Security and Privacy of Wireless Implantable Medical Devices

Security Forum 2013
Hagenberg, 17.04.2013

Dipl.-Ing. Dr. Gregor Koenig
Outlook

- Overview
- Device Hacking
- Safety & Utility Goals
- Security & Privacy Goals
- Tensions of Goals
- Countermeasure / Approaches in Research
Implantable Medical Devices

- Deep Brain Stimulators
- Ocular Implants
- Cochlear Implants
- Pacemakers
- Implantable Cardiac Defibrillators
- Implantable Sensors, e.g. Glucose
- Implantable Drug Pumps, e.g. Insulin
- Gastric Stimulators
- Smart Pills
- Prosthetic Limbs
Why Wireless IMDs?

- Ease of communication with implanted device
  - During Implantation, Device Setup and Testing
  - Therapy adjustments
  - Software Updates

- Remote monitoring (over internet)
  - Reduction of hospital visits by 40% and cost per visit by $1800\textsuperscript{1}

Default Usage of Programmers

- Used during implantation / operation
- Interrogated and program device wirelessly
- Continuous communication during procedure
- Control device’s test-Mode, e.g. defibrillation
ICD Hacking

- First real attack on Implantable Cardiac Defibrillator
  University of Washington and
  University of Massachusetts Amherst

- ICD Device, on US market since 2003

- Replay Attacks
- Disclosure of Sensitive Data and
  Bio-Signals
- Drain Energy
- Reconfiguration of Device

Halperin, Heydt-Benjamin, Ransford et al., Pacemakers and Implantable Cardiac Defibrillators:
ICD Hacking: Equipment

- Original External Programmer & Device
- GNU Radio Open Source SW Radio
- Low-Cost Radio Hardware and Antenna (< 1000$)
- Standard Oscilloscope
Reverse Engineering

- Physical Layer
  - RF transmission around 175 kHz
  - Modulation
    2-FSK, DBPSK
  - Decoding using known plaintexts
    Non-Return-to-Zero Inverted with Bit Stuffing

- Device Communication

Eavesdropping

• Sensitive Information

• Sniff Vital Signals
  • ICDs emit re-constructible vital signals
Active Attacks

• Replay Attacks
  • Retransmission of recorded traces

• Request ICD and patient data

• Drain Energy
  • Constantly wake up the ICD

• Change Device Configuration
  • Change ICD settings, e.g. date
  • Change Patient/Therapy Configuration
  • Induce electric shock using fibrillation-test mode
Safety and Utility Goals of IMDs

- **Data Access**
  - Patient name, Diagnosis, Therapy, Physiological Values, Events, Allergies, Medication, …
  - Emergency Situations

- **Data Accuracy**
  - Measured Values, Events, and Timestamps have to be correct

- **Device Identification**
  - Presence and Type of Device should be advertised
  - Imagery (MRI)
  - Surgery
Safety and Utility Goals of IMDs 2

• Configurability
  • Choose and Change Settings, e.g. Therapy
  • Patient Access, e.g. Open-Loop Insulin Pumps

• Updatable Software
  • Avoids need to explant device, which may lead to infections etc.

• Multi-Device Coordination
  • Closed-Loop Insulin Pumps, CROS hearing aids

• Resource-efficient

• Auditable
Security and Privacy Goals

• Authorization
  • Personalized Authorization
  • Role-Based Authorization
  • Prevent accidental or intentional misuse

• Device Existence Privacy

• Device Type Privacy
Security and Privacy Goals 2

- Specific-Device ID Privacy
  - Traceability and Location Privacy

- Bearer Privacy

- Measurement and Log Privacy
  - Data Integrity
  - Medical or Technical Logs
Safety Goals vs. Security Goals

• Accessibility vs. Security
  • Cryptographic security vs. Open access requirement in emergency situations

• Device Resources vs. Security
  • Energy consumption of additional computations

• Usability vs. Security
  • Long-distance communication offers advantages, e.g. home-monitoring
  • Increased risk from a security perspective
Classical Approaches

• Classical Cryptographic Approaches
  • Passwords or passphrases cannot be used without limitations
  • Additional Body Implant, e.g. RFID

Denning et al.; Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices; CHI 2010
Additional Approaches

• Activation of Programmer by Authority
  • Programmer with internet access requests authorization e.g. of Manufacturer, primary care site
  • Approved doctor’s ID card
  • Automatically expiring certificates

• Accountability
  • Deter attacker
  • Log of accessing entities in a reliable way Device’s Credentials, Healthcare Professionals Credentials
Secondary Information Channels

- Patient awareness
  - Inform Patient about Access, e.g. Buzzer or Alarm Sound

- Authorization
  - Additional Activation via Near Field Communication
  - Location awareness
    Change of environment e.g. using Accelerometers


D. Halperin et al.; Security and Privacy for Implantable Medical Devices; IEEE Pervasive Computing Vol. 7/1, 2008
Experimental Approaches for BANs

• Body Area Network
  • E.g. Glucometer and Insulin Pump communicating through body

• Biosignals as shared secret for secure communication in BANs
  • Heart Rate Variability
  • R-R Interval of QRS complex
  • Plethysmography

• Topography of body
• Noise in human body

K. Venkatasubramanian; Physiological Value-Based Efficient Usable Security Solutions for Body Sensor Networks; ACM Trans. Sensor Netw. 6, 4, Article 31 (July 2010)
Discussion

• Real Risk?
  • Classification of incident-class does not exist

• Risk Analysis vs. Privacy and Security
  • Introduction of new risks

• Criminal Implications
  • IMD during Autopsy?
Links and Literature

- Ann Arbor Research Center for MD Security
  http://secure-medicine.org
  http://secure-medicine.org/publications

- Professor Kevin FU, University of Michigan
  http://web.eecs.umich.edu/~kevinfu

- USENIX Workshop on Health Information Technologies, 12.08.2013,
  https://www.usenix.org/conference/healthtech13
Thank you!

Dipl.-Ing. Dr. Gregor König
gkoenig@barracuda.com

Barracuda Networks AG
Lassallestraße 7a
1020 Wien