SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks

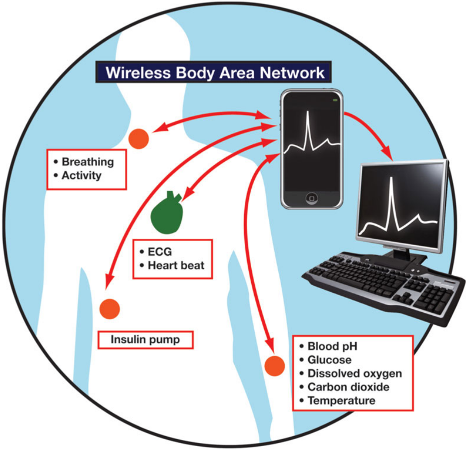
Michael Rushan[JHU], Aviel Rubin[JHU], Denis Foo Kune[Michigan] and Colleen Swanson[Michigan]

Presented by: Matthew S. Bauer

September 20, 2016

Implantable medical devices (IMDs)

Body area networks



Wireless network of heterogeneous devices that are wearable/implantable

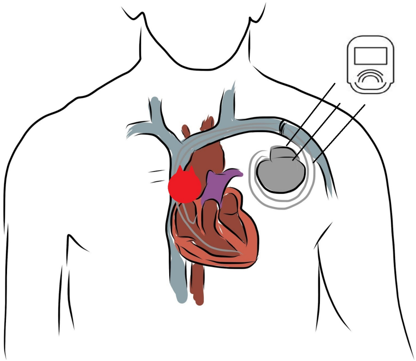
- comprised of sensors, actuators and a sync
- low power/size nodes
- transmission limitations
- stricter reliability requirements

Security and privacy design objectives

Privacy goals:

- Device existence privacy (Device type privacy)
- Device ID privacy
- Measurement and log privacy
- Bearer privacy
- No tracking

Threats - Sensors



Signal interference

- intentional/accidental
- signal injection
- could alter therapy

Signal containment

- physiological signals may not stay within body
- private data leakage

Cardiac Implantable Electrical Devices - Signal Injection[1]

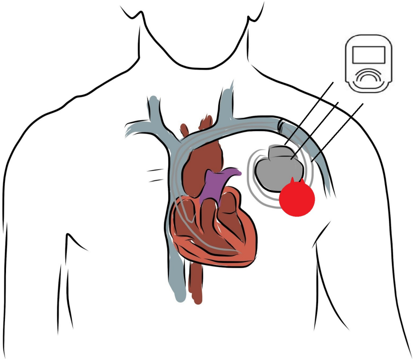
By adding intentional interference to a CIED to mimic particular cardiac waveforms, it was shown that is it possible to alter the therapy delivered by the device (causing pacing inhibitions and defibrillation).

Device	Open air	Open air (defibrillation)	Saline bath	Saline (lead tips only)	SynDaver
Medtronic Adapta	1.40 m	*Not applicable*	*No inhibition*	0.03 m	*Untested*
Medtronic InSync Sentry	1.57 m	1.67 m	*No inhibition*	0.05 m	0.08 m
Boston Scientific Cognis 100-D	1.34 m	*No defibrillation*	*No inhibition*	*Untested*	*Untested*
St. Jude Promote	0.68 m	*No defibrillation*	*No inhibition*	*Untested*	*Untested*

Figure: The median maximum distance at which a pacing inhibition or defibrillation was observed for 4 studied devices in various mediums.

[1]Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors

Threats - Software



Software bugs have resulted in over 500 FDA recalls between 2009 and 2011

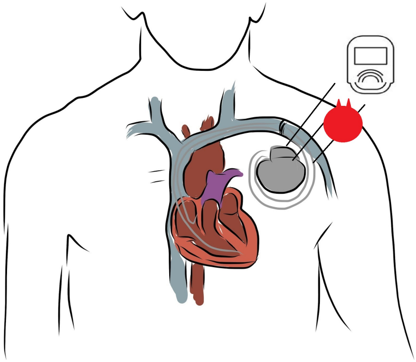
2006-2011 software recalls by severity:

- 33% of class I (chance of harm)
- 66% of class II (temporary effects)
- 77% of class II (non-complaint)

Challenges in software testing

- Failure to apply known engineering techniques / closed design
- Difficulty in modeling human body
  - Recent efforts in building models of human hearts
  - Databases of cardiac data (e.g. MIT PhysioNet portal)
  - Where should data be obtained from?
  - How much data is enough for testing?

Threats - Telemetry



Some existing devices lack authentication

- replay
- eavesdropping
- injection
- DOS

Traditional crytpo often not applicable

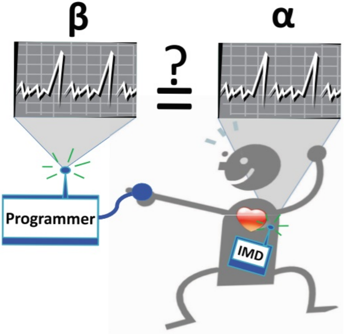
- limited power/processing
- emergency access
- device identification

Securing device telemetry: biometric authentication

Key idea: Use physiological values as a source of randomness for key establishment protocols

Physiological values

- Electrocardiograms
- heart rate
- blood glucose
- blood pressure



Heart-to-Heart protocol

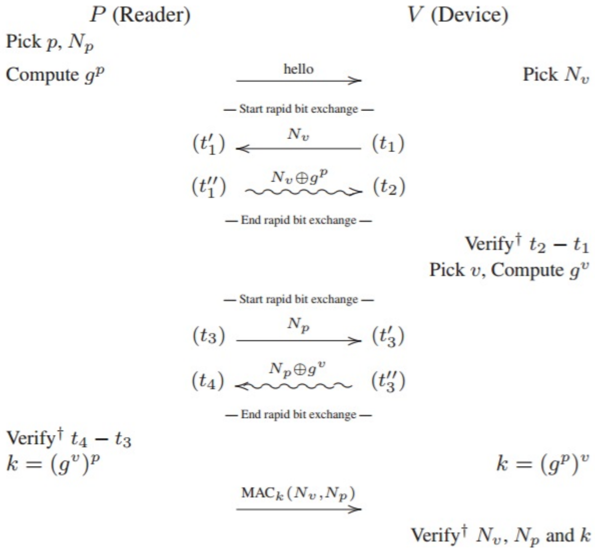
Challenges in biometric authentication

- Need more rigorous analysis of entropy sources and protocols
  - Flaws found in biometric protocols (OPFKA, IMDGuard) allow key space reduction attacks
- Do these protocols handle real world noise?
- Is the randomness property extracted from physiological entropy sources?

Securing device telemetry: distance-bounding protocols

Key idea: measure delays between transmissions between devices to establish proximity. Distance bounds can be computed over various signals such as RF or ultrasonic sound (> 20 kHz)

Distance-bounding protocol[2]



[2]Proximity-based Access Control for Implantable Medical Devices

Securing device telemetry: out of band authentication

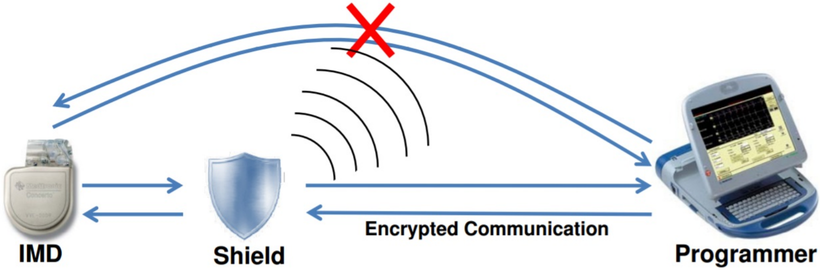
Key idea: use audio and visual channels to exchange authentication (key information)

Examples:

- low frequency audio channel to transmit a random key
- ultra-violet or visible tattoos to record permanent key information

Securing device telemetry: external wearable devices

Key idea: IMD to programmer communicated is mediated through a wearable device.



Challenges in designing external wearable devices

- Need to fail open.
- What communication protocols between IMD and the mediator should be used?
- Can jamming or the proxy be circumvented?

Securing device telemetry: anomaly detection

Key idea: Observe and characterize patterns in device communications to detect unwanted behavior.

Use cases:

- Preventing denial of service attacks
- Identify abnormal IMD communication by signal characteristics (strength, time, angle, etc..)

Challenges in anomaly detection

- Emergency scenarios
- Where is all of the computational overhead of anomaly detecting going to be offloaded to?
- What to do in the case of an anomaly?
  - Alerting the patient
  - Blocking transmissions to the IMD

Discussion

- What is the likelihood of targeted attacks on IMD's? How does this affect security design decisions?
- What do you think is the best approach to securing the telemetry interface?
- What are the right assumptions about attacker capabilities in the various contexts we have discussed? Do we need more data to answer this question?