Medical Devices: Security & Privacy Concerns

Kevin Fu
Associate Professor
Security & Privacy Research Lab
UMass Amherst Computer Science
http://spqr.cs.umass.edu/
http://secure-medicine.org/

NIST Information Security and Privacy Advisory Board (ISPAB) Meeting
July 14, 2011
Acknowledgments

● CS faculty and physicians
  - Prof. Dina Katabi, MIT Computer Science and AI Lab
  - Prof. Tadayoshi Kohno, University of Washington CSE
  - Dr. Daniel Kramer, BIDMC, Harvard Med School
  - Dr. William Maisel, BIDMC, Harvard Med School (fmr)
  - Dr. Matthew Reynolds, BIDMC, Harvard Med School
  - Prof. Dawn Song, UC Berkeley Computer Science Div.

● Research assistants
  - Shane Clark, Benessa Defend, Tamara Denning, Shyamnath Gollakota, Dan Halperin, Steve Hanna, Haitham Hassanieh, Tom Heydt-Benjamin, Andres Molina-Markham, Will Morgan, Pongsin Poosankam, Ben Ransford, Rolf Rolles, Mastooreh Salajegheh, Quinn Stewart
Disclosures

- Patent pending technology:
  - Low-power flash memory
  - Zero-power security
- Received speaker reimbursements from Symantec
- Received income from Microsoft Research

- This presentation is based on both my own research and the research of others. None of the opinions, findings, or conclusions necessarily reflect the views of my past or present employers.
What are the benefits of **software** in medical devices?
Benefits of Medical Device Software

“Recent reports show improvement over the earlier model mechanical hearts”

Source: NY Times, Thoratec
Without software, many medical treatments could not exist.
Medical Devices 101:
A 10-minute residency for the security & privacy researcher
Networking + Wireless!

- 1926: First Internal Pacemaker
- 1960: FDA approved ICD
- 1985: First Cochlear Implant Surgery
- 2006: Wireless Blood Glucose Monitor

Photos from: Medtronic

Pacemakers: Regulate heartbeat
Pacemakers: Regulate heartbeat

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

< Energy for pacing!
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...
An Investigation of the Therac-25 Accidents

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

```
...the machine could not possibly over treat a patient and ... no similar complaints were submitted...”
[Leveson & Turner, 1993]
```
How Much SW in Medical Devices?

- 1983-1997
  - 6% of all recalls attributed to SW
- 1999-2005
  - **Almost doubled**: 11.3% of all recalls attributed to SW
  - 49% of all recalled devices relied on software (up from 24%)
- 1991-2000
  - **Doubled**: # of pacemakers and ICDs recalled because of SW
- 2006
  - Milestone: Over half of medical devices now involve software
- 2002-2010
  - 537+ recalls of SW-based devices affecting 1,527,311+ devices

(1) Software breeds overconfidence, (2) is not thoroughly testable, but (3) is flooding into medical devices.
FDA Center for Devices and Radiological Health

Regulatory pathways

Pre-market approval

It's complicated.
http://www.iom.edu/Activities/PublicHealth/510KProcess/2010-MAR-01.aspx
Medical Device Security & Privacy Concerns

Prof. Kevin Fu, UMass Amherst Computer Science

FDA Center for Devices and Radiological Health

Regulatory pathways

Pre-market notification

[510(k) clearance]

It’s complicated.

http://www.iom.edu/Activities/PublicHealth/510KProcess/2010-MAR-01.aspx
510(k) Substantial Equivalence

- “One of the interesting classes is radiation equipment...Even the software, which I wonder where they got the first predicate for software.”

-David Feigal
Fmr. Director, FDA Center for Devices and Radiological Health (CDRH)

[Institute of Medicine Meeting 2, June 2010: Public Health Effectiveness of the FDA 510(k) Clearance Process]
Contributing factors for S&P risks in medical devices
Specification of Requirements

- Risk not unique to medical devices, just ignored

```
```
Perhaps the most striking [difference] is the almost complete lack of regard, in the medical-device software domain, for the specification of requirements."

[NITRD Report on High-Confidence Medical Devices: Cyber-Physical Systems for 21st Century Health Care, Feb 2009]
Implementation Errors

BAXTER HEALTHCARE PTE. LTD. COLLEAGUE 3 CXE VOLUMETRICINFUSION PUMP 80FRN

Catalog Number 2M9163
Event Date 07/30/2007
Event Type Death Patient Outcome Death;
Manufacturer Narrative

Evaluation of the device indicates the reported condition of fail code 16:310 was confirmed but could not be duplicated during service. The pump passed power on self-test on ac. The front bezel was opened & a visual inspection of all wires, harness connections, and user interface module printed circuit board was performed. The master and slave software programmable read only memory were found inserted correctly. No visual damage was found. The batteries had 10 charge/discharge cycles & 0 discharges below alarm threshold. The pump passed the keypad test. The device has been returned to baxter technical service for repair. The buffer overflow issue resulting in failure code 16:310 found in the software version utilized in colleague infusion pumps has been found to be repeatable in a specific clinical situation, and has resulted in multiple patient adverse events over a short period of time following initiation of deployment of this software version in the us. The issue is caused by an overflow in the memory buffer that feeds the main processor. The c2006 software version includes several changes that have increase the utilization level of this buffer, resulting in a higher probability of overflow. For the
Implementation Errors

- Infusion pump: Underdosed patient experienced
  - increased intracranial pressure
  - followed by brain death
- Factor: Buffer overflow shut down infusion pump
  - Failure difficult to reproduce during service
  - Software upgrade tickled the coding error
- Caused failure of drug infusion
  - propofol (sedation/anesthetic)
  - levophed (blood pressure)
  - insulin
Emerging issues for information security and privacy
Managerial issues: Diffusion of responsibility
Dirty Secrets: SW Maintenance

Firefox 1.5.0.2 Ready to Install

Firefox has just completed downloading an important update. This update must now be restarted so that the update can be installed.

Update: Firefox 1.5.0.2

Click Restart Firefox Now to close all Firefox windows and install the update.

Click Later to continue without restarting. The update will be installed the next time you start Firefox.
Software Update Woes

- Health Information Technology (HIT) devices globally rendered unavailable
- Cause: Automated software update went haywire
- Numerous hospitals were affected April 21, 2010
  - Rhode Island: a third of the hospitals were forced to postpone elective surgeries and stop treating patients without traumas in emergency rooms."
  - Upstate University Hospital in New York: 2,500 of the 6,000 computers were affected.

The Vancouver Sun

Web-security giant McAfee paralyzes computers at hospitals, universities worldwide with update
Users are Helpless

Before you post it would be wise to ask why the computer needs to be downgraded. I am setting up a medical imaging facility and I am trying to do the same thing as well. The PACS system we are integrating with is only compatible with SP2. I order 6 new Dell workstations and they came preloaded with SP3. There are "actual versions" of programs out there that require SP2. For instance, the $250,000 Kodak suite I am installing. Plus a $30,000/yr service contract. This holds true for the majority of the hospitals which have PACS systems.

However, if what you are saying is true then I found something useful within your post. You stated "if you installed XP with integrated sp3, it is not possible to downgrade sp3 to sp2," is this true? Do you have any supporting documentation as this would be very helpful so that I can provide Dell with a reason why I need to order downgraded XP discs.
Users are Helpless

"As can be seen on the product page for Windows XP, support for SP2 ends tomorrow, while the majority of Windows XP users still haven't upgraded to SP3. This could open up millions of users/businesses to exploitation, since security updates for SP2 will stop coming in while security fixes to SP3 may clue hackers in to vulnerabilities."
Security falls outside the purview of the Food and Drug Administration, [FDA spokeswoman Karen Riley] said, unless mandated measures taken to protect data end up causing problems.

... “We don’t weigh in on security per se, but on measures like encryption that might affect or could have an impact on product safety and effectiveness, we might look at it.”

Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility

Issued
November 4, 2009

For
Medical device manufacturers, hospitals, medical device user facilities, healthcare IT and procurement staff, medical device users, biomedical engineers

Issue
FDA wants to remind you that cybersecurity for medical devices and their associated communication networks is a shared responsibility between medical device manufacturers and medical device user facilities. The proper maintenance of cybersecurity for medical devices and hospital networks is vitally important to public health because it ensures the integrity of the computer networks that support medical devices.

FDA is aware of misinterpretation of the regulations for the cybersecurity of medical devices that are connected to computer networks. FDA’s interpretation of the regulations can be found in the 2005 guidance for industry and its accompanying information for healthcare organizations.
Managerial issues: Diffusion of responsibility

Who’s covered when Secure Health IT hits the fan?
Physical safeguard issues
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.

[Source: truTV crime library]
(a) General. The Food and Drug Administration has the authority under the Federal Food, Drug, and Cosmetic Act (the act) to establish a uniform national requirement for tamper-evident packaging of OTC drug products that will improve the security of OTC drug packaging.
Administrative issues:

Insufficient software/security expertise available to FDA
Technical issues
Achoo!

The Weekly World News: the only reliable journal
Viruses on Radiology Equipment?

“over 122 medical devices have been compromised by malware over the last 14 months”

Statement of The Honorable Roger W. Baker
[House Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations, Hearing on Assessing Information Security at the U.S. Department of Veterans Affairs]

**MAUDE Adverse Event Report**

FUJIFILM MEDICAL SYSTEM USA, INC. IIP COMPUTED RADIOGRAPHY READER AND WORKSTATION

**Model Number IIP**
**Event Date** 06/13/2009
**Event Type** Malfunction
**Event Description**

Delay in treatment related to equipment failure on 4 patients. The images were frozen on the list and would not transmit on the fuji reader equipment. The system was rebooted without change. A few hours later the system was again shut down and rebooted and the images then did transfer. Images were repeated on equipment in another department. The next day the same issue occurred with 4 more patients and the system was shut down to await evaluation by the manufacturer. This problem was traced to a computer virus (conficker) which was found to be affecting 6 fuji cr units. The hospital's imaging service engineer applied a microsoft patch (ms08-067) to the 6 fuji units to prevent the virus from re-infecting the systems. Subsequent to this problem one of the fuji units experienced a shutdown, which was repaired by replacement of a defective power supply. This failure is not thought to be related to the virus issue.
How significant are intentional, malicious malfunctions in software?
Information Assurance or Bliss?

“NOT ONE SINGLE CASE THROAT
“To our knowledge there has not been a single reported incident of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide,” a Medtronic spokesman, Robert Clark

[B. Feder, “A Heart Device Is Found Vulnerable to Hacker Attacks” NY Times, March 12, 2008]
“To our knowledge there has not been a single reported incident of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide,” a Medtronic spokesman, Robert Clark

[B. Feder, “A Heart Device Is Found Vulnerable to Hacker Attacks” NY Times, March 12, 2008]

Since January 2009, the VA has detected that 181 medical devices have been infected with a virus, but "none has resulted in any major harm to our patients, to our knowledge," Ledsome says.

[VA’s acting director of field security operations]

To our knowledge there has not been a single reported incident of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide,” a Medtronic spokesman, Robert Clark [B. Feder, “A Heart Device Is Found Vulnerable to Hacker Attacks” NY Times, March 12, 2008]

Since January 2009, the VA has detected that 181 medical devices have been infected with a virus, but "none has resulted in any major harm to our patients, to our knowledge," Ledsome says. [VA’s acting director of field security operations] [H. Anderson, HealthcareInfoSecurity.com, June 21, 2011]

St. Jude Medical, the third major defibrillator company, said it used “proprietary techniques” to protect the security of its implants and had not heard of any unauthorized or illegal manipulation of them. [B. Feder, “A Heart Device Is Found Vulnerable to Hacker Attacks” NY Times, March 12, 2008]
“To our knowledge there has not been a single reported incident of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide,” a Medtronic spokesman, Robert Clark
[B. Feder, “A Heart Device Is Found Vulnerable to Hacker Attacks” NY Times, March 12, 2008]

Since January 2009, the VA has detected that 181 medical devices have been infected with a virus, but "none has resulted in any major harm to our patients, to our knowledge," Ledsome says.
[VA’s acting director of field security operations]

Boston Scientific said it used encryption in its defibrillators, and doubted its devices could be hacked.
[K. Winsstein, “Heart-Device Hacking Risks Seen” WSJ, March 12, 2008]
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.
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
Implantation Scenario

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

Photos: Medtronic; Video: or-live.com
Privacy??

Implanting physician

Diagnosis

Also:
Device state
Patient name
Date of birth
Make & model
Serial no.
... and more
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
Wirelessly Induce Fatal Heart Rhythm

ICD software allows wireless induction of ventricular fibrillation

[Halperin et al., IEEE Symposium on Security & Privacy 2008]
Technical issues
Vulnerabilities are in plain sight.
When will risk become a tangible threat?
Ways Forward?
Thoughts to Consider

- S&P standards for all relevant phases of product lifecycle
  - holistic system-level properties, not just components
  - reporting and collection of statistics about S&P issues
  - informed consent of patients
  - not causing unwarranted anxiety

- Interdisciplinary educational programs
  - Increase number of people trained in medical devices and S&P

- Emergency response plans for rare, catastrophic events
  - Stuxnet meets implantable medical device or hospital ward?
  - Zero-days addressed by in-clinic appointment? Not effective.

- Open research platforms for innovation
Strategic Healthcare Advanced Research Projects (SHARP) is sponsored by the Office of the National Coordinator of the United States Department of Health and Human Services.

Began in April 2010 and lasts 4 years

**SHARP research areas:**
- Security and Privacy (SHARPS)
- Patient-Centered Cognitive Support
- Health Applications and Networking Platforms
- Secondary Use of Health Records

[www.sharps.org](http://www.sharps.org)

**SHARPS Rationale**
- Cyber security and privacy (S&P) risks are a significant barrier to the deployment and meaningful use of health information technology.
- Many key challenges in these areas can be addressed with emerging and new technologies in S&P.
- SHARPS teams computer scientists who specialize in S&P with healthcare specialists interested in S&P for HIT. The aim is to produce new levels of communication and tech transfer.

**SHARPS Environments**
- **EHR** – Electronic Health Records, managing patient records within an enterprise
- **HIE** – Health Information Exchange, sharing records between enterprises or between an enterprise and a patient in the form of a Personal Health Record
- **TEL** – Telemedicine, monitoring remotely, communicating with multimedia, and controlling implanted medical devices

**SHARPS Participating Institutions**
- University of Illinois at Urbana-Champaign
- Carnegie Mellon University
- Dartmouth College
- Harvard University and Beth Israel Deaconess Medical Center
- Johns Hopkins University and Children's Medical And Surgical Center
- New York University
- Northwestern University and Memorial Hospital
- Stanford University
- University of California, Berkeley
- University of Massachusetts Amherst
- University of Washington
- Vanderbilt University

http://HealthIT.HHS.gov/sharp
Medical Device Security & Privacy Concerns • Prof. Kevin Fu, UMass Amherst Computer Science
How Might NIST Help?

- Coordinate S&P standards for medical devices
  - DHHS FDA burdened with its remit for safety and effectiveness
  - HIPAA within DHSS OCR is mostly post-market (reminder: P = portability, not privacy)
  - Entities with most ability to address S&P risks have least incentive (manufacturers, regulators)
  - Entities with most incentive to address S&P risks have least ability (patients, health care professionals)

- Help remove roadblocks to medical device S&P research
  - Researchers accepting resources from industry, branded as biased
  - But S&P innovation unrealistic without industrial participation
  - Contracts with manufacturers lead to S&P vulnerability dark matter
    - Secret hospital contracts prevent legitimate S&P research
    - Reinforces “no evidence” claims and promotes “everything’s fine” mindset
Wireless + Internet Can Improve Healthcare

But not without fully understanding trustworthy computing

Insulin pump  Artificial pancreas  Neurostimulators

Artificial vision  Obesity control  Programmable Vasectomy

Photos: Medgadget
Further Reading

- Kevin Fu. Software issues for the medical device approval process. Statement to the Special Committee on Aging, United States Senate, Hearing on a delicate balance: FDA and the reform of the medical device approval process, Wednesday, April 13, 2011.

http://spqr.cs.umass.edu/publications.php