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

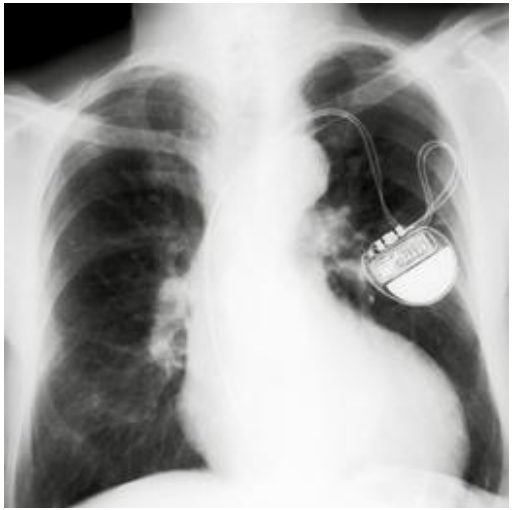
Rushanan et al.

IEEE Symposium on Security and Privacy, 2014

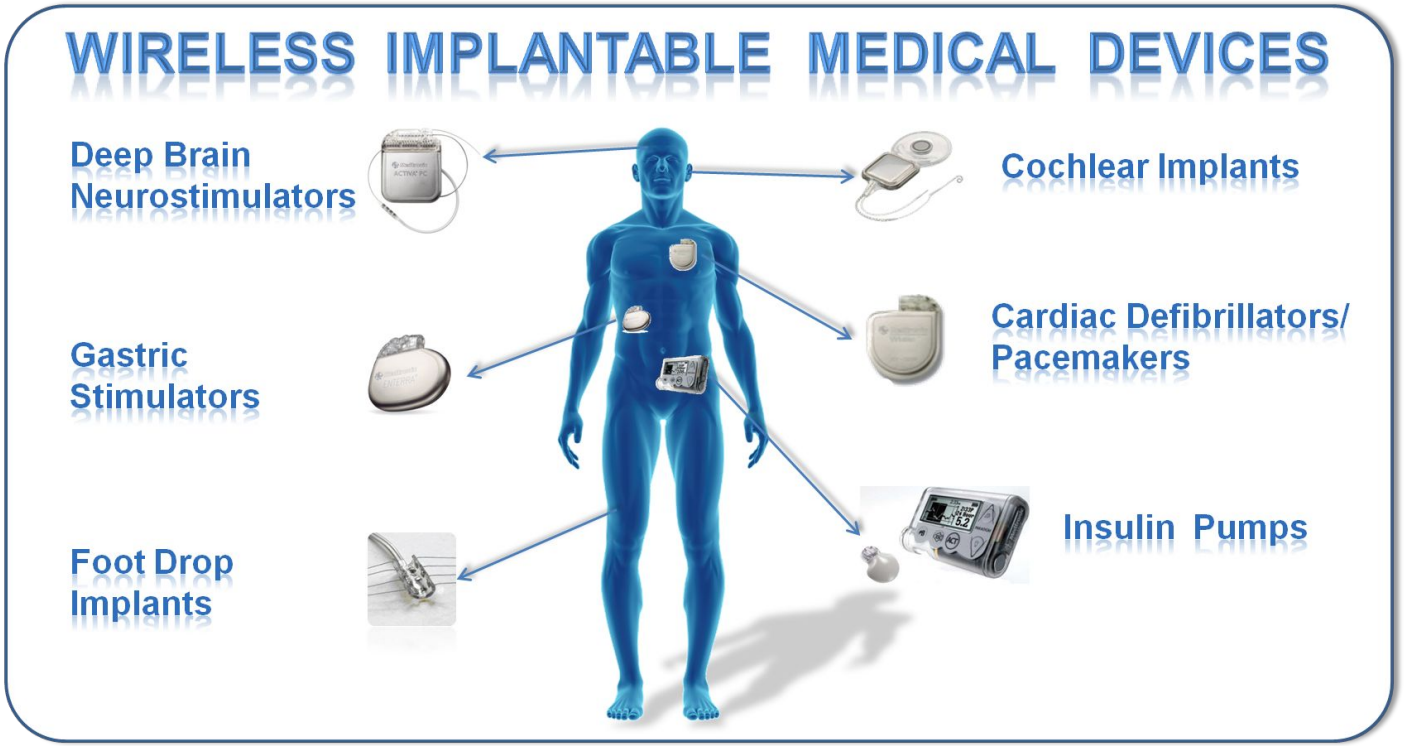
Presented by: Sam White

Background

- Implantable Medical Devices (IMDs) and Body Area Networks (BANs) are becoming widely used
  - Remote monitoring of patient's health
  - Treatment can be adjusted wirelessly
- Made possible by advances in technology
  - Energy-efficient architectures
  - Low-power wireless connectivity
  - Low cost of embedded systems



Background


WIRELESS IMPLANTABLE MEDICAL DEVICES
Deep Brain Neurostimulators
Cochlear Implants
Gastric Stimulators
Cardiac Defibrillators/ Pacemakers
Foot Drop Implants
Insulin Pumps

Background

- IMDs raise many questions related to security:
  - Integrity of data
  - Availability of the system
  - Confidentiality of the patient
- Trade-offs in privacy and security:
  - Encrypted data not accessible outside patient’s health care network

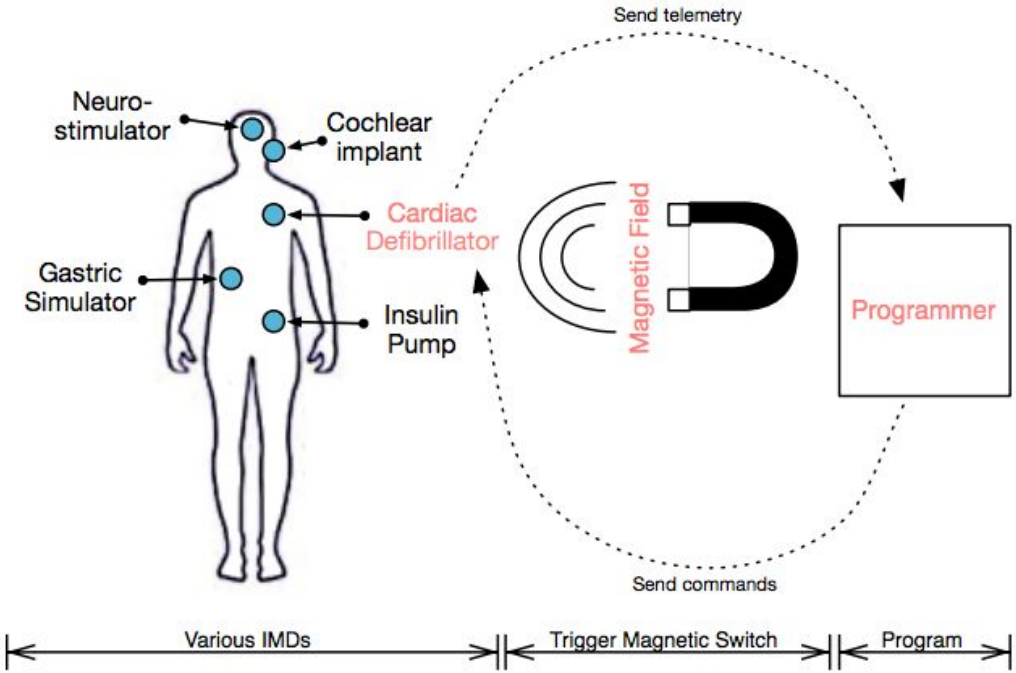
Motivation

- Research on the security of IMDs and BANs is still an emerging field
  - What are the key concepts and issues?

- Subdivide current/past work into 3 categories:
  1. Security of wireless telemetry
  2. Detection & prevention of software vulnerabilities
  3. Security of hardware & sensor interfaces

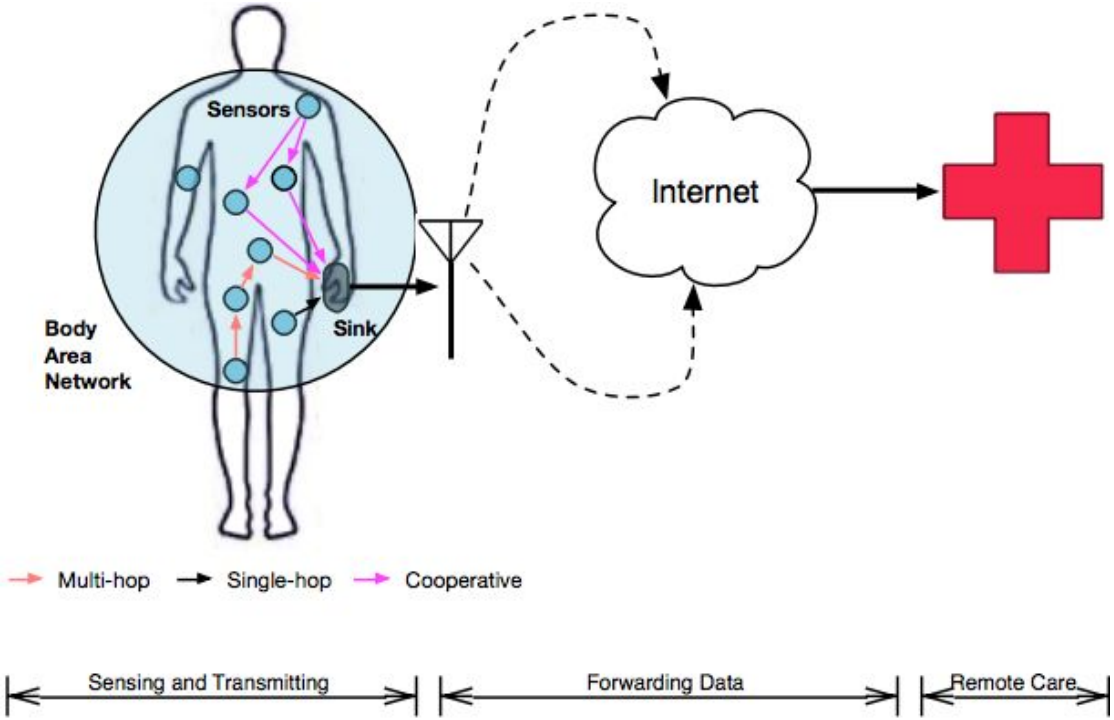
Definitions

- IMDs consist of:
  - Analog front-end
  - Memory and storage
  - Microprocessor
  - Telemetry interface
  - Power mgmt.



Definitions

- BANs consist of:
  - Sensors
  - Actuators
  - Sink



Definitions

- Medical Implant Communication Service (MICS) has a dedicated radio frequency band
- Communication protocols for IMDs:
  - ISO/IEEE 11073: full communication stack protocol
  - HL7, IHE, ASTM F2761: application layer protocols
    - Security mechanisms are mostly optional

Privacy

- IMDs and BANs must protect patient’s privacy:
  - Device-existence privacy
  - Device-type privacy
  - Device-specific ID privacy
  - Measurement and log privacy
  - Bearer privacy
  - Tracking

Adversarial Model

- The adversarial model applies to IMDs and BANs
  - Passive vs. active adversaries
  - Outsider vs. insider
  - Single entity vs. coordinated group
  - Sophisticated vs. unsophisticated
- Threats can be targeted at:
  - Patient
  - System resources
  - Device manufacturer

Telemetry Interface Threats

- Previous work has exposed many vulnerabilities in the telemetry interface
- Various solutions have been proposed:
  - Biometric key generation
  - Distance-bounding protocols
  - Out-of-Band authentication
  - External wearable devices
  - Anomaly detection

Software Threats

- IMDs are increasingly software-controlled digital circuits, rather than analog devices
  - Software bugs are the cause of 30-40% of device recalls
- But, the proprietary software is closed source ...

Research Issues

- Reproducibility of results is difficult because:
  - Privacy of patients
  - Proprietary software, firmware
  - Lack of access to current devices
  - Use of simulated human bodies
  - Use of physiological values

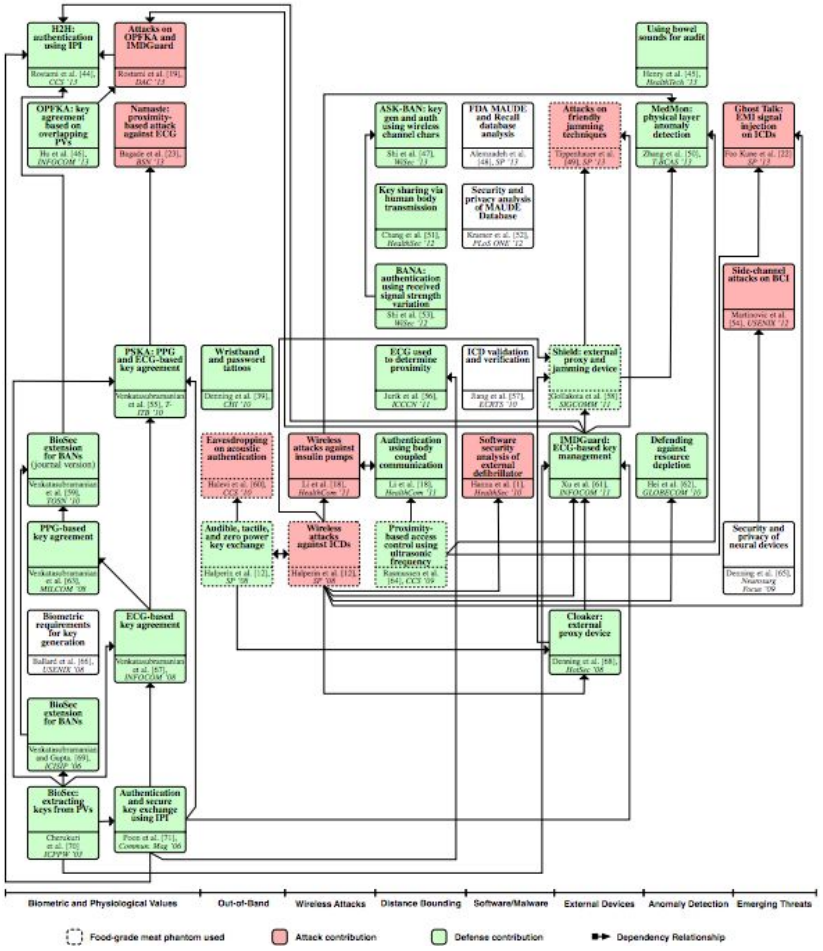
Research Issues

- The use of physiological values in cryptographic key generation is questionable
  - Is the distribution of interpulse intervals random enough to be secure?
  - Is IPI detectable? (from a distance? by touch?)

Research

Threat	Attacks	Goal Compromised by Indicated Threat					Defenses
		Confidentiality	Integrity	Availability	Privacy	Safety	
Wireless eavesdropping	[12], [18], [49]	✓			✓		[12], [18], [44], [46], [47], [50], [51], [53], [55], [58], [59], [61], [63], [64], [67]–[75]
Wireless modification	[12], [18], [19]		✓	✓		✓	[12], [18], [44], [46], [47], [50], [51], [53], [55], [58], [59], [61], [63], [64], [67]–[75]
Wireless replay	[12], [18]		✓	✓		✓	[12], [18], [44], [46], [47], [50], [51], [53], [55], [58], [59], [61], [63], [64], [67]–[75]
Wireless jamming				✓		✓	[61], [68]
Analog sensor injection	[22]		✓			✓	[22]
Battery depletion	[12]			✓		✓	[12], [58], [62], [68]
Protocol Design Flaws	[12], [18], [19], [23], [49], [60]	✓	✓	✓	✓	✓	Not Applicable
Software Flaws	[76]	✓	✓	✓	✓	✓	[57], [76]
Side channels	[23], [54], [60]	✓	✓	✓	✓	✓	[54]

Research


H2H: authentication using IPI
Rostami et al. [44], CCS '13
Attacks on OPFKA and IMDGuard
Rostami et al. [19], DAC '13
OPFKA: key agreement based on overlapping PVs
Hu et al. [46], INFOCOM '11
Namaste: proximity-based attack against ECG
Bagade et al. [23], BSN '13
Using bowel sounds for audit
Henry et al. [45], HealthTech '13
ASK-BAN: key gen and auth using wireless channel chars
Shi et al. [47], WiSec '13
FDA MAUDE and Recall database analysis
Alemzadeh et al. [48], SP '13
Attacks on friendly jamming techniques
Tippenhauer et al. [49], SP '13
MedMon: physical layer anomaly detection
Zhang et al. [50], TJICAS '13
Ghost Talk: EMI signal injection on ICDs
Foo Kune et al. [22], SP '13
Key sharing via human body transmission
Chang et al. [51], HealthSec '12
Security and privacy analysis of MAUDE Database
Kramer et al. [52], PLoS ONE '12
BANA: authentication using received signal strength variation
Shi et al. [53], WiSec '12
Side-channel attacks on BCI
Martinovic et al. [54], USENIX '12
PSKA: PPG and ECG-based key agreement
Venkatasubramanian et al. [55], P-ITB '10
Wristband and password tattoo
Denning et al. [39], CHI '10
ECG used to determine proximity
Jurik et al. [56], ICCCN '11
ICD validation and verification
Jiang et al. [57], EURTS '10
Shield: external proxy and jamming device
Gollakota et al. [58], SIGCOMM '11
BioSec extension for BANs (journal version)
Venkatasubramanian et al. [59], TOSN '10
Eavesdropping on acoustic authentication
Halevi et al. [60], CCS '10
Wireless attacks against insulin pumps
Li et al. [18], HealthCom '11
Authentication using body coupled communication
Li et al. [18], HealthCom '11
Software security analysis of external defibrillator
Halevi et al. [1], HealthSec '10
IMDGuard: ECG-based key management
Xu et al. [61], INFOCOM '11
Defending against resource depletion
Hei et al. [62], GLOBECOM '10
PPG-based key agreement
Venkatasubramanian et al. [63], MILCOM '09
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. [64], CCS '09
Security and privacy of neural devices
Denning et al. [65], Neurosurg Focus '09
Biometric requirements for key generation
Ballard et al. [66], USENIX '10
ECG-based key agreement
Venkatasubramanian et al. [67], INFOCOM '08
Cloaker: external proxy device
Denning et al. [68], HotSec '08
BioSec extension for BANs
Venkatasubramanian and Gupta, [69], ICISIP '09
BioSec: extracting keys from PVs
Cherukuri et al. [70], ICPPW '03
Authentication and secure key exchange using IPI
Poon et al. [71], Commun. Mag '06
Biometric and Physiological Values
Out-of-Band
Wireless Attacks
Distance Bounding
Software/Malware
External Devices
Anomaly Detection
Emerging Threats
Food-grade meat phantom used
Attack contribution
Defense contribution
Dependency Relationship

Conclusions

- IMDs are increasingly popular
- The security and privacy are open research questions
- Formally categorizing past research helps:
  - Clarify the state of the field
  - Relate future research directions to past work
  - Illustrate the impact of the research on practice

Discussion

- What trade-offs in security/privacy are acceptable to patients?
- Are there other ways to categorize the research?
- What about research into patient privacy?
- What has changed in the field since Halperin et al.’s 2008 paper?

Thank you