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/

March 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
Risks of Implantable Medical Devices: Just Add Internet + Wireless

Image from www.nasaexplores.com

Sunday, March 29, 2009
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.¹

With information for this article taken from publicly available documents, we present a detailed accident investigation of the factors involved in the overdoses.
Malfunctions

Reprinted from permission

\[ \text{JOURNAL OF PACING AND CLINICAL ELECTROCARDIOLOGY, Volume 25, No. 12, December 2002} \]
\[ \text{Copyright } \text{2002 by Futura Publishing Company, Inc., Armonk, NY 10504-4018} \]

Changing Trends in Pacemaker and Implantable Cardioverter Defibrillator Generator Advisories

WILLIAM H. MAISEL, WILLIAM G. STEVENSON, and LAURENCE 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

Pacemakers and ICD Generator Malfunctions

Analysis of Food and Drug Administration Annual Reports

William H. Maisel, MD, MPH
Meghan Mythen, MD
Ryan D. Zwillman, MD
Thomas P. George, MD, MPH
Oscar H. Tovar, MD
Daniel D. Schacht, MD

Pacemakers and implantable cardioverter-defibrillators (ICDs) are two of the most clinically significant and complex medical devices used in modern cardiology practice. They are essential tools for maintaining patients’ quality of life and are expected to be reliable and safe. However, like all medical devices, pacemakers and ICDs have the potential to malfunction, and such malfunctions can have serious consequences for patients.

Introduction

Pacemaker and implantable cardioverter-defibrillator (ICD) generator recalls and safety alerts (collectively referred to as “advisories”) occur frequently, affecting many patients, and are increasing in number and rate. The US Food and Drug Administration (FDA) is responsible for the safety and oversight of medical devices in the United States. FDA Enforcement Reports are issued to report advisories, including those involving pacemaker and ICD generators. These advisories are issued to notify physicians and patients of the potential for device malfunction. While pacemaker and ICD advisories are common, actual device malfunctions are relatively rare. Nevertheless, advisories increase patient anxiety and may lead to utilization of hospital resources.

A number of advances in device therapy occurred during the 1990s. Pacemakers now routinely provide features to preserve battery life, promote physiological pacing, and provide increased diagnostic capabilities. ICDs continue to shrink in size while maintaining their battery life and high energy capabilities. In addition, they have increasingly sophisticated algorithms for rhythm detection and now have the potential to treat atrial and ventricular arrhythmias.

Pacemaker and ICD generator advisories are most often issued because of potential hardware or software (computer programming) malfunctions. This study was undertaken to determine if advances in device therapy have been accompanied by changes in trends in advisory activity. 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.

Methods

The authors’ methods have been previously described in detail. The number of pacemaker and ICD advisories was determined by reviewing all weekly FDA Enforcement Reports from January 1991 through December 2000 and verifying all recalls and safety alerts with the manufacturer when possible (Tables I and II). Only advisories that occurred when possible (Tables I and II).

©2002 American Medical Association. All rights reserved.

November 14, 2009 16:10

Downloaded from www.jama.com at University of Massachusetts Hadley School on October 8, 2016

William H. Maisel, MD, MPH
Meghan Mythen, MD
Ryan D. Zwillman, MD
Thomas P. George, MD, MPH
Oscar H. Tovar, MD
Daniel D. Schacht, MD

Pacemakers and implantable cardioverter-defibrillators (ICDs) are two of the most clinically significant and complex medical devices used in modern cardiology practice. They are essential tools for maintaining patients’ quality of life and are expected to be reliable and safe. However, like all medical devices, pacemakers and ICDs have the potential to malfunction, and such malfunctions can have serious consequences for patients.

Introduction

Pacemaker and implantable cardioverter-defibrillator (ICD) generator recalls and safety alerts (collectively referred to as “advisories”) occur frequently, affecting many patients, and are increasing in number and rate. The US Food and Drug Administration (FDA) is responsible for the safety and oversight of medical devices in the United States. FDA Enforcement Reports are issued to report advisories, including those involving pacemaker and ICD generators. These advisories are issued to notify physicians and patients of the potential for device malfunction. While pacemaker and ICD advisories are common, actual device malfunctions are relatively rare. Nevertheless, advisories increase patient anxiety and may lead to utilization of hospital resources.

A number of advances in device therapy occurred during the 1990s. Pacemakers now routinely provide features to preserve battery life, promote physiological pacing, and provide increased diagnostic capabilities. ICDs continue to shrink in size while maintaining their battery life and high energy capabilities. In addition, they have increasingly sophisticated algorithms for rhythm detection and now have the potential to treat atrial and ventricular arrhythmias.

Pacemaker and ICD generator advisories are most often issued because of potential hardware or software (computer programming) malfunctions. This study was undertaken to determine if advances in device therapy have been accompanied by changes in trends in advisory activity. 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.

Methods

The authors’ methods have been previously described in detail. The number of pacemaker and ICD advisories was determined by reviewing all weekly FDA Enforcement Reports from January 1991 through December 2000 and verifying all recalls and safety alerts with the manufacturer when possible (Tables I and II). Only advisories that occurred when possible (Tables I and II).
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
## Arrhythmia Logbook Report

### 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>222 Diverted</td>
</tr>
<tr>
<td>1,229</td>
<td>20-JUN-05 12:08</td>
<td>Spont</td>
<td>VF</td>
<td>216 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 Kellerman 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.

truTV crime library
Bad People Do Exist

Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen  03.28.08 | 8:00 PM

Internet grievers 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
First Internal Pacemaker
1926

FDA approved ICD
1978

First Cochlear Implant Surgery
1985

Wireless Blood Glucose Monitor
2006

Networking + Wireless!

Photos from: Medtronic
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
In the Clinic: Wireless
At Home: Wireless + Internet

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

Photo by Kevin Fu
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]
Adversaries
Do Not Play by the Rules
802.11 WiFi Sniper Yagi

Photo: Engadget
Uninvited Radio Suitcases

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

Hospital

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

Sunday, March 29, 2009
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

Photo: Medtronic
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.
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!

BZZZZZZZZZZZZZZZZZZZZZ

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

Modulate ~4 kHz acoustic wave
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.
Going the Distance

Change is in the airwaves
As cellphone firms consider opening networks, startup is ready to carry signal

By Carolyn Y. Johnson, Globe Staff | November 29, 2007

“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!

The Weekly World News: the only reliable journal
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

Sunday, March 29, 2009
For More Information


