SoK: Security and Privacy in Implantable Medical Devices

Michael Rushanan[1], Denis Foo Kune[2],
Colleen M. Swanson[2], Aviel D. Rubin[1]

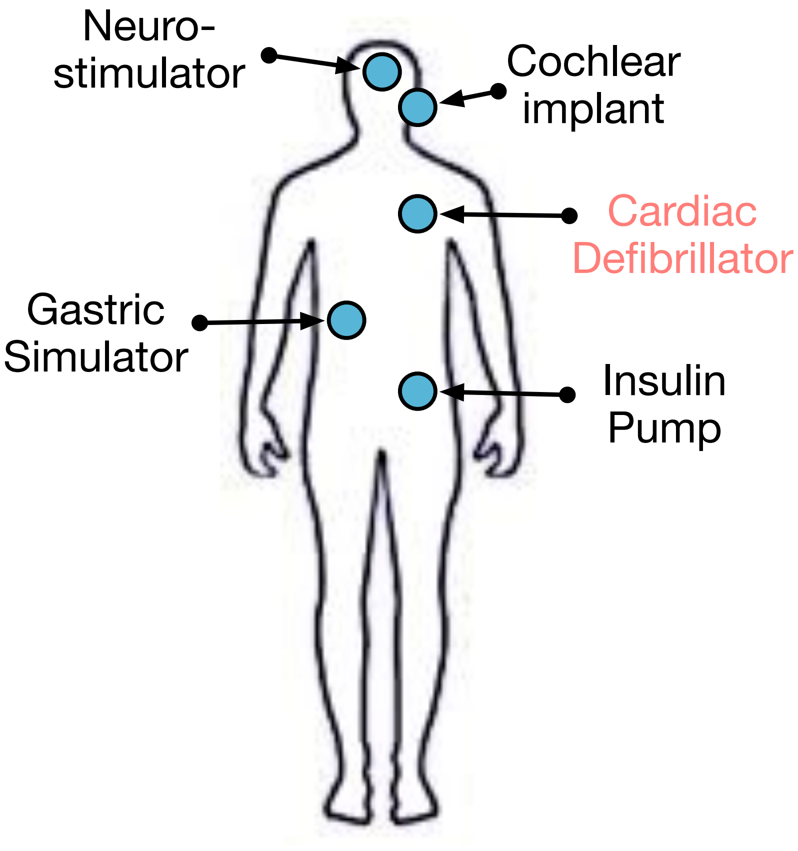
1. Johns Hopkins University

2. University of Michigan

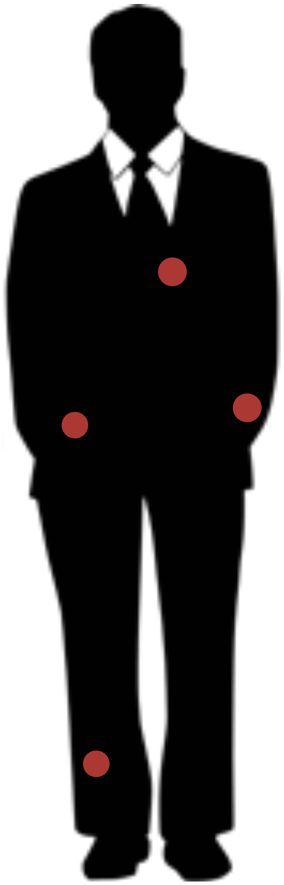
This work was supported by STARnet, the Dept. of HHS under award number 90TR0003-01, and the NSF under award number CNS1329737, 1330142.

What is an Implantable Medical Device?

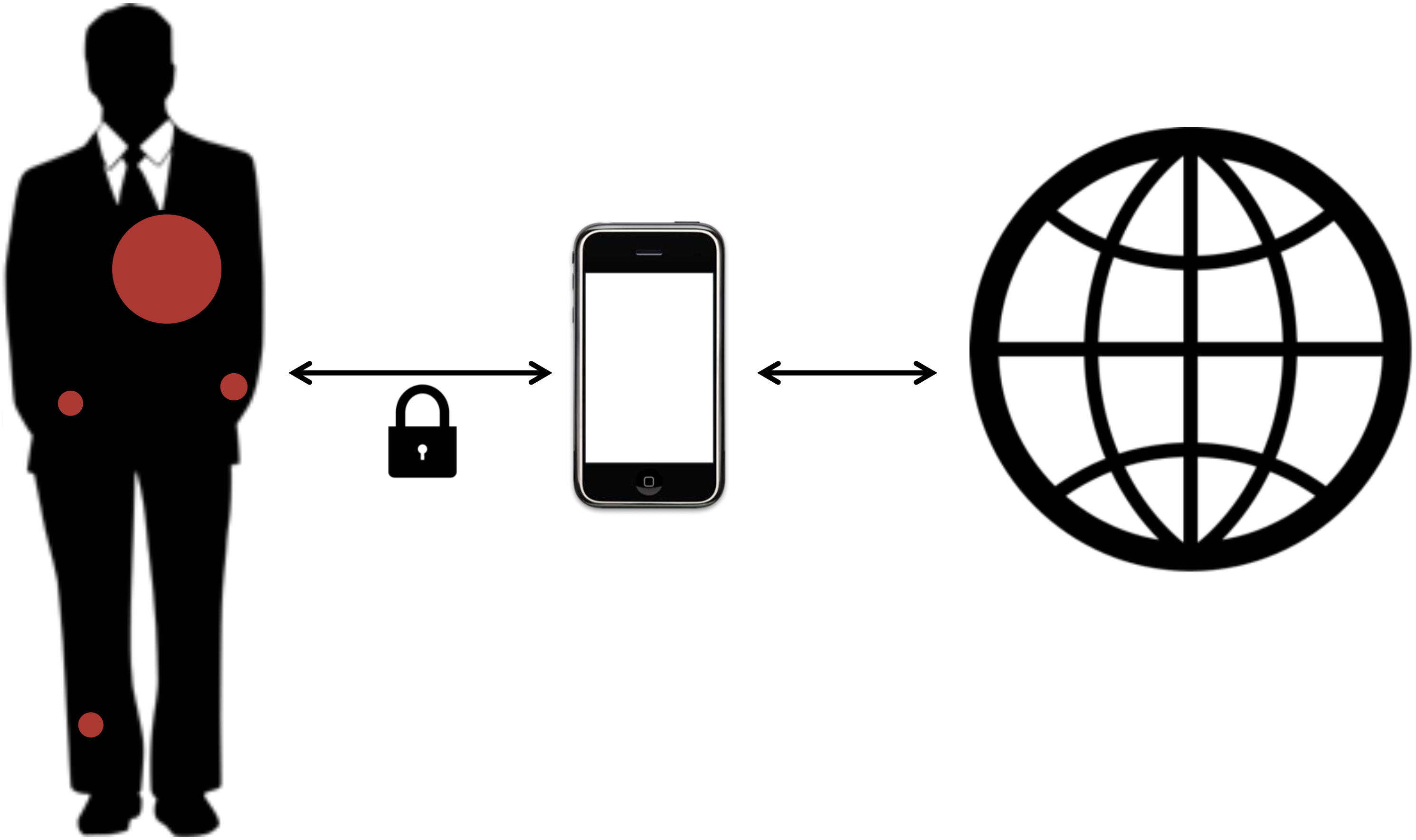
- The FDA strictly defines a medical device
- Device
  - Embedded system that can sense and actuate
- Implantable
  - Surgically placed inside of a patient's body
- Medical
  - Provides diagnosis and therapy for numerous health conditions



Implantable Medical Devices are not your typical PCs



Implantable Medical Devices are not your typical PCs



Implantable Medical Devices are not your typical PCs

- There exists *resource limitations*
  - The battery limits computation and is not rechargeable
- There are *safety and utility* concerns
  - The IMD must be *beneficial* to the patient and *elevate* patient safety above all else
  - Security and privacy mechanisms must not *adversely* affect the patient or therapy
- Lack of security mechanisms may have *severe* consequences
- IMD's provide *safety-critical* operation
  - Must fail-open in the context of an emergency

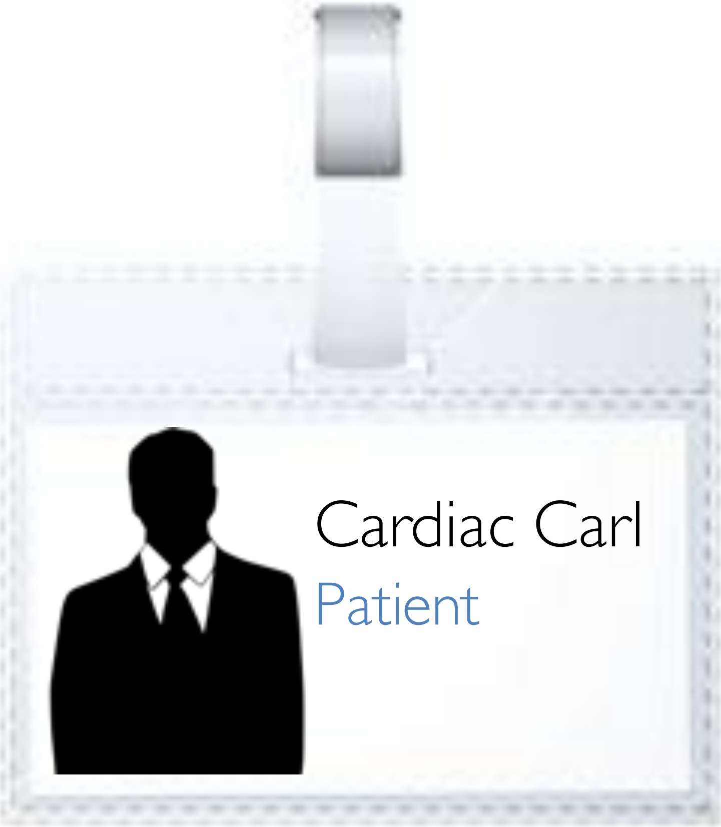
Research Questions

- How do we provide security and privacy mechanisms that adequately consider safety and utility?
- When do we use traditional security and privacy mechanisms or invent new protocols?
- How do we formally evaluate security and privacy mechanisms?
- Novel attack surfaces

A Healthcare Story

Alice

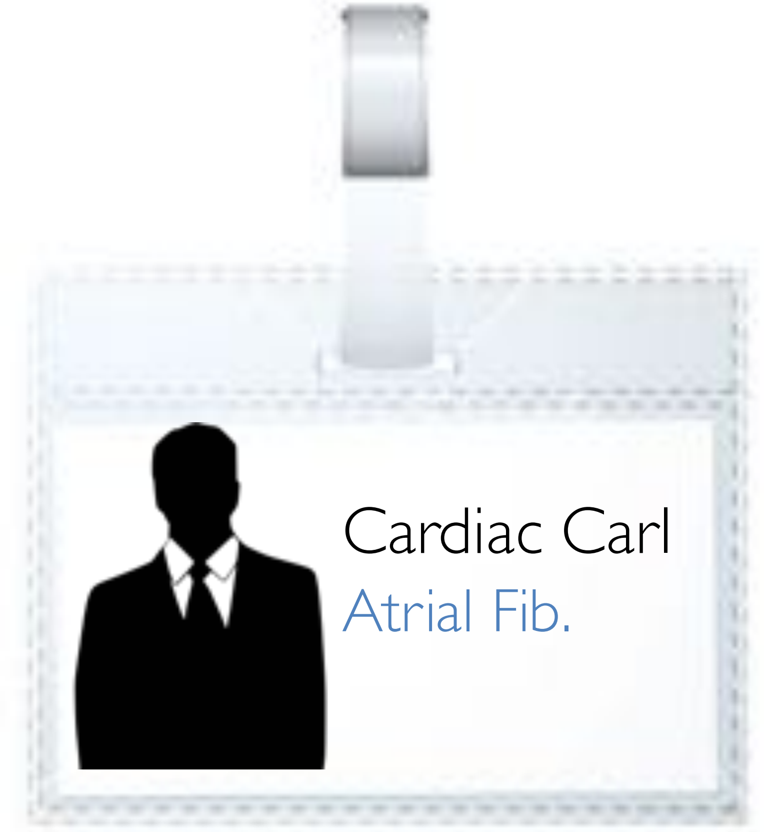
Nurse



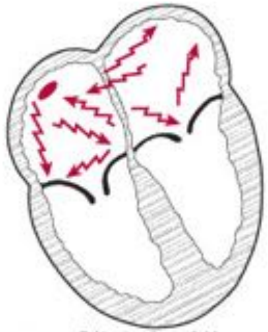
Cardiac Carl

Patient

Cardiac Carl’s Condition



- Atrial Fibrillation

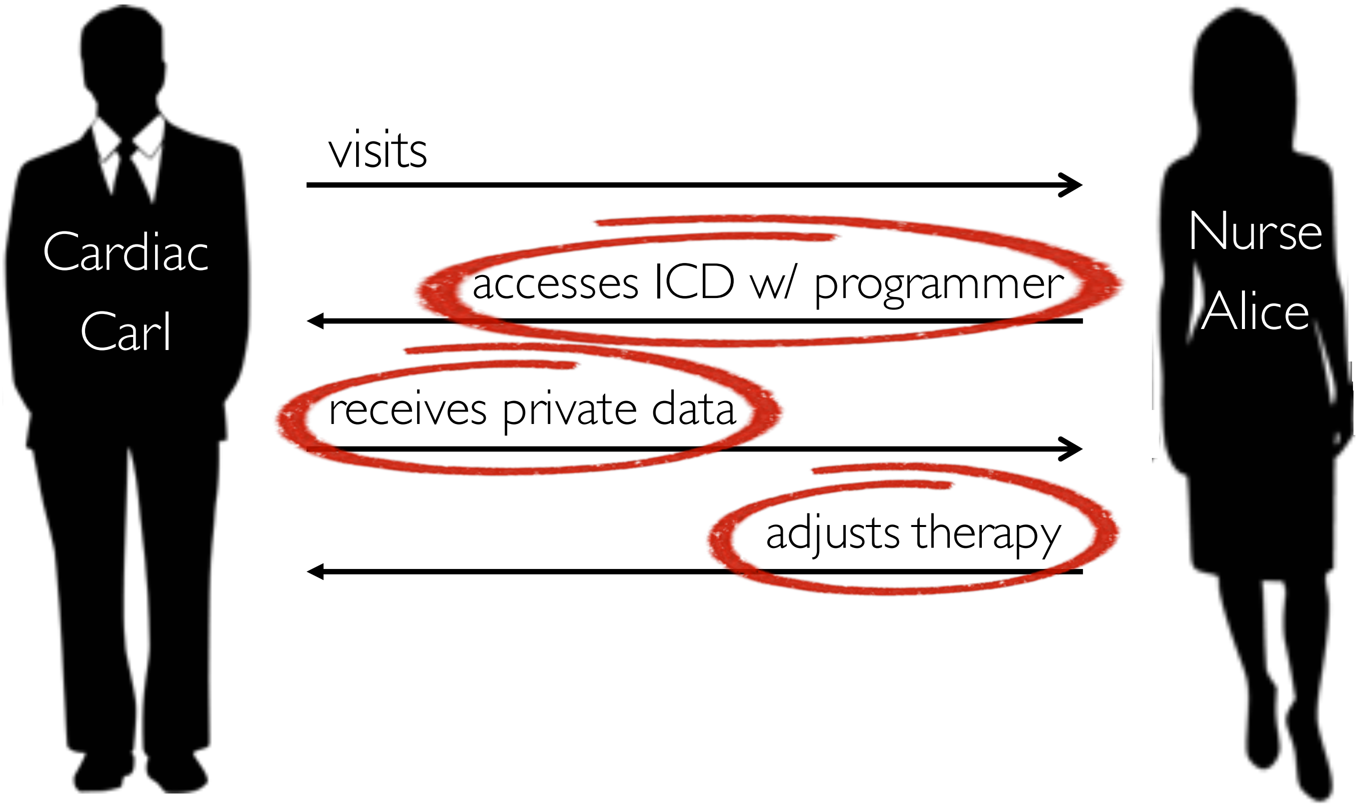


© Harriet Greenfield

- Implantable Cardioverter Defibrillator
- His ICD is safety-critical

Alice and Carl's Relationship

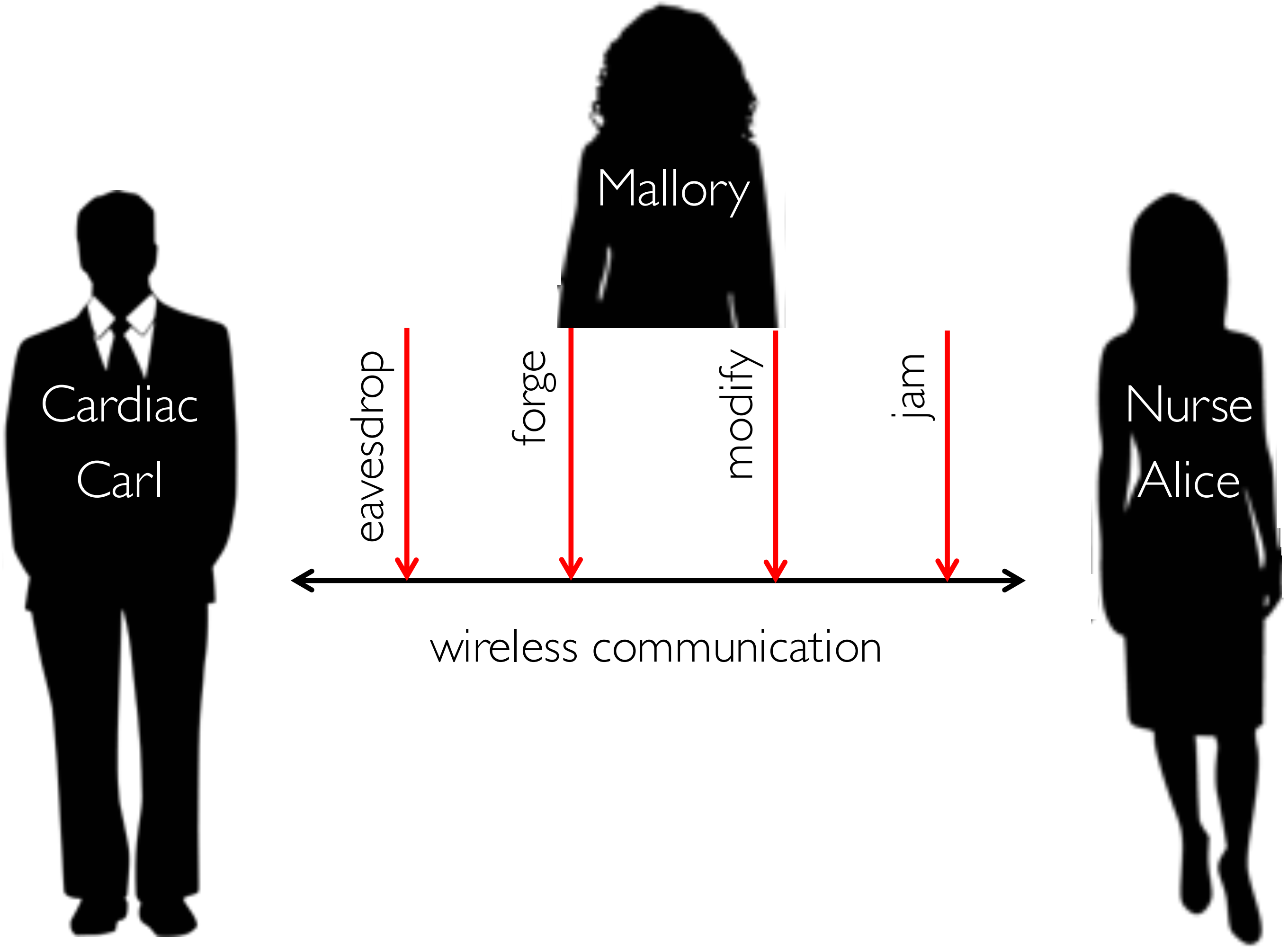
Where are the *security and privacy mechanisms*?



Alice and Carl’s Relationship

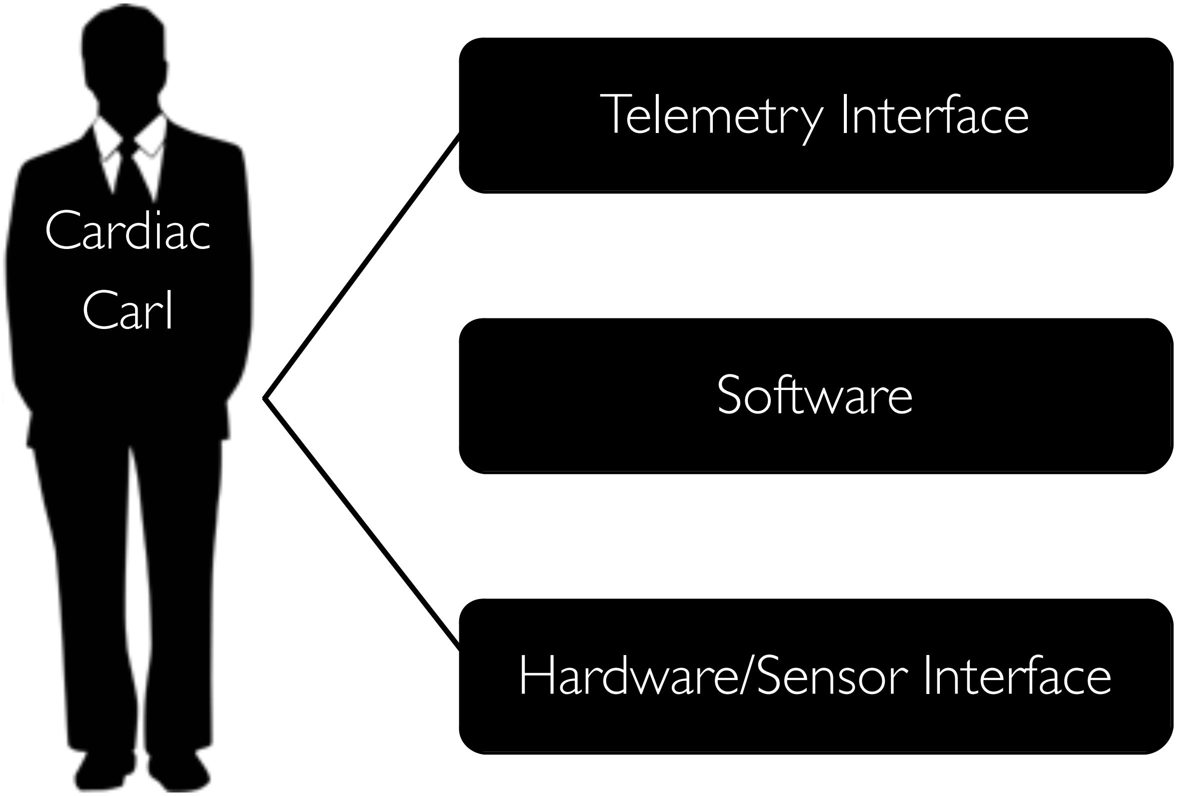
Carl
Mallory
Hacker Elite
Alice

~~Alice~~ Mallory and Carl's Relationship



[Halperin, S&P, 08], [Li, HealthCom, 11]

Attack Surfaces



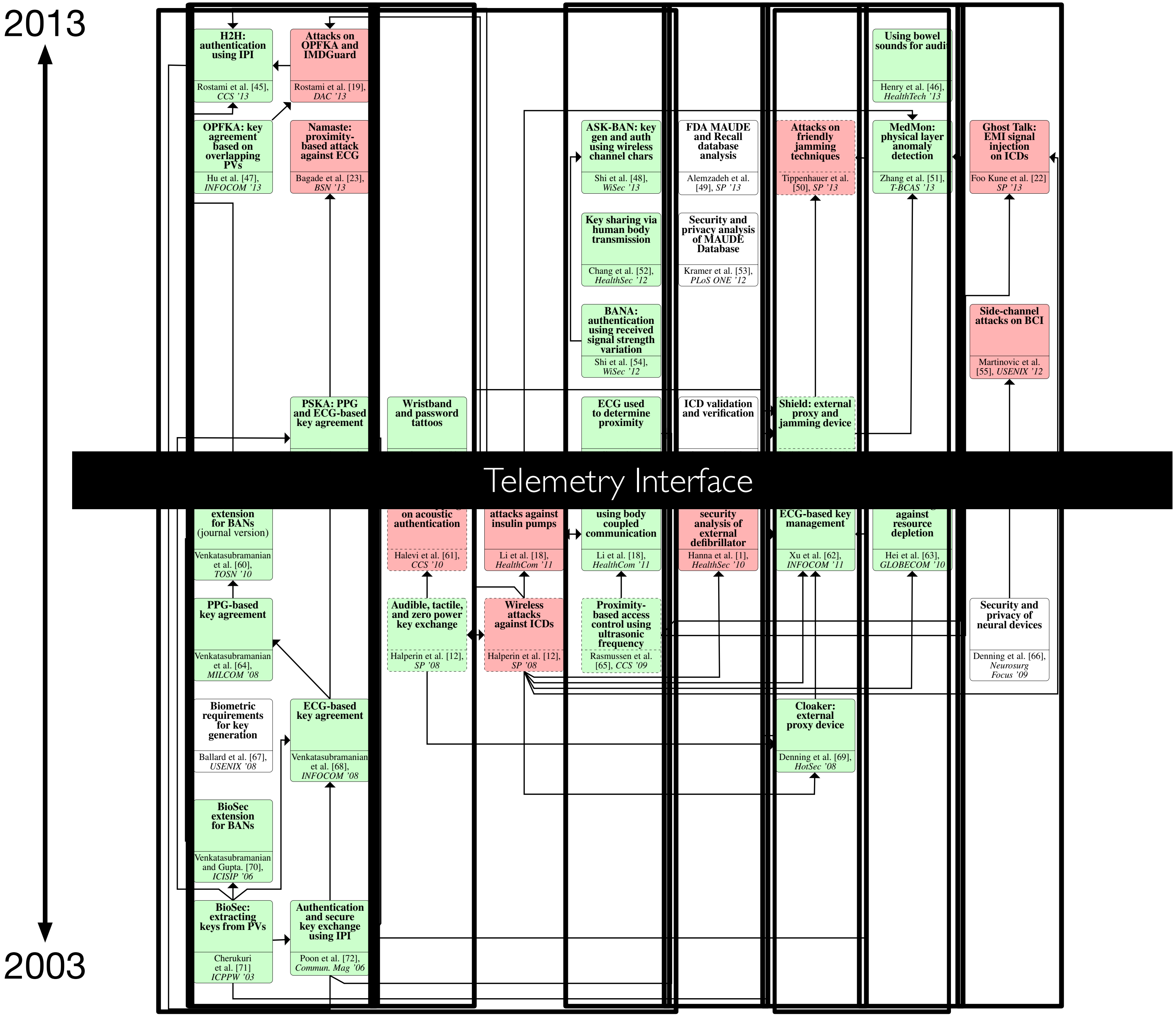
Security and Privacy Mechanisms

- Security and Privacy mechanisms exist in standards
  - Medical Implant Communication Services
  - Wireless Medical Telemetry Service

- These mechanisms are optional

- Interoperability *might* take priority of security

[Foo Kune, MedCOMM, 12]



Telemetry Interface

2013

2003

H2H: authentication using IPI
Rostami et al. [45], *CCS '13*

Attacks on OPFKA and IMDGuard
Rostami et al. [19], *DAC '13*

Using bowel sounds for audit
Henry et al. [46], *HealthTech '13*

OPFKA: key agreement based on overlapping PVs
Hu et al. [47], *INFOCOM '13*

Namaste: proximity-based attack against ECG
Bagade et al. [23], *BSN '13*

ASK-BAN: key gen and auth using wireless channel chars
Shi et al. [48], *WiSec '13*

FDA MAUDE and Recall database analysis
Alemzadeh et al. [49], *SP '13*

Attacks on friendly jamming techniques
Tippenhauer et al. [50], *SP '13*

MedMon: physical layer anomaly detection
Zhang et al. [51], *T-BCAS '13*

Ghost Talk: EMI signal injection on ICDs
Foo Kune et al. [22] *SP '13*

Key sharing via human body transmission
Chang et al. [52], *HealthSec '12*

Security and privacy analysis of MAUDE Database
Kramer et al. [53], *PLoS ONE '12*

BANA: authentication using received signal strength variation
Shi et al. [54], *WiSec '12*

Side-channel attacks on BCI
Martinovic et al. [55], *USENIX '12*

PSKA: PPG and ECG-based key agreement

Wristband and password tattoos

ECG used to determine proximity

ICD validation and verification

Shield: external proxy and jamming device

extension for BANs (journal version)
Venkatasubramanian et al. [60], *TOSN '10*

on acoustic authentication
Halevi et al. [61], *CCS '10*

attacks against insulin pumps
Li et al. [18], *HealthCom '11*

using body coupled communication
Li et al. [18], *HealthCom '11*

security analysis of external defibrillator
Hanna et al. [1], *HealthSec '10*

ECG-based key management
Xu et al. [62], *INFOCOM '11*

against resource depletion
Hei et al. [63], *GLOBECOM '10*

PPG-based key agreement
Venkatasubramanian et al. [64], *MILCOM '08*

Audible, tactile, and zero power key exchange
Halperin et al. [12], *SP '08*

Wireless attacks against ICDs
Halperin et al. [12], *SP '08*

Proximity-based access control using ultrasonic frequency
Rasmussen et al. [65], *CCS '09*

Security and privacy of neural devices
Denning et al. [66], *Neurosurg Focus '09*

Biometric requirements for key generation
Ballard et al. [67], *USENIX '08*

ECG-based key agreement
Venkatasubramanian et al. [68], *INFOCOM '08*

Cloaker: external proxy device
Denning et al. [69], *HotSec '08*

BioSec extension for BANs
Venkatasubramanian and Gupta. [70], *ICISIP '06*

BioSec: extracting keys from PVs
Cherukuri et al. [71] *ICPPW '03*

Authentication and secure key exchange using IPI
Poon et al. [72], *Commun. Mag '06*

Research Challenges

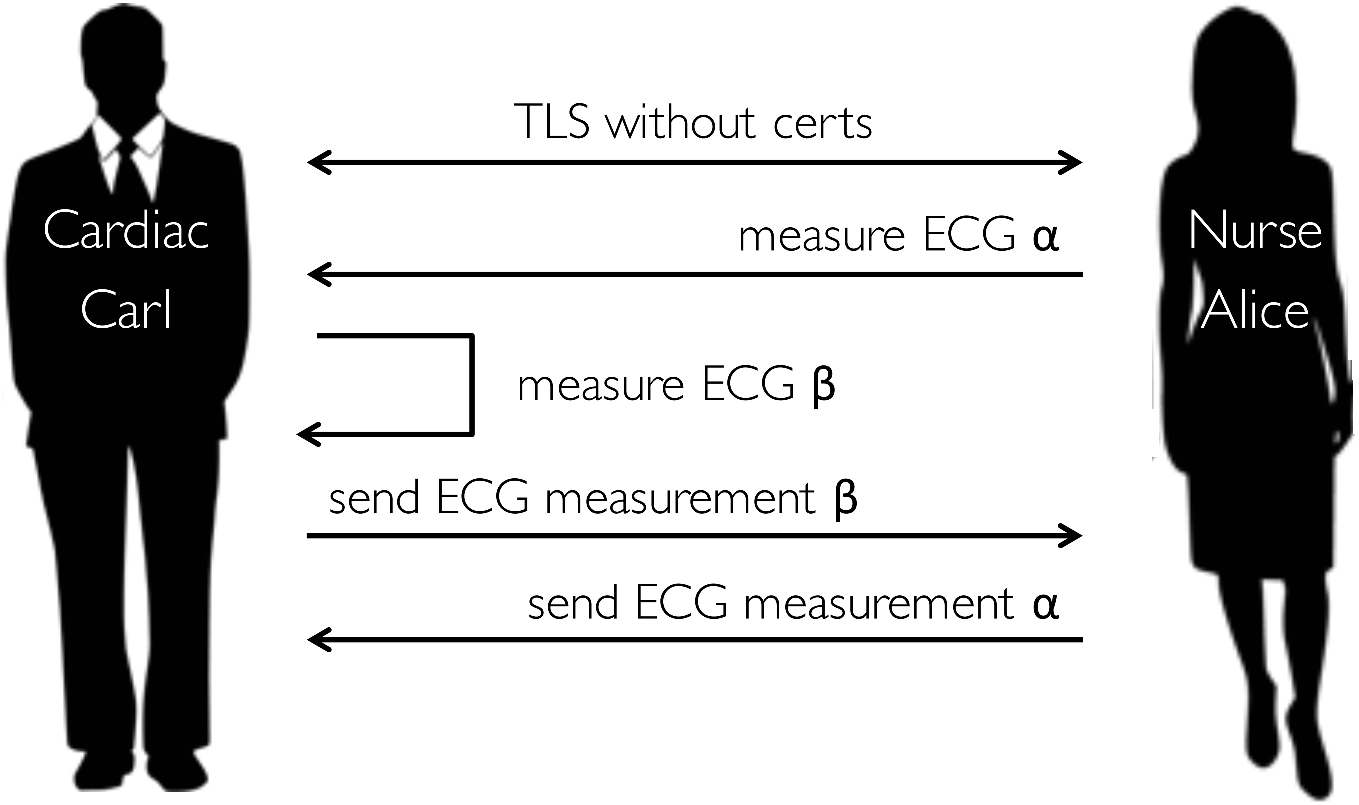
- Access to Implantable Medical Devices
  - Is much harder then getting other components

- Reproducibility
  - Limited analysis of attacks and defenses
  - Do not use *meat-based* human tissue simulators
  - Do use a calibrated saline solution at 1.8 g/L at 21 ◦C
    - The complete design is described in the ANSI/AAMI PC69:2007 standard [92, Annex G]

Security and Privacy Mechanisms

- Biometric and Physiological Values
  - Key generation and agreement
- Electrocardiogram (ECG)
  - Heart activity signal
- Interpulse interval
  - Time between heartbeats

H2H Authentication Protocol



Cardiac Carl

Nurse Alice

TLS without certs

measure ECG α

measure ECG β

send ECG measurement β

send ECG measurement α

[Rostami, CCS, 13]

H2H Authentication Protocol

- **Adversarial Assumptions**
  - Active attacker with full network control
  - The attacker cannot:
    - Compromise the programmer
    - Engage in a denial-of-service
    - Remotely measure ECG to weaken authentication

[Rostami, CCS, 13]

Physiological Values as an Entropy Source

- How do ECG-based protocols work in practice?
  - Age, Exertion, Noise

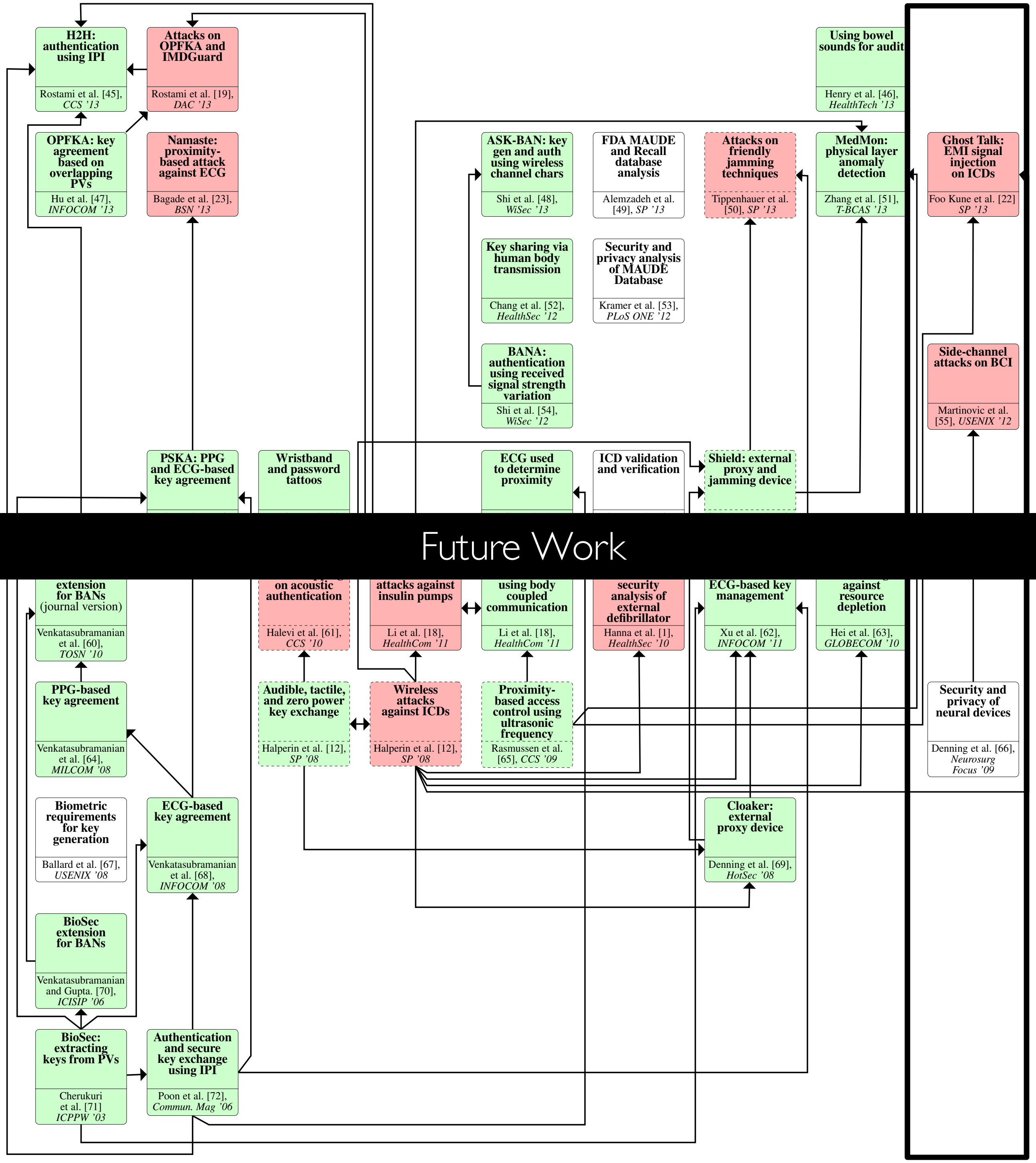
[Rostami, S&P, 2013] [Chang, HealthTech, 2012]

- ECG-based protocols rely on an analysis of ideal data in an unrealistic setting
  - Data sample is close to their ideal distribution
  - Very accurate estimate of distribution characteristics
  - Extract randomness using the estimate on the same data sample

- Observability
  - Using video processing techniques to extract ECG-signals

[Poh, Biomedical Engineering, 11]

Future Work



H2H: authentication using IPI — Rostami et al. [45], *CCS '13*

Attacks on OPFKA and IMDGuard — Rostami et al. [19], *DAC '13*

Using bowel sounds for audit — Henry et al. [46], *HealthTech '13*

OPFKA: key agreement based on overlapping PVs — Hu et al. [47], *INFOCOM '13*

Namaste: proximity-based attack against ECG — Bagade et al. [23], *BSN '13*

ASK-BAN: key gen and auth using wireless channel chars — Shi et al. [48], *WiSec '13*

FDA MAUDE and Recall database analysis — Alemzadeh et al. [49], *SP '13*

Attacks on friendly jamming techniques — Tippenhauer et al. [50], *SP '13*

MedMon: physical layer anomaly detection — Zhang et al. [51], *T-BCAS '13*

Ghost Talk: EMI signal injection on ICDs — Foo Kune et al. [22] *SP '13*

Key sharing via human body transmission — Chang et al. [52], *HealthSec '12*

Security and privacy analysis of MAUDE Database — Kramer et al. [53], *PLoS ONE '12*

BANA: authentication using received signal strength variation — Shi et al. [54], *WiSec '12*

Side-channel attacks on BCI — Martinovic et al. [55], *USENIX '12*

PSKA: PPG and ECG-based key agreement

Wristband and password tattoos

ECG used to determine proximity

ICD validation and verification

Shield: external proxy and jamming device

extension for BANs (journal version) — Venkatasubramanian et al. [60], *TOSN '10*

on acoustic authentication — Halevi et al. [61], *CCS '10*

attacks against insulin pumps — Li et al. [18], *HealthCom '11*

using body coupled communication — Li et al. [18], *HealthCom '11*

security analysis of external defibrillator — Hanna et al. [1], *HealthSec '10*

ECG-based key management — Xu et al. [62], *INFOCOM '11*

against resource depletion — Hei et al. [63], *GLOBECOM '10*

PPG-based key agreement — Venkatasubramanian et al. [64], *MILCOM '08*

Audible, tactile, and zero power key exchange — Halperin et al. [12], *SP '08*

Wireless attacks against ICDs — Halperin et al. [12], *SP '08*

Proximity-based access control using ultrasonic frequency — Rasmussen et al. [65], *CCS '09*

Security and privacy of neural devices — Denning et al. [66], *Neurosurg Focus '09*

Biometric requirements for key generation — Ballard et al. [67], *USENIX '08*

ECG-based key agreement — Venkatasubramanian et al. [68], *INFOCOM '08*

Cloaker: external proxy device — Denning et al. [69], *HotSec '08*

BioSec extension for BANs — Venkatasubramanian and Gupta. [70], *ICISIP '06*

BioSec: extracting keys from PVs — Cherukuri et al. [71] *ICPPW '03*

Authentication and secure key exchange using IPI — Poon et al. [72], *Commun. Mag '06*

Trusted Sensor Interface

- Current systems trust their analog sensor inputs
- This assumption may not always hold
- Forging signals using electromagnetic interference
  - Inject cardiac waveform

[Foo Kune, S&P, 2013]

Neurosecurity

- Neurostimulators
  - What are the new attack surfaces
  - What are the implications of recording and transmitting brainwaves

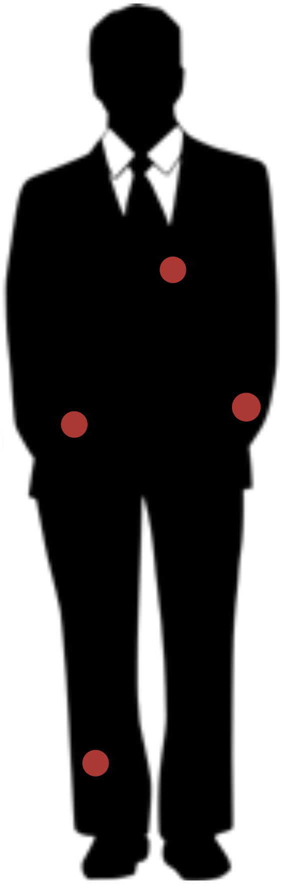
- Brain computer interfaces

- Cognitive recognition *could* leak:
  - Passwords, personal information

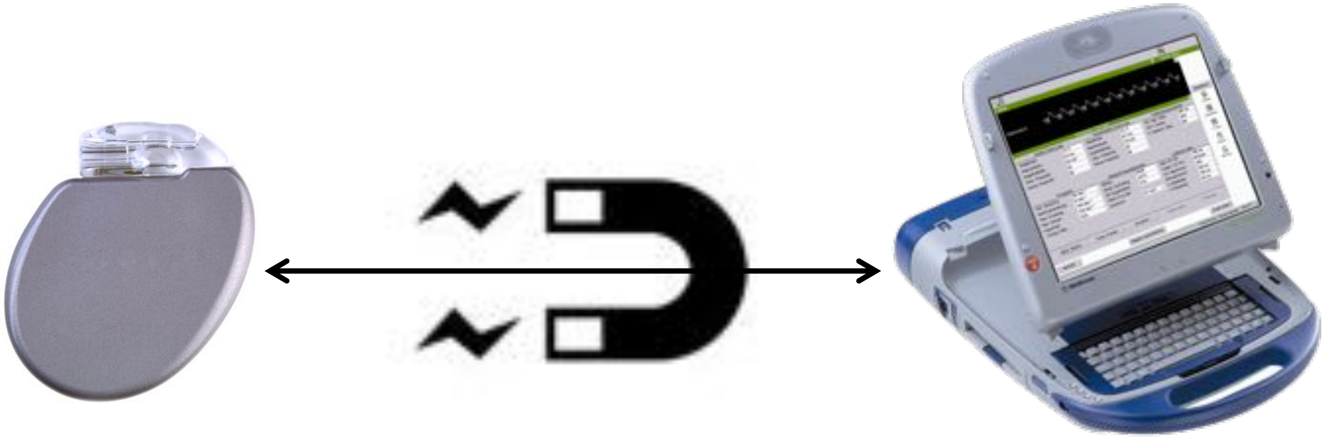
[Martinovic, USENIX, 2012], [Denning, Neurosurg Focus, 09]

Questions?

- IMDs are becoming more common
  - Improving patient outcome
- Research gaps exists
  - Software
  - Sensor Interface
- Areas for future work include
  - Physiological values as an Entropy Source
  - Trusted Sensor Interface
  - Neurosecurity
- See our paper for more details!



This is Not Just an Engineering Problem



[Halperin, S&P, 08]