Implantable Medical Device Security

or

How the Meat Industry Advances Phys. Security

Paul Elliott
CIS607 Physical Security
February 15, 2012
What the heck is an IMD?

Examples: pacemakers, implantable cardiac defibrillators, drug delivery systems, neurostimulators

Help treat and prevent:

- cardiac arrhythmia, diabetes, Parkinson’s disease, etc

Nearly 25 million deployed in the United States by 2008 (*cough* Baby Boomers *cough*)
(Software) Bugs in the Hospital

- Things never work perfectly
  - At least 6 software-related “Class I” FDA recalls in first half of 2010 (SFLC)
  - Therac-25 – when bugs kill patients
  - Legal system compounds: Riegel vs Medtronic, 2008

So Looking Forward…

- Difficult to prevent even *unintentional* problems, let alone provide security against a determined adversary

- Better to identify these security flaws now rather than later
  - 1982 Tylenol Scare

- What are specific additional challenges for implementing security in the unique realm of implantable medical devices?
Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses
Implantable Cardiac Defibrillator
- Communicates patient data and telemetry
- Administer therapies

- 2.6 million pacemakers and ICDs implanted between 1990-2002

- Wireless capability introduced around 2003-2004
How It Works

- Surgically implanted with initial settings (ie: patient info)
- Test the thing..IMPORTANT
- Communicates wirelessly with commercial programmer (the device, not the savvy geek)
Enter Eve and Mallory

- Insider with commercial programmer…well, you’re toast.
- Passive Adversary
  - Gone Fishing...for private patient data
- Active Adversary
  - Create traffic interference or spurious commands
Tools of the (Hacking) Trade

- Universal Software Radio Peripheral (USRP)

Who/What/Where are you?
Do as I command!
Steps:
1. Find the right frequency
2. Determine modulation (for ICD and programmer)
3. Decode into binary

All this accomplished by just listening (no cryptography)

Successful Attacks

- **Eavesdropping:**
  - Disclosing patient and telemetry data
  - Also DoS battery power

- **Replay (replay replay) attacks:**
  - Locate the device (“I know you’re in there..”),
  - Modification: change patient data, (re)set the ICD’s clock
  - Mayhem: change therapies, induce fibrillation, administer high voltage shock
Let’s Recap

- At the time of this work commercial ICD programmers were not registered, had no enforcement of authorized use only, and could communicated freely with the ICD.
- With a homebrew software radio, an attacker can eavesdrop on sensitive information and initiate replay attacks.
- Where is the silver lining?
Proposed Defenses

- **Key goals:**
  - Security, privacy

- **Key constraints:**
  - Zero-power, sensible

- **Solution: WISPer**
  - Zero-power notification
  - Zero-power authentication
  - Sensible key exchange
Detection: Notification for Patients

- “Chirps” when detecting wireless requests
- Could also produce vibration
- Benefit: notify the primary stakeholder of potential attacks
- Evaluation: audible through 1 cm of bacon

Prevention: Authentication

- Encrypt traffic between device programmer and ICD
- Key management problem (heard that before…)

Use audible signal to exchange 128-bit nonce
- Only audible to programming head, in contact with body
- Used to compute secret key for authentication scheme

- The Shield - “jammer-cum-receiver” (full duplex radio)
- Small wearable device (no need to modify IMD)

Gollakota et al “They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices” (SIGCOMM ’11)
Limitations

- Limited attack
  - Short distance (few centimeters)
  - Time consuming (replay message multiple times)
  - Looked at only a single ICD model

- Is this really a problem?
But Wait! There’s More..

- Host of other (insecure) implantable devices
  - Continuous glucose monitors and insulin pumps

The FDA-approved Medtronic Guardian® REAL-Time Continuous Glucose Monitoring System alerts diabetes patients to high and low glucose levels, allowing them to better manage their diabetes.

©Copyright Medtronic, Inc.
And It Gets Worse…

- Future directions
  - Larger wireless range (over dedicated MICS)
  - Less human input (glucose monitor and insulin pump)
- Software radios in our pockets
- Weak software evaluation in FDA approval process
  - Can’t rely on accountability
What Can We Do?

- Better regulations
  - Remove commercial programmers from “trusted circle”
  - Software review in FDA approval stressing threat models

- Context-aware security (ex: fibrillation tests)
  - Difficult to model all contexts

- Other suggestions?
IMDs and medical technology save lives, but let’s be smart about how we implement them.

- Model *intentional* attacks in the absence of past incidents.

Keep in mind the unique conflicts:

- Security versus safety.
Resources


- All images courtesy of Google Images (unless otherwise stated)