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

Kevin Fu
Assistant Professor
Department of Computer Science
University of Massachusetts Amherst
http://www.cs.umass.edu/~kevinfu/

Dartmouth College Computer Science Colloquium
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
Risks of Implantable Medical Devices: Just Add Internet + Wireless
A fatal exception 0E has occurred at 0137:BFFA21C9. The current application will be terminated.

* Press any key to terminate the current application.
* Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue _
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
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.¹

With information for this article taken from publicly available documents, we present a detailed accident investigation of the factors involved in the overdoses.
Changing Trends in Pacemaker and Implantable Cardioverter Defibrillator Generator Advisories

WILLIAM H. MAISEL, WILLIAM G. STEVENSON, and LAURANCE M. EPSTEIN

From the Cardiac Arrhythmia Service, Cardiovascular Division, Department of Medicine, Brigham and Women’s Hospital, Boston, Massachusetts

MAISEL, W.H., ET AL.: Changing Trends in Pacemaker and Implantable Cardioverter Defibrillator Generator Advisories. Pacemaker and implantable cardioverter defibrillator (ICD) generator recalls and safety advisories occur frequently, affect many patients, and are increasing in number and rate. It is unknown if advances in device technology have been accompanied by changing patterns of device advisory type. Weekly FDA Enforcement Reports from January 1990 to December 2000 were analyzed to identify all advisories involving pacemaker and ICD generators. This article represents additional analysis of previously cited advisories and does not contain additional recalls or safety alerts over those that have been previously reported. The 29 advisories (affecting 159,061 devices) from the early 1990s (1991–1995) were compared to the 23 advisories (affecting 364,084 devices) from the late 1990s (1998–2000). While the number of device advisories did not change significantly, ICD advisories became more frequent and a three-fold increase in the number of devices affected per advisory was observed. The number of devices affected by hardware advisories increased three-fold, due primarily to a 700-fold increase in electronic/injury abnormalities and a 20-fold increase in potential battery/capacitor malfunctions. Other types of hardware abnormalities (defects in the device header, hermetic seal, etc.) became less common. The number of devices recalled due to firmware (computer programming) abnormalities more than doubled. The remarkable technological advances in pacemaker and ICD therapy have been accompanied by changing patterns of device advisory type. Accurate, timely physician and patient notification systems, and routine pacemaker and ICD patient follow-up continue to be of paramount importance. (PACE 2002; 25:1670–1678)

Pacemaker and ICD Generator Malfunctions

Analysis of Food and Drug Administration Annual Reports

William H. Maisel, MD, MPH
Maryann Moreland, MD
Beau D. Zwicknauer, MD
Thomas P. Cross, MD, MPH
Owen H. Tevar, MD
Benjamin Tillman, PhD, MPA
Daniel H. Schulz, MD

ACKNOWLEDGMENTS AND IMPLANTABLE CARDIOVERTER-DEFIBRILLATORS (ICDs) are at the cutting edge of medical innovation of the past century. Yet, despite millions of implants worldwide and their increasingly frequent use, surprisingly little is known about device reliability. Pacemakers and ICDs occasionally malfunction. Several database registries have monitored pacemaker and ICD safety performance but have been limited by their relatively small size or voluntary nature. In total, hundreds of device malfunctions affecting dozens of pacemaker and ICD models have been reported. A study of pacemaker and ICD advisories, a surrogate marker of device reliability, demonstrated that the number and rate of pacemakers and ICDs affected by advisory has increased since 1990.

Pacemakers and ICDs have become increasingly sophisticated. For example, devices in the early 1990s typically had less than 1 kbit of random access memory, compared with more than 20 kbit in modern ICDs. Mean ICD failures have decreased in size by more than 80% during the past 15 years, while maintaining their high energy output and timely performance.

Although pacemakers and ICDs are implantable lifelong devices that have saved many lives, careful monitoring of device performance is still required.

Reprinted with permission from JOURNAL OF PACING AND CLINICAL ELECTROCARDIOLOGY, Volume 25, No. 12, December 2002 Copyright © 2002 by Futura Publishing Company, Inc., Amherst, NY 14226-6138

December 2002 PACE, Vol. 25, No. 12

Address for reprints: William H. Maisel, M.D., M.P.H., Cardiovascular Div. Brigham and Women’s Hospital, 75 Francis St. Boston, MA 02115. Fax: 617-732-7134; email: wmasel@partners.org

Received April 30, 2002; revised July 17, 2002; accepted September 12, 2002.

December 2002, PACE, Vol. 25, No. 12

©2002 American Health Association. All rights reserved.
Wardrobe Malfunctions

Hospital Bracelets Face Hurdles as They Fix Hazard

Roosevelt Hospital in Manhattan began using the standard red and yellow wristbands this month, but is hesitating on purple.

By ANEMONA HARTOCOLLIS
Published: September 24, 2008
## Episode Query Selections

### Show All Episodes

<table>
<thead>
<tr>
<th>Episode</th>
<th>Date/Time</th>
<th>Type</th>
<th>Rate bpm</th>
<th>Therapy/Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,230</td>
<td>23-JUN-05 19:10</td>
<td>Spont</td>
<td>VF</td>
<td>Diverted</td>
</tr>
<tr>
<td>1,229</td>
<td>20-JUN-05 12:08</td>
<td>Spont</td>
<td>VF</td>
<td>Diverted</td>
</tr>
<tr>
<td>1,228</td>
<td>21-MAY-07 21:22</td>
<td>ATR</td>
<td>130</td>
<td>???:??</td>
</tr>
<tr>
<td>1,227</td>
<td>21-MAY-07 15:01</td>
<td>ATR</td>
<td>121</td>
<td>06:20 h:m</td>
</tr>
<tr>
<td>1,226</td>
<td>21-MAY-07 15:01</td>
<td>ATR</td>
<td>119</td>
<td>00:45 m:s</td>
</tr>
<tr>
<td>1,225</td>
<td>21-MAY-07 15:00</td>
<td>ATR</td>
<td>120</td>
<td>00:11 m:s</td>
</tr>
<tr>
<td>1,224</td>
<td>21-MAY-07 15:00</td>
<td>ATR</td>
<td>119</td>
<td>00:16 m:s</td>
</tr>
<tr>
<td>1,223</td>
<td>21-MAY-07 15:00</td>
<td>ATR</td>
<td>118</td>
<td>00:07 m:s</td>
</tr>
<tr>
<td>1,222</td>
<td>21-MAY-07 14:59</td>
<td>ATR</td>
<td>119</td>
<td>00:09 m:s</td>
</tr>
</tbody>
</table>
Is a malicious intentional malfunction a risk of real concern?
The Tylenol Scare of 1982

The Tylenol Terrorist

By Rachael Bell

The Tylenol Terrorist: Death in a Bottle

On September 29, 1982, 12-year-old Mary Kelleman of Elk Grove Village, Illinois, woke up at dawn and went into her parents' bedroom. She did not feel well and complained of having a sore throat and a runny nose. To ease her discomfort, her parents gave her one Extra-Strength Tylenol capsule. At 7 a.m. they found Mary on the bathroom floor. She was immediately taken to the hospital where she was later pronounced dead. Doctors initially suspected that Mary died from a stroke, but evidence later pointed to a more sinister diagnosis.

This story was reported by Jonathan Saltzman, John R. Ellement, Milton J. Valencia, and David Abel of the Globe staff. It was written by Saltzman.

CAMBRIDGE -- FBI agents and State Police investigators searched a Cambridge condominium yesterday that is the longtime home of a leading suspect in the 1982 deaths of seven people from cyanide-laced Tylenol capsules in the Chicago area, one of the most notorious unsolved crimes in the last generation.
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
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
Home monitor

Photos: Medtronic; Video: or-live.com
At Home: Wireless + Internet

Home monitor
What’s special about security?
Correctness is easy.

Security is hard.

Photo by Kevin Fu
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]
Our Security Analysis of a Pacemaker + ICD
Method #1: Steal Device Programmer

✦ Insider attack
✦ Thief can reverse engineer, modify...
✦ Risk: get “root” on many implants

Issue: ICD’s trusted computing base is large.

Photo: Medtronic
Why Steal When You Can Build?

✦ Software radio
✦ GNU Radio software, $0
✦ USRP board, $700
✦ Daughterboards, antennas: $100

~10 cm (un-optimized)
Method #2: Eavesdrop Private Info

Implanting physician

Diagnosis

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

... and more
Method #2: Eavesdrop Private Info

In the future:
Sophisticated devices may divulge a lot more data.

Challenge:
Can we add encryption?

Photo:
Medtronic
Method #3: Sniff Vital Signs

Eavesdropping setup

ICD emits reconstructible vital signs

Issue: Vital signs can say plenty.
Methods that Replay Traffic

✦ Ours: “Deaf” (transmit-only) attacks

✦ Caveats: Close range; only one ICD model tested; attacks not optimized; takes many seconds

\[ \sim 10 \text{ cm} \]
Method #4: Drain Energy

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

“Are you awake? Are you awake?”

“Now I am!”
Method #5: Turn Off Therapies

- "Stop detecting fibrillation."
- Device programmer would warn here

**Issue:** Can quietly change device state.

<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><em>AX&gt;B</em></td>
<td><em>AX&gt;B</em></td>
<td><em>AX&gt;B</em></td>
<td>B&gt;A*</td>
<td><em>AX&gt;B</em></td>
<td>B&gt;A*</td>
</tr>
</tbody>
</table>

*Active Can Off*
Method #6: 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.
Defensive Direction: 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

Auth

Go ahead!

ICD
WISPer as Gatekeeper

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

• Session setup

1 cm

Tissue

Modulate ~4 kHz acoustic wave

ICD

Programming head

Key material
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
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.
Future Healthcare Infrastructure

Measurement and Data Collection
- Pacemaker
- Wireless Monitor
- Insulin Pump
- Wireless Reprogrammer
- Heart Rate Monitor
- ID Bracelet

Routing and Storage
- Government Database
- Network Cloud

Processing and Control

“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
Achoo!
Non-Technical Challenges

- Manufacturers beholden only to regulators
  - Remit to regulate safety & effectiveness, but not security & privacy in U.S.
  - Unfinished legislation (U.S. Medical Device Safety Act of 2009)
- No database of ICD reprogrammers
  - Thousands of reprogrammer consoles
  - No way to check if an adversary has one
Medical Device Trends

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

Issue: These trends breed S&P risks that must be kept in check.
Summary of IMD Sec. & Priv.

- **Risks today: Unintentional interference**
  - Threats: Metal detectors, accidents, misidentification
  - Metric of evaluation: Safety and effectiveness
  - Significance: Risks increase with device complexity

- **Coming risks: Intentional interference**
  - Threats from wireless and Internet connectivity
  - Metric of evaluation: Security and privacy
  - Significance: Risks increase with communication complexity
  - Malware: Human-computer-immunodeficiency (HCI) virus?
  - Tough problems: Software updates, remote monitoring, ...
Challenging Technology Landscape!

Auditability

Safety (open access)

Psychological Effects

High Impact

Patient Usability

Security (closed access)

IMD Response Time

Storage Constraints

Battery Life
Wireless + Internet Can Improve Healthcare

But not without fully understanding security and privacy

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

Photos: Medgadget
For More Information

Links on secure-medicine.org and bing:kevin fu

- New England Journal of Medicine
- Neurosurgical Focus
- CACM Inside Risks Column
- Design of Medical Devices Conference
- USENIX Workshop on Power Aware Computing and Systems (HotPower)
- American Heart Association Annual Scientific Sessions
- USENIX Workshop on Hot Topics in Security (HotSec)
- IEEE Symposium on Security and Privacy
- IEEE Pervasive Computing, Special Issue on Implantable Electronics
- Conference on RFID Security