Implantable Medical Devices: Security + Privacy for Pervasive, Wireless Healthcare

Presenter: Kevin Fu
Yoshi Kohno & William Maisel

http://www.secure-medicine.org/

CMOS Workshop, February 18, 2009
Many Collaborators

- **William H. Maisel, MD, MPH**
  - Director, Pacemaker and Defibrillator Service, Beth Israel Deaconess Medical Center
  - Assistant Professor, Harvard Medical School

- **Tadayoshi Kohno**
  - Assistant Professor, CSE, University of Washington

- **Students**
  - Shane Clark, Benessa Defend, Tamara Denning, Dan Halperin, Tom Heydt-Benjamin, Andres Molina, Will Morgan, Ben Ransford, Mastooreh Salajegheh
IMD Security & Privacy is Hard

- Background
  - Unintentional medical malfunctions
  - Intentional medical malfunctions
  - Pacemaker & Implantable Cardioverter Defibrillator (ICD)

- Security analysis of a pacemaker/ICD
  - Violate patient privacy
  - Induce a fatal heart rhythm

- Defensive methods
  - Protect the battery, proper use of cryptography

- The Future
Unintentional Malfunctions in Medical Care
Unintentional Accidents

An Investigation of the Therac-25 Accidents

Nancy G. Leveson, University of Washington
Clark S. Turner, University of California, Irvine

Computers are increasingly being introduced into safety-critical systems and, as a consequence, have been involved in accidents. Some of the most widely cited software-related accidents in safety-critical systems involved a computerized radiation therapy machine called the Therac-25. Between June 1985 and January 1987, six known accidents involved massive overdoses by the Therac-25 — with resultant deaths and serious injuries. They have been described as the worst series of radiation accidents in the 35-year history of medical accelerators.

With information for this article taken from publicly available documents, we present a detailed accident investigation of the factors involved in the overdoses...
Is a malicious intentional malfunction a risk of real concern?
Bad People Do Exist

Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen  03.28.08 | 8:00 PM

Internet griefers descended on an epilepsy support message board last weekend and used JavaScript code and flashing computer animation to trigger migraine headaches and seizures in some users.

The nonprofit Epilepsy Foundation, which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security.

"We are seeing people affected," says Ken Lowenberg, senior director of web and print publishing at the Epilepsy Foundation. "It's fortunately only a handful. It's possible that people are just not reporting yet -- people affected by it may not be coming back to the forum so fast."

The incident, possibly the first computer attack to inflict physical harm on the victims, began Saturday, March 22, when attackers used a script to post hundreds of messages embedded with flashing animated gifs.

The attackers turned to a more effective tactic on Sunday, injecting JavaScript into some posts that redirected users' browsers to a page with a more complex image designed to trigger seizures in both photosensitive and pattern-sensitive epileptics.
Background: Pacemaker & Defibrillator 101
Photos from:
Medtronic
Photos from: Medtronic
Pacemakers: Regulate heartbeat
Pacemakers: Regulate heartbeat
Pacemakers: Regulate heartbeat

> Energy spent on radio & computing, etc. overhead!

< Energy for pacing!
ICDs: Resynchronize the heart

- Implantable Cardioverter Defibrillator (ICD)
- Related to pacemaker
- Large shock: resync heart
- Monitors heart waveforms
Our Tested Pacemaker + ICD

Physical characteristics:
~5-year battery
Waveform memory
Radio interface w/ programmer

Therapies:* 
Steady pacing shocks
≤35 J defibrillation shocks

* detail in [Webster, 1995]
Implantation Scenario

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

Device Programmer

Photos: Medtronic; Video: or-live.com
Implantation Scenario

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

Photos: Medtronic; Video: or-live.com
Implantation Scenario

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring

Photos: Medtronic; Video: or-live.com
Adversaries
Do Not Play by the Rules
802.11 WiFi Sniper Yagi
Uninvited Radio Suitcases

Our Security Analysis of a Pacemaker + ICD
Computer Security

• **Computer Security (Informal Definition):**
  Study of how to design systems that behave as intended in the presence of **determined, malicious** third parties

• **Security is different from reliability**
  ‣ The malicious third party controls the **probability distribution** of malfunctions
  ‣ Security researchers focus on understanding, modeling, anticipating, and defending against these malicious third parties

[This description drawn from the work of Prof. Yoshi Kohno with permission]
Build Your Own Clinic

~10 cm (un-optimized)
Method: Eavesdrop Private Info

Diagnosis
Method: Eavesdrop Private Info

Diagnosis

Hospital
Method: Eavesdrop Private Info

Implanting physician

Diagnosis

Hospital
Method: Eavesdrop Private Info

Implanting physician

Diagnosis

Also:
- Device state
- Patient name
- Date of birth
- Make & model
- Serial no.
- ... and more

Hospital
Method: Sniff Vital Signs

Eavesdropping setup

ICD emits reconstructible vital signs

Issue: Vital signs can say plenty.
Replay Traffic

Photo: Medtronic
Method: Drain Energy

- Implant designed for infrequent radio use
- Radio decreases battery lifetime
Method: Drain Energy

- Implant designed for **infrequent** radio use
- Radio decreases battery lifetime

“Are you awake? Are you awake?”
Method: Drain Energy

- Implant designed for infrequent radio use
- Radio decreases battery lifetime

“Are you awake? Are you awake?”

“Now I am!”
Replay: Turn Off Therapies

<table>
<thead>
<tr>
<th>Rx1</th>
<th>Rx2</th>
<th>Rx3</th>
<th>Rx4</th>
<th>Rx5</th>
<th>Rx6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>35 J</td>
<td>35 J</td>
<td>35 J</td>
<td>35 J</td>
<td>35 J</td>
<td>35 J</td>
</tr>
<tr>
<td>AX&gt;B*</td>
<td>AX&gt;B*</td>
<td>AX&gt;B*</td>
<td>B&gt;AX*</td>
<td>AX&gt;B*</td>
<td>B&gt;AX*</td>
</tr>
</tbody>
</table>

- “Stop detecting fibrillation.”
- Device programmer would warn here

Issue: Can quietly change device state.
Replay: Affect Patient’s Physiology

- **Induce fibrillation** which implant ignores
- Again, at close range
- In other kinds of implant:
  - Flood patient with drugs
  - Overstimulate nerves, ...

**Issue:** Puts patient safety at risk.

Photo: or-live.com
Defensive Direction: Zero-Power
(No time today. Google for “pacemaker zero-power”)
Prototype Defenses

- Focus on sleep deprivation
- In zero power (harvested RF energy)
  - Challenge-response authentication
  - Patient notification mechanism
  - Sensible key exchange
- Human is in the loop
Prototype defenses against some of the attacks.

Main idea: defend without using battery.
B.Y.O.P.

- **WISP** = RFID + computation [UbiComp ’06]
- **WISPer** = **WISP** + our code
- “Maximalist” crypto [RFIDSEC ’07]
- Prototype: 913 MHz RFID band

Goal: External party pays for power.
Patient notification

ICD
Patient notification

Auth

ICD
Patient notification

Auth

Go ahead!

BZZZZZZZZZZZZZZZZZZZZZZZZ

ICD
WISPer as Gatekeeper

- Authenticate against WISPer
- WISPer to ICD: “OK to use radio”
- Acoustic patient notification
- How to deter enemies? (Open question!)
Sensible key exchange

- Session setup

![Diagram showing key exchange process involving a programming head, tissue, key material, and an ICD. The diagram illustrates the modulation of an acoustic wave at approximately 4 kHz.]
Testing WISPer: Simulated Torso

Energy harvesting through tissue is possible.
How WISPer Could Work

- Auxiliary device (possibly integrated)
- Audible or tactile patient alert
- Patient detects activity: am I in a clinic?
- Fail open: sensible, tactile key exchange
IMDs + Wireless + Internet: The Future

(Condensed version of the future. Ask Kevin for details.)
Yet some remarkable changes are on the horizon, said Dr. Larry Wolff, a UC Davis Medical School professor who specializes in implanting defibrillators. "I believe over time we could make programming changes on the telephone," he said, although that's not possible now.
Going the Distance

“Eventually, Vanu’s [software radio] technology could be used to create a phone.”
Future Threats: Viruses?

- Software updates?
- SQL injection?
- Buffer overflows?
- Radio as infection vector?
- Computer viruses, full circle?

Image credit: Health & Development Initiative, India
Medical Device Trends

- Further computerization of care
- Longer range communication
- Tight integration with the Internet
- Cooperation among devices

Issue: All of these bring risks.
Summary of IMD Sec. & Priv.

- Risks today: Unintentional interference
  - Radio interference
  - Threats: Metal detectors, accidents, misidentification

- Future risks: Intentional interference
  - Threats from wireless and Internet connectivity
  - Malware: Human-computer-immunodeficiency (HCI) virus?
  - Tough problems: Software updates, remote monitoring, ...
Wireless + Internet Can Improve Healthcare

But not without fully understanding security and privacy

- Insulin pump
- Artificial pancreas
- Neurostimulators
- Artificial vision
- Obesity control
- Programmable Vasectomy
Extra slides

- Google us for more information.