PACEMAKERS AND IMPLANTABLE CARDIAC DEFIBRILLATORS:
SOFTWARE RADIO ATTACKS AND ZERO-POWER DEFENSES

Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark,
Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel

MEDICAL TECHNOLOGY

- Implantable Medical Devices (IMDs)
  - pacemakers
  - Implantable Cardioverter Defibrillators (ICDs)
  - neurostimulators
  - drug pumps

... TURNED WIRELESS

- Wireless Communication
  - patient data
  - current settings
- Wirelessly Reprogrammable
  - alter device behavior non-invasively

ADVERSARY TYPES

- Adversary with a commercial ICD programmer
- Passive adversary (without commercial programmer)
- Active adversary (without commercial programmer)

INTERCEPTING ICD COMMUNICATIONS

- Reverse-engineered some of the communications protocol
- Constructed a commodity (not commercial) software radio
- Eavesdropping with Universal Software Radio Peripheral and GNU Radio libraries

EAVESDROPPING

- Patient data transmitted in cleartext
  - name
  - date of birth
  - medical ID number
  - patient history
- Also sent data about physician and ICD

ACTIVE ATTACKS

- Transmit-only replay attacks
  - disclosing ICD, patient, and cardiac data
  - changing patient name or ICD clock
  - changing therapies
  - inducing fibrillation (safeguards built into commercial model)
- Power denial of service attack

DEFENSE CONCERNS

- Balance security with ease of use in medical emergencies
- Zero-power defenses are ideal
    - ICDs run on batteries
    - Power is a precious commodity
    - Battery replacement can be invasive

ZERO-POWER DEFENSES

- Zero-Power Notification
- Zero-Power Authentication
- Zero-Power Sensible Key Exchange

ZERO-POWER NOTIFICATION

- Notifies patient of *any* activity
- Uses an implanted piezo-element to produce sound
- Built on Wireless Identification and Sensing Platform (WISP), which contains RFID technology
- WISP draws energy from the radio frequency signal, which is used for power instead of the battery
- Piezo-element can also produce vibration instead of sound

ZERO-POWER AUTHENTICATION

- All commercial programmers know a master key K_M, and each device has an identity I

1. Programmer submits a request to authenticate to WISP
2. WISP harvests power and responds with I and a nonce N
3. Programmer computes $K = f(K_M, I)$ and sends $R = \mathrm{RC5}(K, N)$
4. WISP verifies the correctness of R

- Successful zero-power authentication should be required before engaging in power-consuming processes

ZERO-POWER SENSIBLE KEY EXCHANGE

- Allows for secure communications between a programmer and an IMD

  1. Programmer supplies unmodulated radio frequency signal to power the IMD
  2. IMD generates and sends a random value as a session key

- Intended to not be easily overheard

QUESTIONS