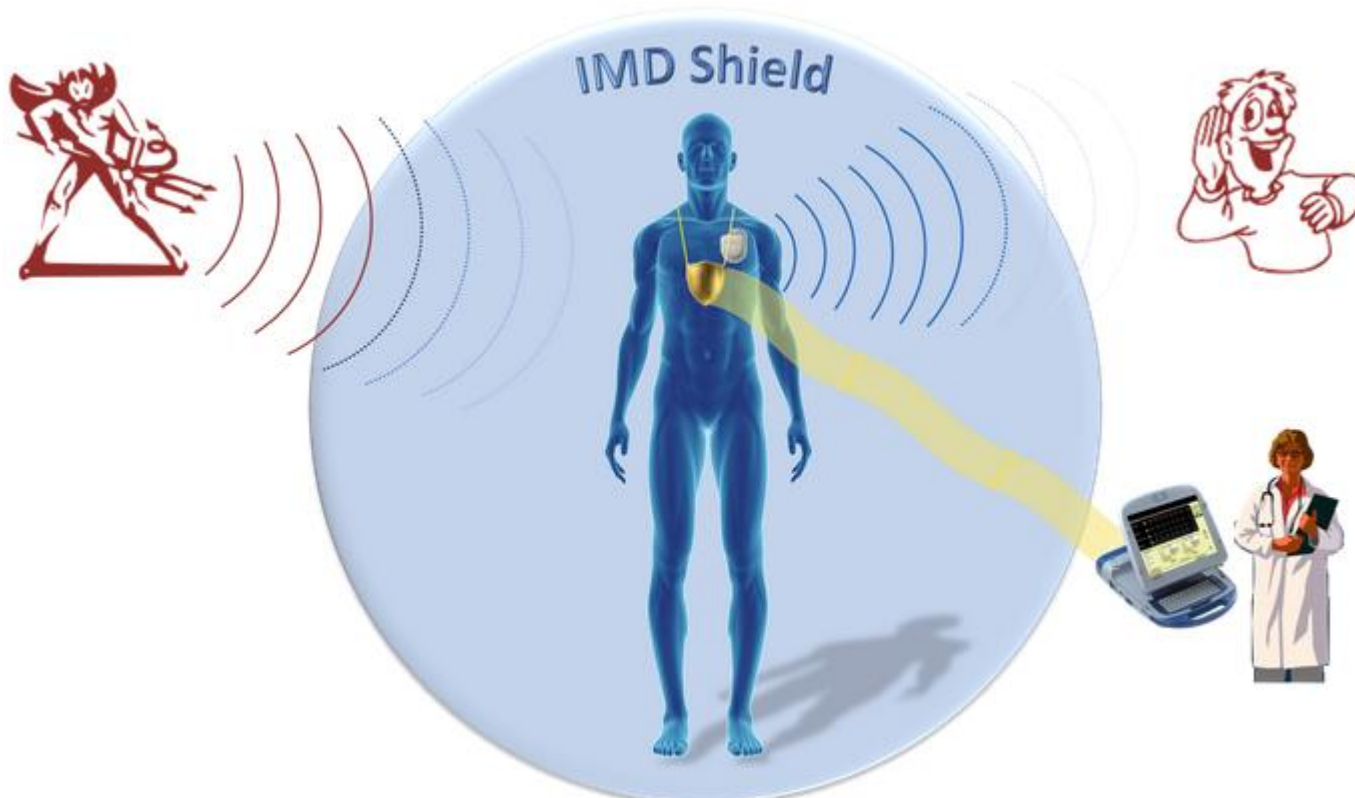
- Passwords: how to make them available?
  - Tattooed passwords (visible, UV visible)
  - Bracelet
- Biometrics (face recognition)
- Smart Cards
- Touch-to-access policy
- Key-based systems
- Shields
  - Necklace
  - Computational wristband



-- Figures from Denning et al.

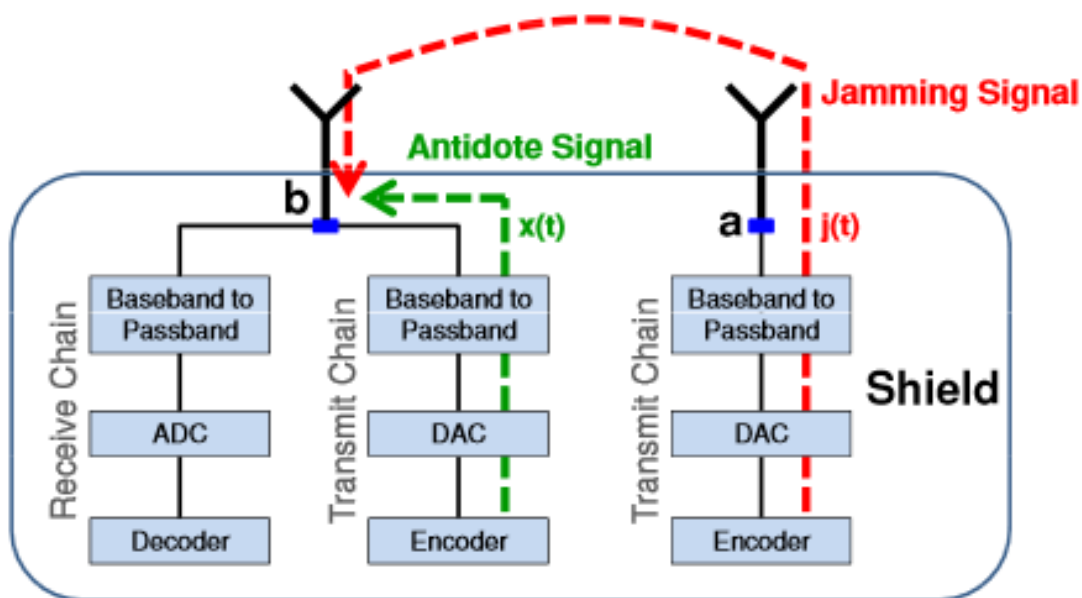
# IMD Shield

- Proxy (messages exchanges)
- Authentication + encryption (channel)



# IMD Shield - Implementation

- Jammer design (full duplex radio)



- S. Gollakota et al. MIT

# Wristbands / Alert Bracelets

- Safety in emergencies
- Security & Privacy under adversarial conditions
- Battery life

# Wristbands / Alert Bracelets

- Protection is granted while wearing the bracelet
- Remove to gain access to the IMD
- Inform patients about malicious actions – But not preventive
- Authentication + symmetric encryption
- Disadvantages



--Denning et al.



# Wristbands / Alert Bracelets

- Protection is granted while wearing the bracelet
- Remove to gain access to the IMD
- Inform patients about malicious actions – But not preventive
- Authentication + symmetric encryption
- Disadvantages
  - Relies on the patient wearing the bracelet
  - Reactive
  - Cognitive effects on patients



--Denning et al.

# Usability Considerations

# Usability Considerations

- Hospitals not having correct equipment
- Visual indicator of patients condition (something is wrong). Personal dignity.
- Carrying one more device
- Aesthetics
  - Wristbands (especially). “Mockups are unaesthetic”
  - Tattoos
- Mental and physical inconvenience
- Cultural and historical associations

# Electronic Medical Records

- Why do we want *electronic* medical records?
- What are privacy/security concerns about electronic medical records?
- How do we mitigate those concerns?

# Questions?