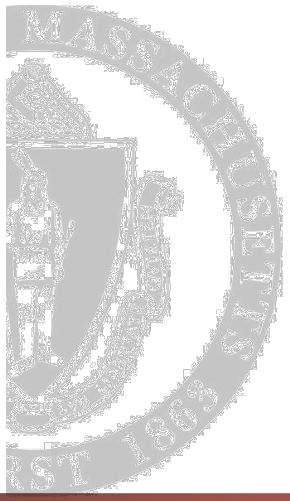
Trustworthy Medical Device Software



Kevin Fu

Associate Professor
Security & Privacy Research Lab
UMass Amherst Computer Science

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

MIT CSAIL seminar
November 2011

The Next Hour...

- Modern complexity of software-controlled medical devices
- Policies that were not designed for big d(technology)/dt
- A bit of technology

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.
- Graduate 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

- Support from NSF, HHS, DHS, IOM, Microsoft Research, Symantec, McAfee
- Visiting scientist at FDA
- Board member of NIST ISPAB
- Patent pending technology:
  - Low-power flash memory
  - Zero-power security

Hat: zazzle.com

- 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.
- This publication was made possible in part by Grant Number HHS 90TR0003/01. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the HHS. This material is supported by the NSF under CNS-0831244. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

What are the benefits of **software** in medical devices?

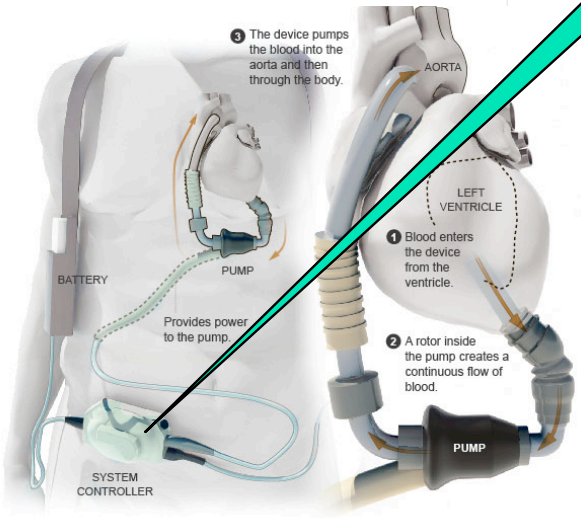
Benefits of Medical Device Software

DOCTOR'S WORLD

A New Pumping Device Brings Hope for Cheney

By LAWRENCE K. ALTMAN, M.D.
Published: July 19, 2010

The New York Times **July 19, 2010**



Computer

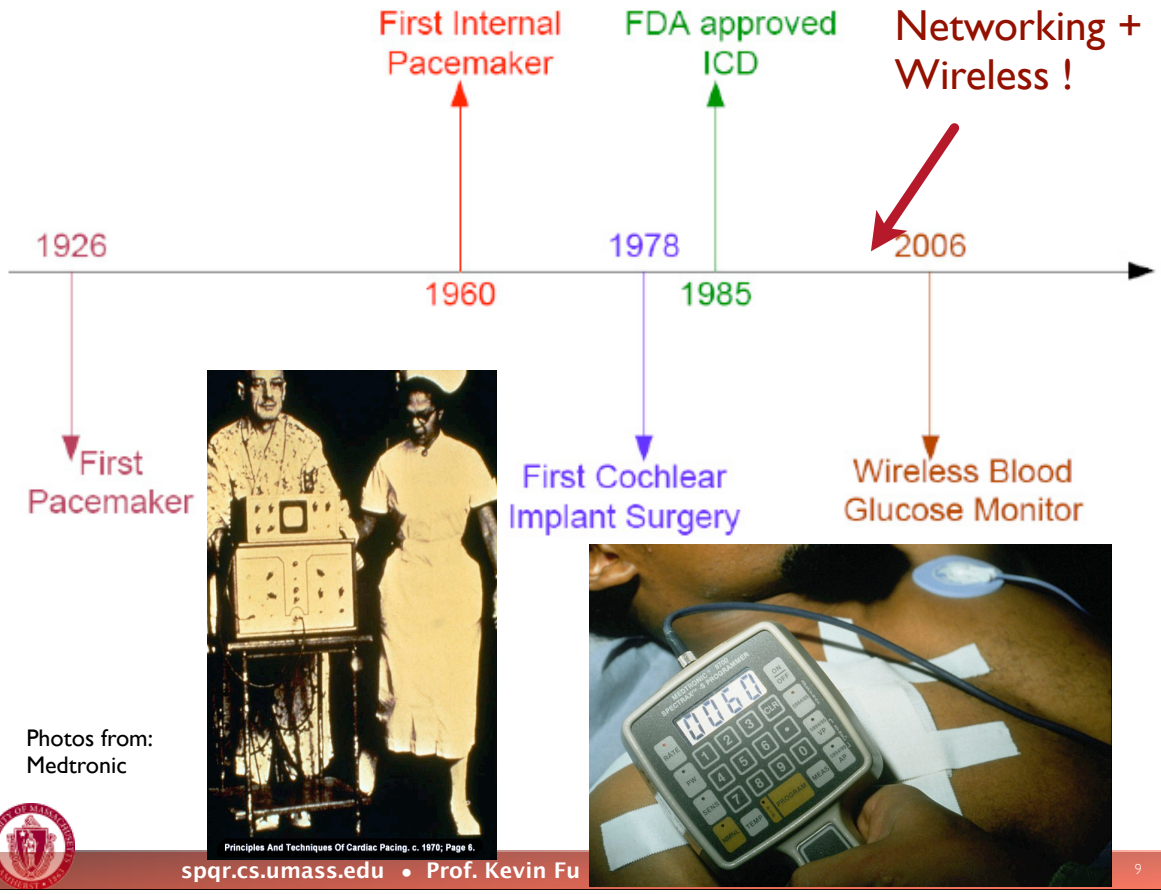
"Recent reports show improvement over the earlier model mechanical hearts"

Source: NY Times, Thoratec

Without software,
many medical treatments
could not exist.

Medical Devices 101:

A 10-minute residency for the computer scientist



9

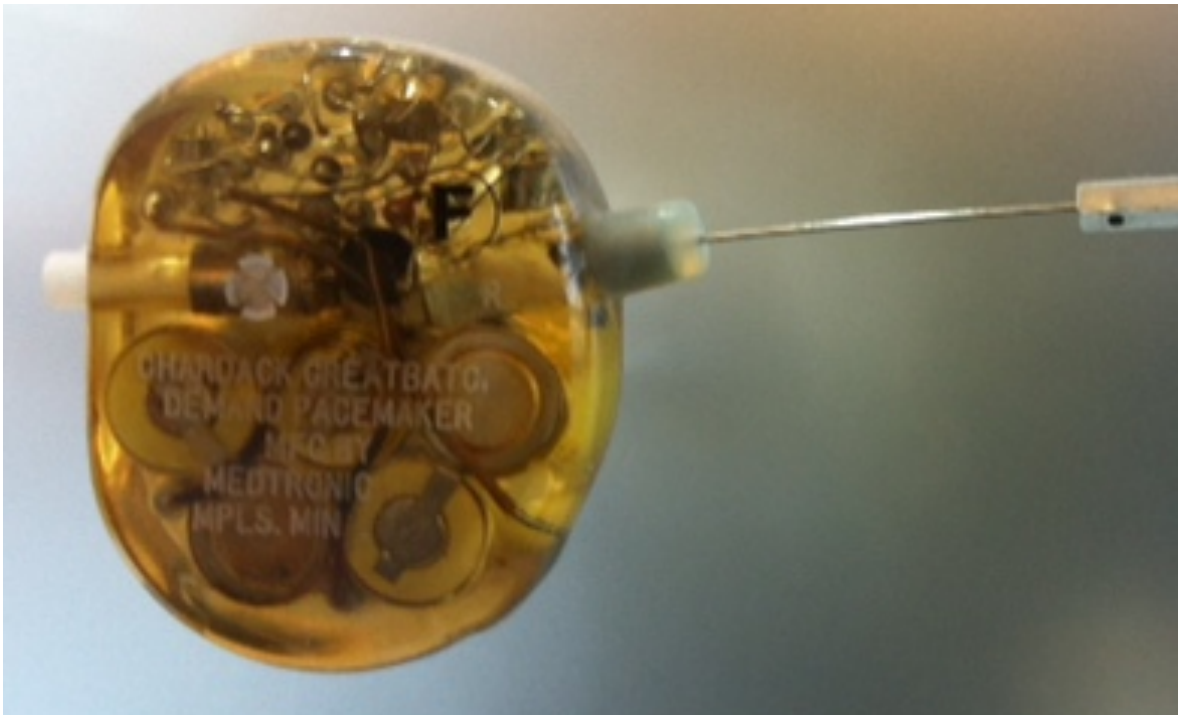
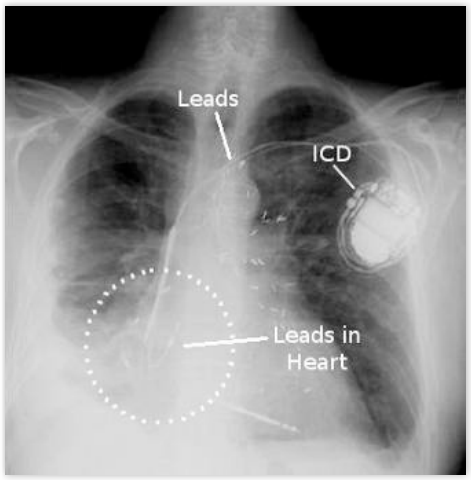


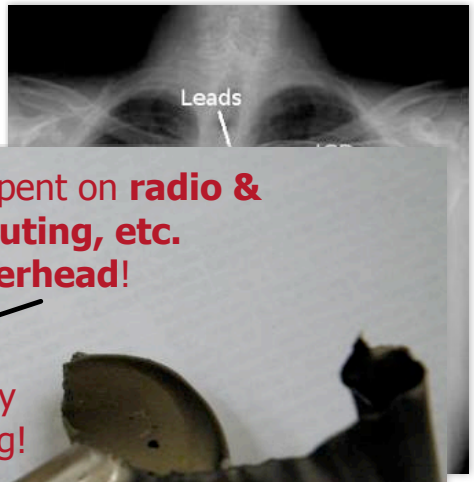
Photo by Kevin Fu @ Medtronic museum

10

Pacemakers: Regulate heartbeat



Pacemakers: Regulate heartbeat



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

< Energy for pacing!

Overconfidence in Software

IEEE Computer 1993

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

Overconfidence in Software

IEEE Computer 1993

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]

spqr.cs.umass.edu • Prof. Kevin Fu • UMass Amherst Computer Science 12

12

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

[Sources: Bliznakov et al. 2006, Faris 2006, Maisel et al. 2002, Wallace & Kuhn 2001, Computer history museum, eurogramer.net, wikipedia, businesspundit.com, imdb.com, coverbrowser.com, thefilmtalk.com]

Why Is Software Different?

- Discrete (not continuous)
  - 0.9999 inch nail vs. 1.0001 inch nail: Small error usually OK
  - Single error in software: 20mL versus 200mL infusion
  - Generally no analogous notion of safety margin
- Cannot be tested thoroughly

(radiation therapy)

``'...there is **not enough time** ... **to check** the behavior of a complicated device to **every** possible, conceivable kind of **input**,' said Dr. Williamson...."
[Walt Bogdanich, NY Times, 1/26/2010]

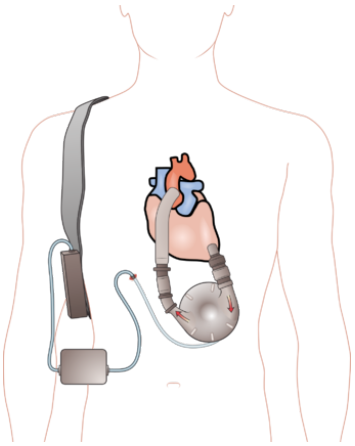
[Source: Parnas 1985, Pfleeger et al. 2001]

(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



Credit: Madhero88

It's complicated.
http://www.iom.edu/Activities/PublicHealth/510KProcess/2010-MAR-01.aspx

FDA Center for Devices and Radiological Health

Regulatory pathways

Pre-market notification [510(k) clearance]

Credit: Nemo's great uncle

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**."

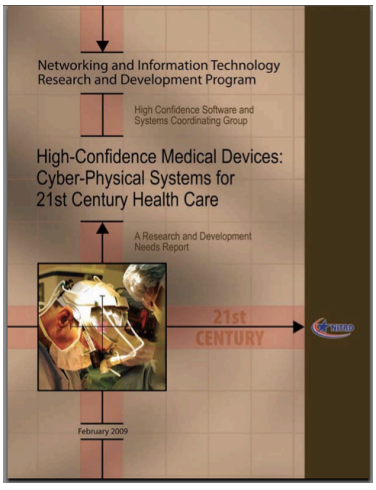
-David Feigal
Fmr. Director, FDA Center for Devices and Radiological Health (CDRH)
[Institute of Medicine Meeting 2, June 2010:
Public Health Effectiveness of the FDA 510(k) Clearance Process]

Recurring themes in **un**trustworthy 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]

Symptom: Implementation Errors

U.S. Food and Drug Administration

A-Z Index | Search

Home | Food | Drugs | Medical Devices | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Radiation-Emitting Products | Tobacco Product

FDA Home > Medical Devices > Databases

MAUDE Adverse Event Report

CDRH SuperSearch

510(k) | Registration & Listing | Adverse Events | Recalls | PMA | Classification | Standards
CFR Title 21 | Radiation-Emitting Products | X-Ray Assembler | Medsun Reports | CLIA

BAXTER HEALTHCARE PTE. LTD. COLLEAGUE 3 CXE VOLUMETRICINFUSION PUMP 80FRN Back to Search Results

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 version of software utilized in pumps outside of the us (vb), including the one involved in this complaint from another country, the buffer utilization level is significantly lower. The complaint rate for the vb software is

Symptom: 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

U.S. Food and Drug Administration

A-Z Index | Search

Home | Food | Drugs | Medical Devices | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Radiation-Emitting Products | Tobacco Products

FDA Home > Medical Devices > Databases

MAUDE Adverse Event Report

CDRH SuperSearch

510(k) | Registration & Listing | Adverse Events | Recalls | PMA | Classification | Standards
CFR Title 21 | Radiation-Emitting Products | X-Ray Assembler | Medsun Reports | CLIA

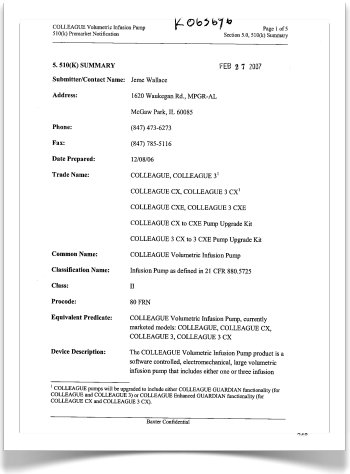
BAXTER HEALTHCARE PTE. LTD. COLLEAGUE 3 CXE VOLUMETRICINFUSION PUMP 80FRN Back to Search Results

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 version of software utilized in pumps outside of the us (vb), including the one involved in this complaint from another country, the buffer utilization level is significantly lower. The complaint rate for the vb software is approximately 1 complaint per million infusions (cpmi) as compared to a complaint rate of 163 cpmi on the c2006 software. Based on these differences, colleague infusion pumps with the vb software are not considered equivalent to those with the c2006 software.

Sample 510(k) Summary

- Where is software mentioned?
  - "Non-clinical testing associated with compliance and safety, **software**, and intended use claims were performed according to the Baxter Healthcare Corporation Product Development Process."
  - "Human Factors evaluation and use scenario testing was performed under simulated use and environmental conditions utilizing clinical care personnel from hospital environments."
  - "All tests successfully passed the acceptance criteria."



K062678

Page 1 of 5

COLLEAGUE Volumetric Infusion Pump
510(k) Premarket Notification

Section 5.0, 510(k) Summary

5. 510(K) SUMMARY

FEB 27 2007

Submitter/Contact Name:	Jesse Wallace
Address:	1620 Waukegan Rd., MPGR-AL McGaw Park, IL 60085
Phone:	(847) 473-6273
Fax:	(847) 785-5116
Date Prepared:	12/08/06
Trade Name:	COLLEAGUE, COLLEAGUE 3[1] COLLEAGUE CX, COLLEAGUE 3 CX[1] COLLEAGUE CXE, COLLEAGUE 3 CXE COLLEAGUE CX to CXE Pump Upgrade Kit COLLEAGUE 3 CX to 3 CXE Pump Upgrade Kit
Common Name:	COLLEAGUE Volumetric Infusion Pump
Classification Name:	Infusion Pump as defined in 21 CFR 880.5725
Class:	II
Procode:	80 FRN
Equivalent Predicate:	COLLEAGUE Volumetric Infusion Pump, currently marketed models: COLLEAGUE, COLLEAGUE CX, COLLEAGUE 3, COLLEAGUE 3 CX
Device Description:	The COLLEAGUE Volumetric Infusion Pump product is a software controlled, electromechanical, large volumetric infusion pump that includes either one or three infusion

[1] COLLEAGUE pumps will be upgraded to include either COLLEAGUE GUARDIAN functionality (for COLLEAGUE and COLLEAGUE 3) or COLLEAGUE Enhanced GUARDIAN functionality (for COLLEAGUE CX and COLLEAGUE 3 CX).

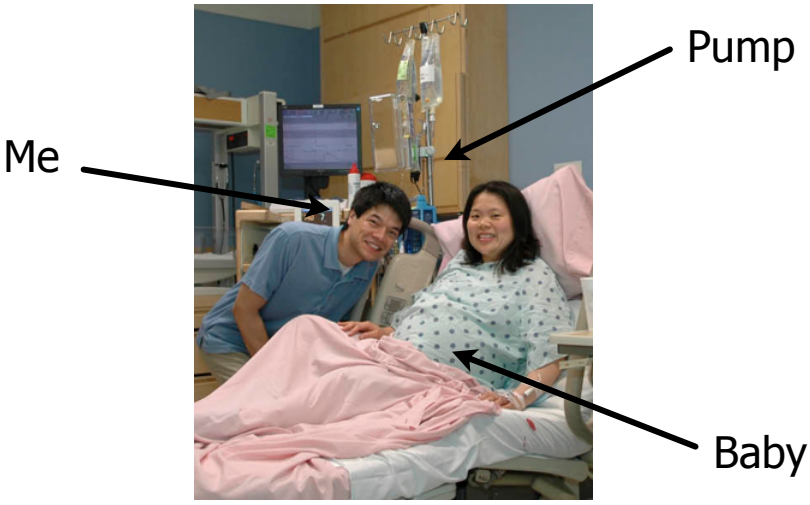
Baxter Confidential

- **Requirements specification? Systems engineering? Modern software engineering? Software validation? Formal methods? Type safe languages? Static analysis?**

What about human factors and software?

Infusion Pump UI and Software

- Used safely and effectively every day, but...
- Linked to **500+ deaths** and 56,000 adverse events



[US Recall News]

Pump+SW Problems=Deadly Cocktail

- "... 710 patient deaths linked to problems with the devices ... either because a hospital worker **entered incorrect dosage** data into a pump or because the device's **software malfunctioned**."

[Barry Meier, NY Times, 4/23/2010]

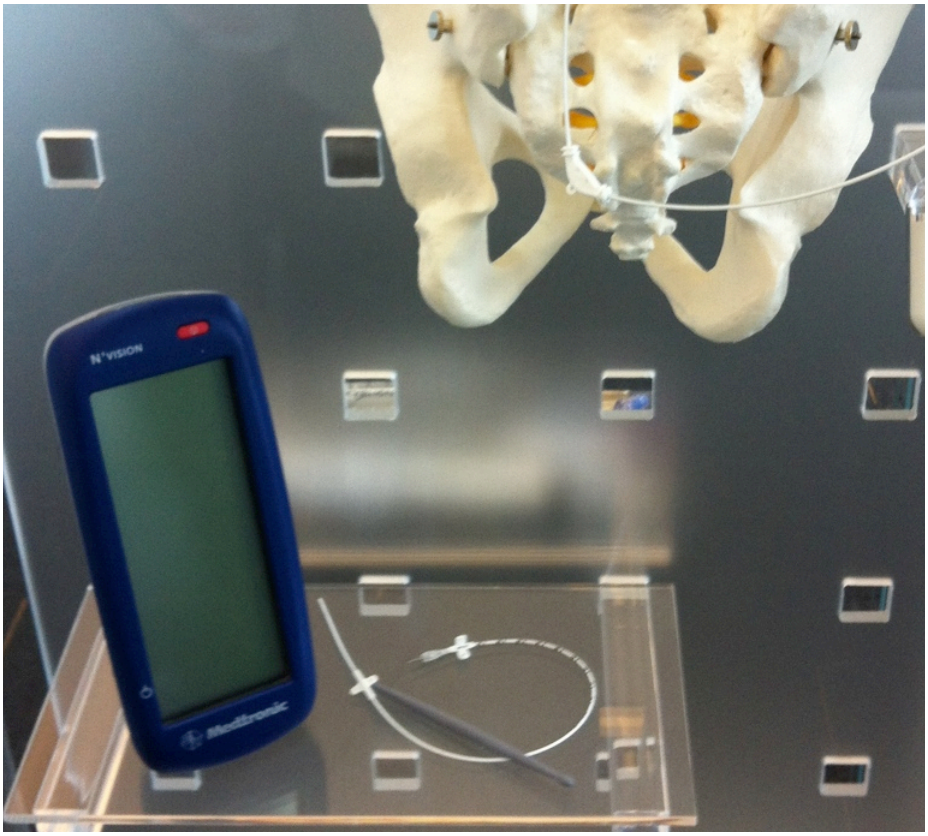
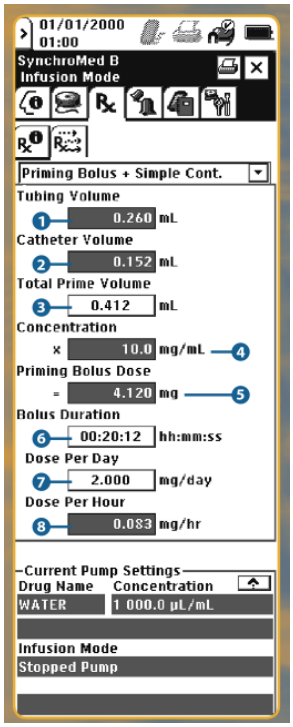


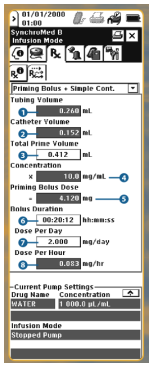
Photo by Kevin Fu @ Medtronic museum

User Interface: Timing is Everything



[Photos: Medtronic]

User Interface: Timing is Everything



HCP: "discovered a bolus was given in 20 **min** versus the intended 20 **hrs**"

FDA: "...software... did not provide a label for the hours/minutes/seconds fields; the new software has this labeling."

[Photos: Medtronic]

Human Factors: User Interface

``There is nothing on the machine that tells the technologist that they've dialed in a badly incorrect radiation exposure."

-Dr. James Thrall
Chairman of the American College of Radiology
Professor of Radiology, Harvard Medical School
[Source: Walt Bogdanich & Rebecca R. Ruiz, NY Times, 2/9/2010]

[Creative Commons license, IndyDina with Mr. Wonderful's photostream]

[Photo: Jerome-Parks family and Walt Bogdanich, NY Times, 1/23/2010]

[US Recall News]

Better analysis of human factors in SW could prevent injury and death.

Wireless medical devices: great benefits, but subtle, inconvenient risks

Alert: Patient Expired. Yesterday.

- Overconfidence in wireless technology
- Cardiac monitor did not transmit until 10 hours later
- Wireless: Great benefits, subtle risks

BRAEMAR BRAEMER AF 920-WIRELESS EVOLUTION Back to Search Results

Event Date 08/22/2009
Event Type Death **Patient Outcome** Death;
Event Description

The pt, was wearing a cardiac event monitor provided by ecardio diagnostics. The monitor transmitted two recordings in 2009. The first at 1641 which was time/date stamped at 1030. The second recording which transmitted at 1644 which time-date stamped at 1630 am. The recordings did not transmit until 10 hours after the event was recorded and then transmitted in reverse order -according to the time-date stamp info. This is a wireless monitor and should have transmitted at the time of the recording. The pt expired. Dates of use: 30 days. Event abated after use stopped or dose reduced? no.

Wireless: Pump Batteries Deplete?

- Network "heartbeat" causes device to consume power?
- Wireless: Great benefits, subtle risks

HOSPIRA HOSPIRA PLUM A PLUS INFUSION PUMP Back to Search Results

Model Number PLUM A PLUS
Event Date 05/06/2008
Event Type No Answer Provided
Event Description

Continued complaints of battery failures on an inventory of 523 pumps even though batteries have been replaced in as litle as one month. The pump has normal warnings and shutdown processes when battery depletion is detected. There has been a continued discussion with the company. Their response has been slow or not at all. They have indicated we are not using their batteries and not fully recharging the pumps between use as the reason for failure, however we have 255 pumps in the same type of environment we are using without the wireless communications that have normal battery failure life. (1-5 years)this causes a delay in treatment and excessive full time employee time finding a replacement. We believe the pump continues to send a "heartbeat" to the network server even when turned off which causes premature depletion. The company has not responded to that statement officially. ========== health professional's impression==========there are repeated battery failures with this product which uses wireless downloads and communication. We believe it is because of the extra current used for communications causing a pre-mature battery failure/ depletion of the battery.

Search Alerts/Recalls

Wireless Makes Everything Better?

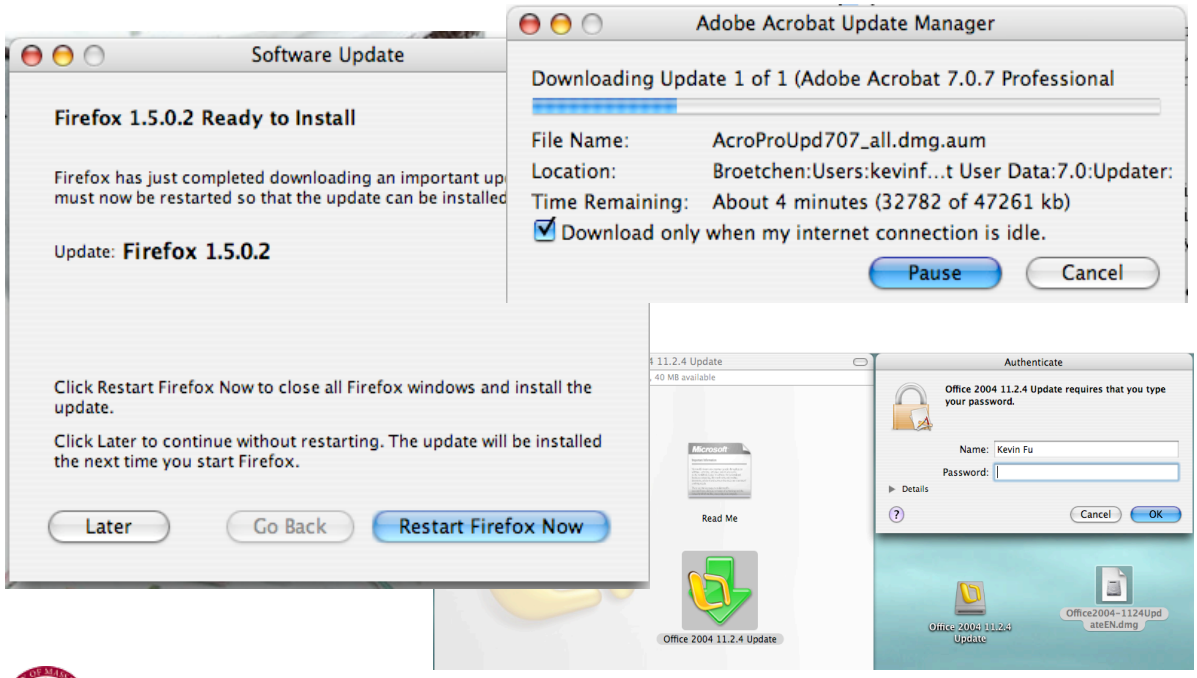
[Photos: http://uncyclopedia.wikia.com/wiki/Bacon & Cisco & Sysco]

Emerging issues for information security and privacy:

managerial, physical safeguards, administrative, technical

Managerial issues:
Diffusion of responsibility

Dirty Secrets: SW Maintenance



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

Losing Patience with a Computer

- Endlessly rebooting machine caused distraction
- HCPs did not notice cardiac infarction in patient
- Electronic Health Records carry similar risks of distraction

PHILIPS MEDICAL SYSTEMS ALLURA XPER FD10 IZI (ANGIOGRAPHIC X-RAY SYSTEM) Back to Search Results

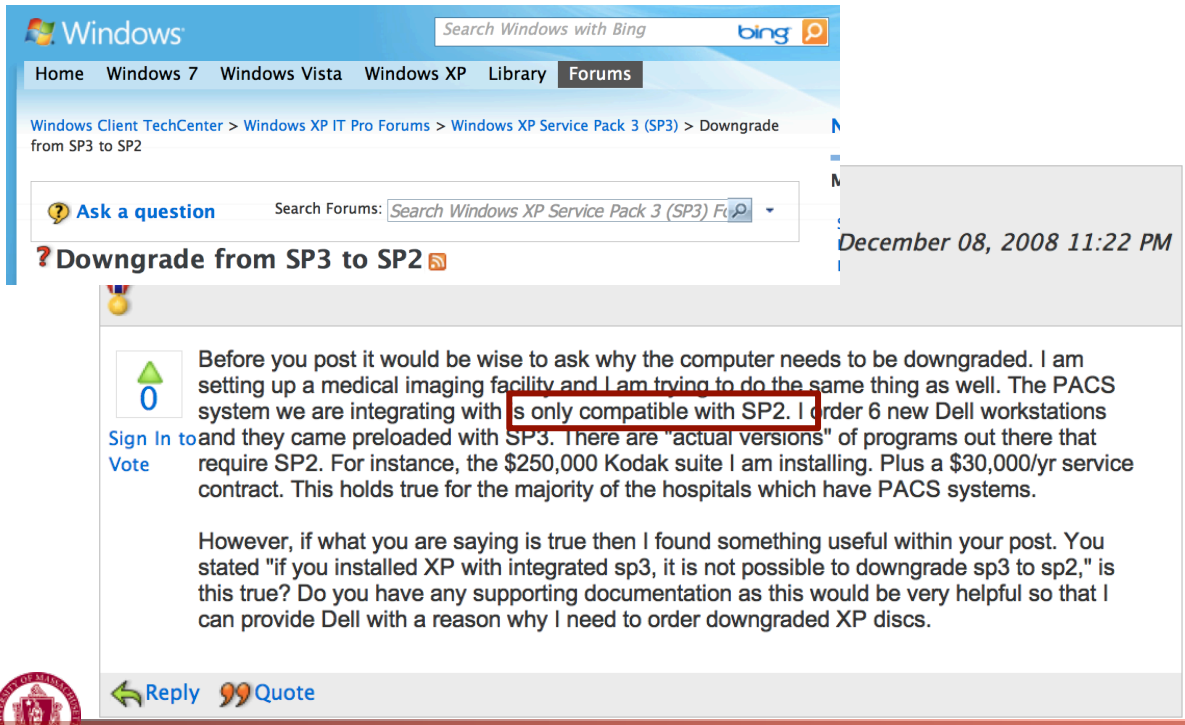
Model Number 722003
Device Problem Computer failure
Event Date 08/11/2009
Event Type Death **Patient Outcome** Death;
Event Description

This report is being filed upon notification from our x-ray manufacturer in other country, to submit this event. Problem: the pt was having an x-ray procedure. During the procedure, the system locked up with a message stating there was insufficient disk space to run windows. The system took several reboots to make it operational. The pt was experiencing a cardiac infarct during the failure.

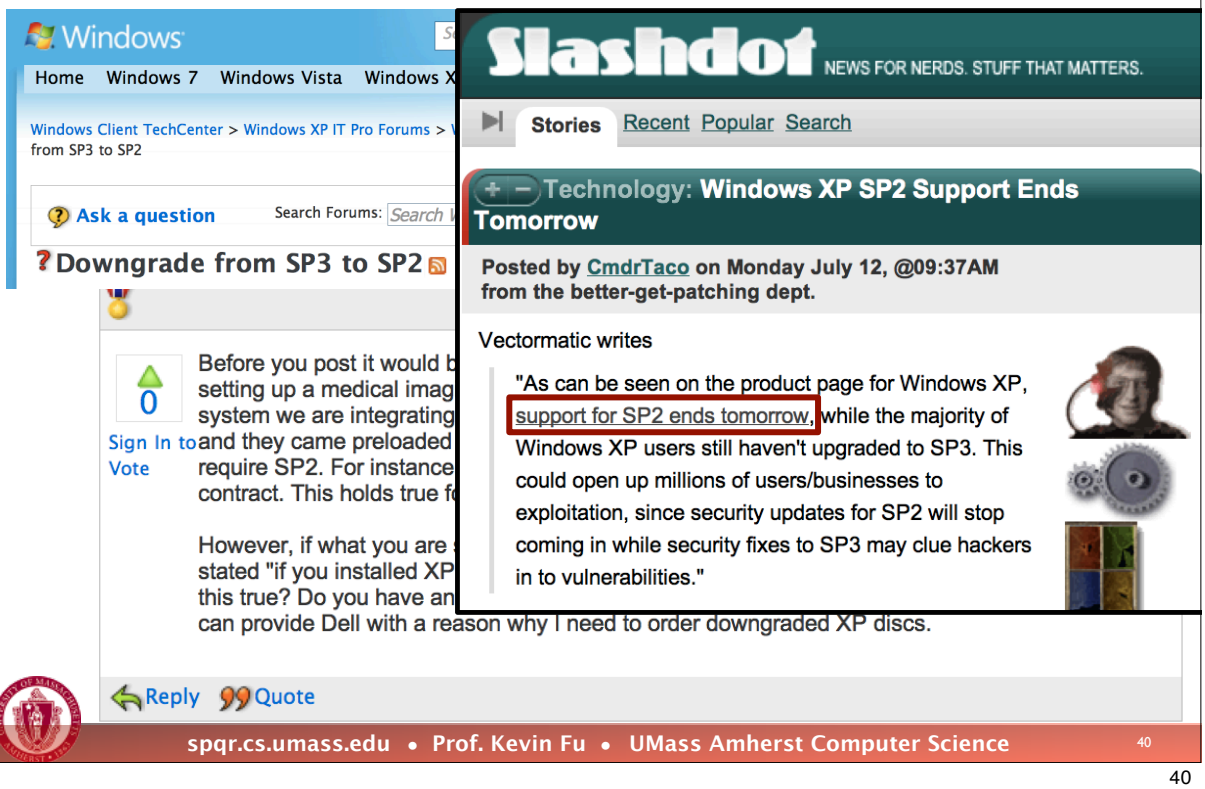
Manufacturer Narrative

Eval results and conclusions: the investigation is still ongoing on this event. When the investigation is completed, a follow-up report will be sent to the fda.

Users are Helpless



Users are Helpless



Operating System: HCPs Problem

- Radiological computers infected with computer virus
- Report of potential to cause harm or death
- Conclusion: Not our problem

PHILIPS MEDICAL SYSTEMS XCELERA LLZ (SYSTEM, IMAGING PROCESSING, RADIOLOGICAL) Back to Search Results

Model Number 830032
Event Date 01/04/2009
Event Type Other
Event Description

The report is being filed upon notification from our info technology manufacturer in (b)(4) to submit this event. In a retrospective review of philips complaints/corrective actions, this issue is now being reported as a mdr. Several computers in the hospital (b)(6)got infected with a computer virus. As a result of this infection, the software (xcelera) could not be used from time to time. This hospital felt that this could have caused a death or serious health deterioration.

Manufacturer Narrative

Conclusions: the responsibility for the maintenance of the it equipment (which requires amongst others the installation of the microsoft office security patches of virus scanners) lies with the customer. Philips medical systems is not responsible for the installation or maintenance of antivirus software or for the integrity of the xcelera system infected with a computer virus. Appropriate network firewalls and virus protection is not the responsibility of philips. Although philips understands the customer's point of view, philips believes that the medical device was not a contributor to the worm attack. There were no reported injuries. Philips is only reporting this matter due to the hospital's safety reported claims.

Not It! Olly Olly Oxen Free!

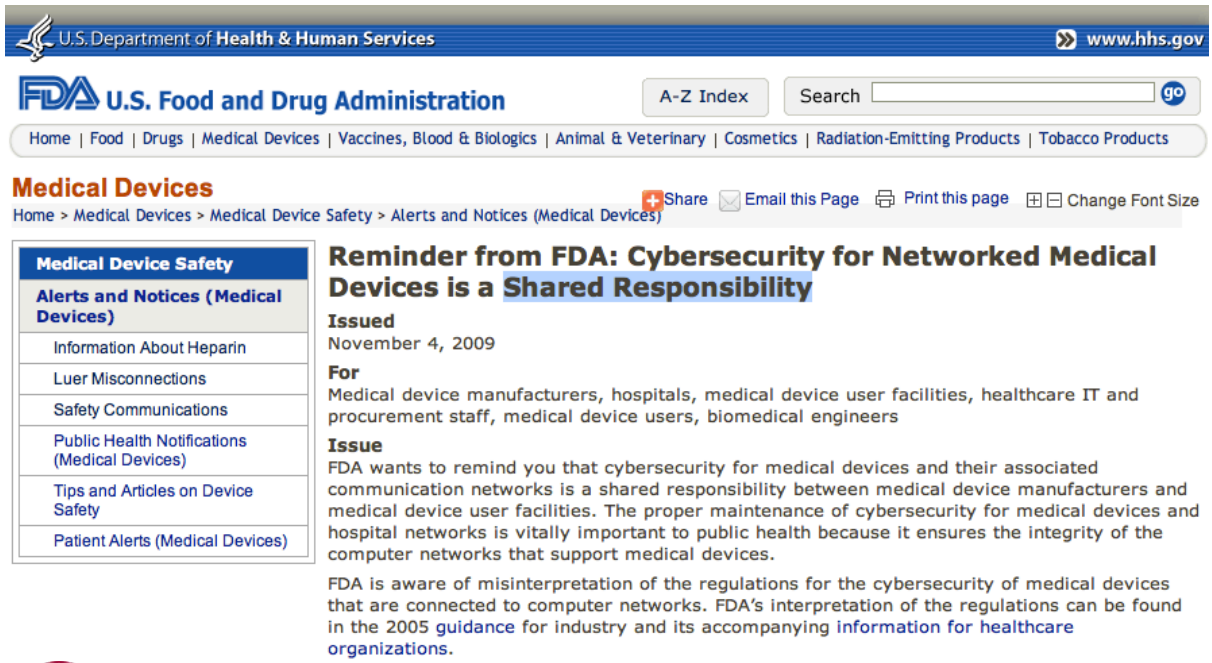
- Security falls outside the purview of the Food and Drug Administration, [**FDA** spokeswoman Karen Riley] said, unless mandated measures taken to protect data end up causing problems.

  …

  "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.**"

  [E. Cooney, "Security of medical devices is a concern," Boston Globe, July 5, 2010]

Still Not It: Hospitals, Manufacturers



U.S. Department of Health & Human Services www.hhs.gov

FDA U.S. Food and Drug Administration A-Z Index Search go

Home | Food | Drugs | Medical Devices | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Radiation-Emitting Products | Tobacco Products

Medical Devices

Share Email this Page Print this page Change Font Size

Home > Medical Devices > Medical Device Safety > Alerts and Notices (Medical Devices)

Medical Device Safety

Alerts and Notices (Medical Devices)

- Information About Heparin
- Luer Misconnections
- Safety Communications
- Public Health Notifications (Medical Devices)
- Tips and Articles on Device Safety
- Patient Alerts (Medical Devices)

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

Print Email SHARE

T Smaller | Larger

By Rachael Bell

The Tylenonl Terrorist: Death in a Bottle

Extra-Strength Tylenol package

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.

[Source: truTV crime library]

Fatal tampering case is renewed

FBI searches a condo in Cambridge

FBI agents carrying items seized from an apartment building on Gore Street in Cambridge walked out before a phalanx of television photographers. Five boxes and a computer were removed, but the FBI would not comment on their contents. (JIM DAVIS/GLOBE STAFF)

February 5, 2009

Email | Print | Single Page | Yahoo! Buzz | ShareThis Text size

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.

Discuss
COMMENTS (5)

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.

21 CFR 211.132 and Security

TITLE 21--FOOD AND DRUGS
CHAPTER I--FOOD AND DRUG ADMINISTRATION
DEPARTMENT OF HEALTH AND HUMAN SERVICES
SUBCHAPTER C--DRUGS: GENERAL

PART 211 -- CURRENT GOOD MANUFACTURING PRACTICE FOR FINISHED PHARMACEUTICALS

Subpart G--Packaging and Labeling Control

Sec. 211.132 Tamper-evident packaging requirements for over-the-counter (OTC) human drug products.

(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

Security 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

CDRH SuperSearch

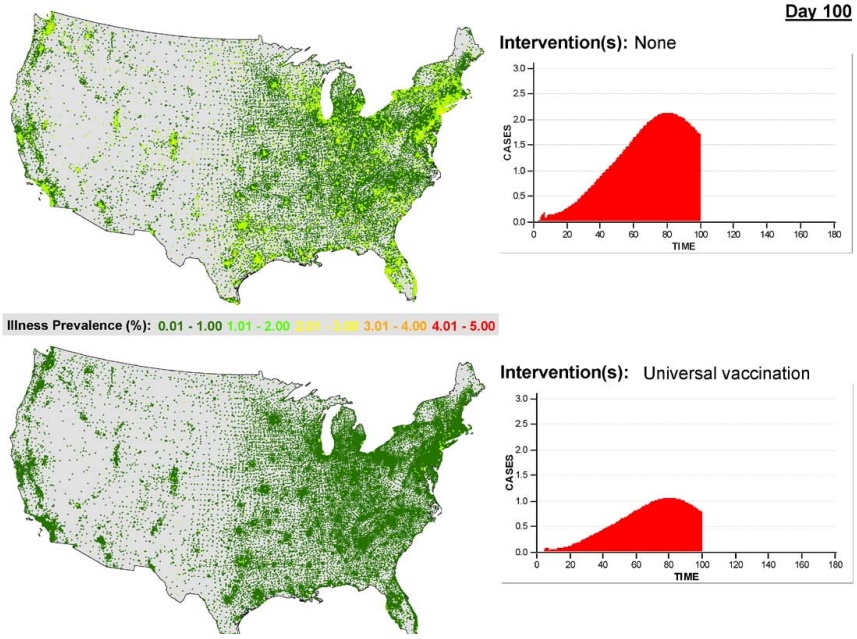
510(k) | Registration & Listing | Adverse Events | Recalls | PMA | Classification | Standards
CFR Title 21 | Radiation-Emitting Products | X-Ray Assembler | Medsun Reports | CLIA

FUJIFILM MEDICAL SYSTEM USA, INC. IIP COMPUTED RADIOGRAPHY READER AND WORKSTATION — Back to Search Results

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

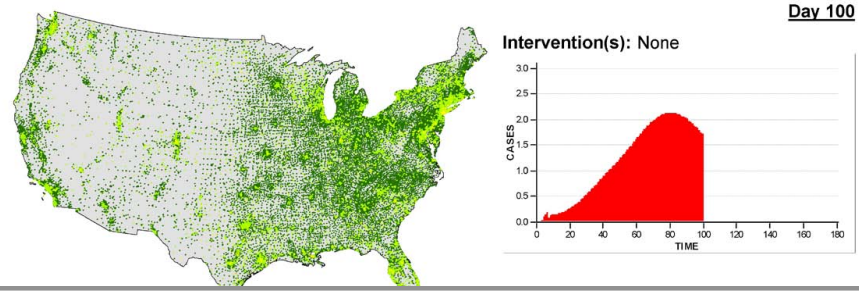
Delay in treatment related to equipment failure on 4 patients. The images were frozen on the list and would not transmit on the fuji reader equipment. The system was rebooted without change. A few hours later the system was again shut down and rebooted and the images then did transfer. Images were repeated 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.

Disease to Malware:Days to Hours



FluTE: Chao et al., *PLoS Computational Biology*, 2010

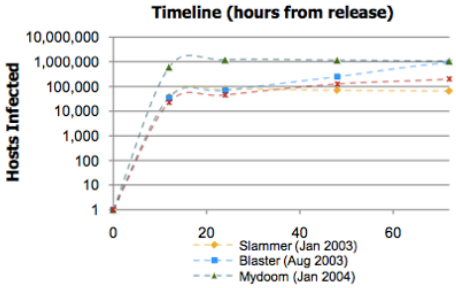
Disease to Malware:Days to Hours



FluTE: Chao et al., *PLoS Computational Biology*, 2010

DARPA

Dark Clouds on the Horizon:
The Network is a *Vulnerability Amplifier*



Slide from Howie Shrobe and others

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]

How significant are **intentional, malicious malfunctions** in software?

Information Assurance or Bliss?

http://tobacco.stanford.edu/

Information Assurance or Bliss?

"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

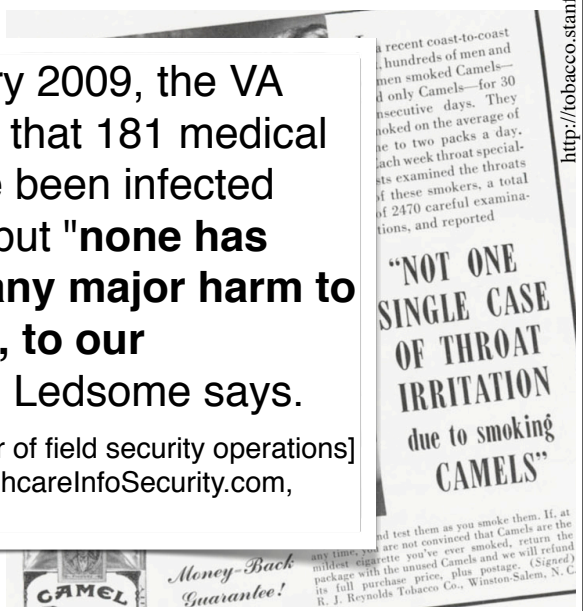
[B. Feder, "A Heart Device Is Found Vulnerable to Hacker Attacks" NY Times, March 12, 2008]

http://tobacco.stanford.edu/

Information Assurance or Bliss?

"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]

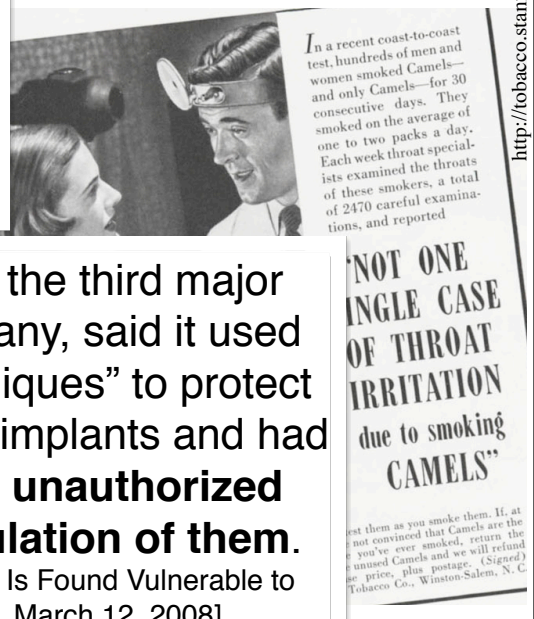


http://tobacco.stanford.edu/

Information Assurance or Bliss?

"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]



http://tobacco.stanford.edu/

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]

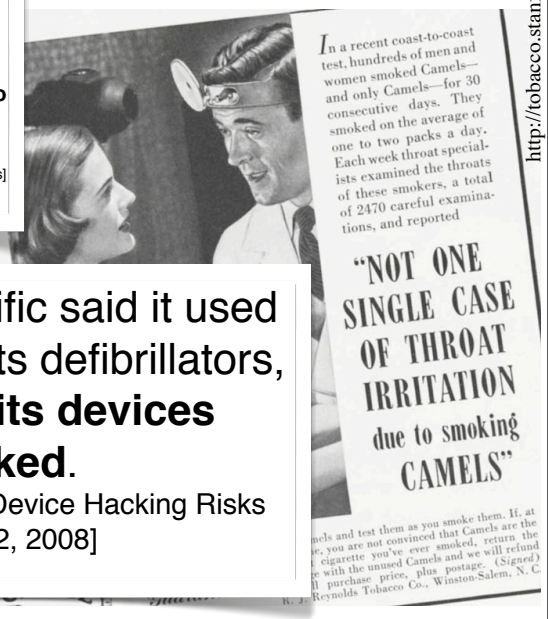
Information Assurance or Bliss?

"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]

Boston Scientific said it used encryption in its defibrillators, and **doubted its devices could be hacked**.
[K. Winstein, "Heart-Device Hacking Risks Seen" WSJ, March 12, 2008]



http://tobacco.stanford.edu/

Informati Ass nce Bliss?

"This is an evolution from having to **think about security and safety** as a healthcare company, and really about keeping people safe on our therapy, to this different question about keeping people safe around criminal or malicious intent."

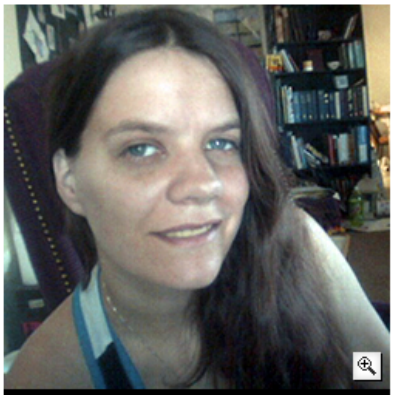
[Catherine Szyman, President, Medtronic diabetes division, Reuters, October 26, 2011]

http://tobacco.stanford.edu/

Bad People Do Exist

Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen 03.28.08 | 8:00 PM



RyAnne Fultz, 33, says she suffered her worst epileptic attack in a year after she clicked on the wrong post at a forum run by the nonprofit Epilepsy Foundation. *Photo courtesy RyAnne Fultz*

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.

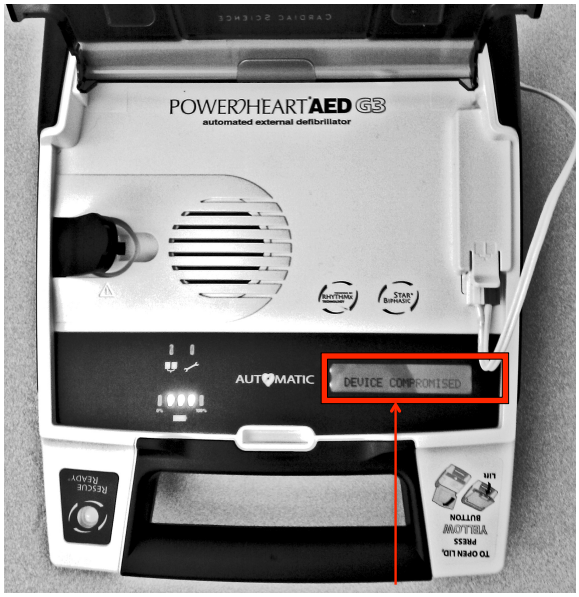
The nonprofit Epilepsy Foundation, which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security.

"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.

AED Firmware Replacement



- Device accepts unauthentic firmware updates
- How do risks change when AEDs become wireless with Internet-based software updates?

DEVICE COMPROMISED

Insulin Pumps, Monitors Vulnerable To Hacking

by THE ASSOCIATED PRESS

Associated Press

Hackers and digital security personnel attend the annual Black Hat conference for digital self defense Thursday, Aug. 4, 2011, in Las Vegas. Even the human bloodstream isn't safe from computer hackers. A security researcher who is diabetic has identified flaws that could allow an attacker to remotely control insulin pumps and alter the readouts of blood-sugar monitors. As a result, diabetics could get too much or too little insulin, a hormone they need for proper metabolism.Â

LAS VEGAS August 5, 2011, 12:03 pm ET

text size A A A

Even the human bloodstream isn't safe from computer hackers.

A security researcher who is diabetic has identified flaws that could allow an attacker to remotely control insulin pumps and alter the readouts of blood-sugar monitors. As a result, diabetics could get too much or too little insulin, a hormone they need for proper metabolism.

Jay Radcliffe, a diabetic who experimented on his own equipment, shared his findings with The Associated Press before releasing them Thursday at the Black Hat computer security conference in Las Vegas.

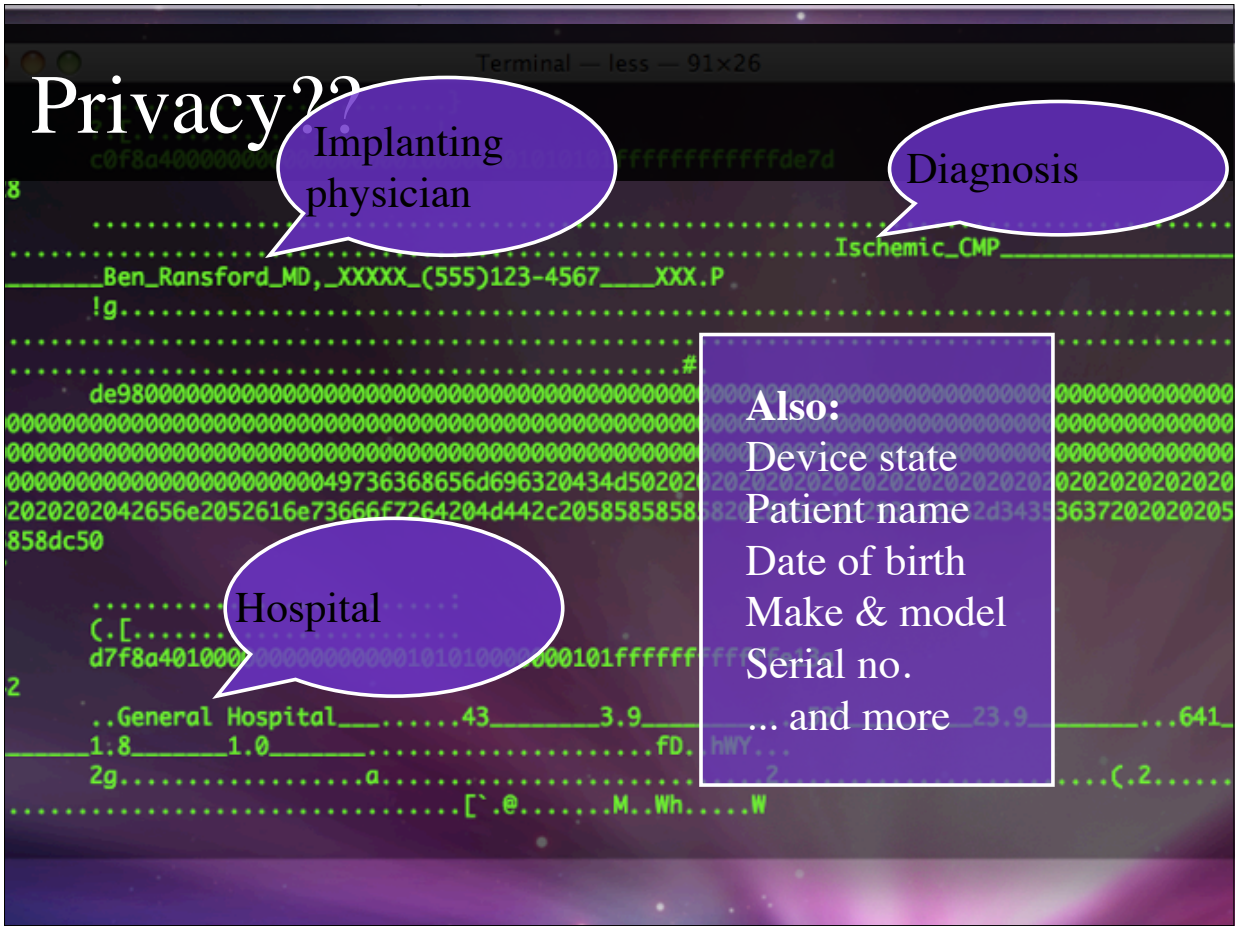
"My initial reaction was that this was really cool from a technical perspective," Radcliffe said. "The second reaction was one of maybe sheer terror, to know that there's no security around the devices which are a very active part of

Implantation Scenario

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

Device Programmer

Photos: Medtronic; Video: or-live.com



Privacy: Wardrobe Malfunctions

The New York Times

N.Y. / Region

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

THE CITY | CONNECTICUT | LONG ISLAND | NEW JERSEY | WESTCHESTER

Hospital Bracelets Face Hurdles as They Fix Hazard

Chester Higgins Jr./The New York Times

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]

How to attract hackers to medical devices:

- Increase software complexity
- Add radio communication
- Trust the Internet for clinical decision making

[http://www.surfersam.com/funny-pictures/hackers.jpg]

Technical issues

Vulnerabilities are in plain sight.
When will risk become a tangible threat?

←Ways Forward ↗ for Software?

[http://en.wikipedia.org/wiki/Washington_State_Route_510]

Trustworthy Medical Device SW

- Software:
  - breeds overconfidence,
  - is not thoroughly testable, but
  - is flooding into medical devices
- Manufacturers could mitigate risks with known technology
  - Avoid hardware as a predicate for software
  - Adopt modern software engineering & systems engineering tech.
  - Create more meaningful specification of requirements
  - Better analyze human factors
  - Develop safety net for security and privacy
- Need: Better surveillance of SW, clearer responsibility, convenient reporting mechanisms

OPEN MEDICAL DEVICE RESEARCH LIBRARY

omdrl.org

symantec. McAfee

Cal

UNIVERSITY OF SOUTH CAROLINA

W

MIT Massachusetts Institute of Technology

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

SHARPS

Strategic Healthcare Advanced Research Projects for Security

www.sharps.org

SHARP research areas:

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

http://HealthIT.HHS.gov/sharp

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

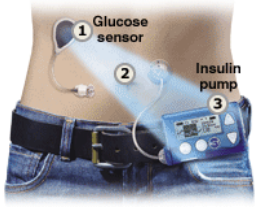
- **EHR** – Electronic Health Records, managing patient records within an enterprise
- **HIE** – Health Information Exchange, sharing records between enterprises or between an enterprise and a patient in the form of a Personal Health Record
- **TEL** – Telemedicine, monitoring remotely, communicating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

Wireless + Internet Can Improve Healthcare

But not without fully understanding trustworthy computing

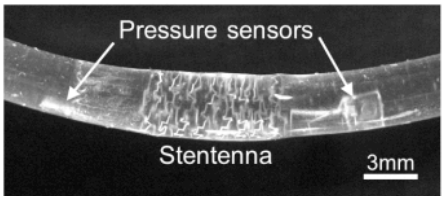


Insulin pump

Obesity control

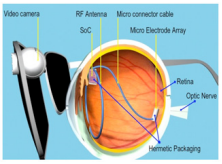
Neurostimulators

Programmable Vasectomy



Smart stent

Artificial pancreas



Artificial vision

Photos: Medgadget, Takahata Lab

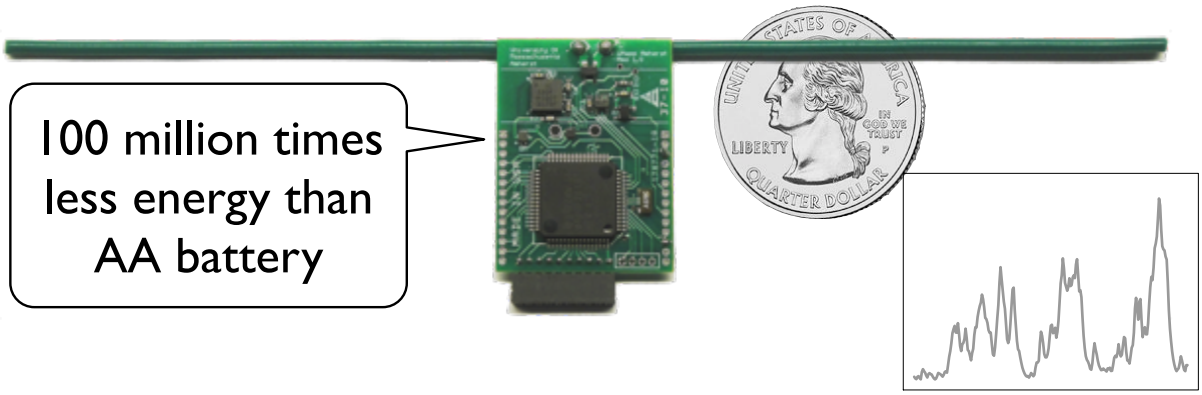
Further Reading

- Steve Hanna, Rolf Rolles, Andres Molina-Markham, Pongsin Poosankam, Kevin Fu, and Dawn Song. Take two software updates and see me in the morning: The case for software security evaluations of medical devices. In *Proceedings of 2nd USENIX Workshop on Health Security and Privacy (HealthSec)*, August 2011.
- Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They can hear your heartbeats: Non-invasive security for implanted medical devices. In *Proceedings of ACM SIGCOMM*, August 2011.
- 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.
- Kevin Fu. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*, Washington, DC, 2011. IOM (Institute of Medicine), National Academies Press.
- Benessa Defend, Mastooreh Salajegheh, Kevin Fu, and Sozo Inoue. Protecting global medical telemetry infrastructure. Technical report, Institute of Information Infrastructure Protection (I3P), January 2008.
- Sinjin Lee, Kevin Fu, Tadayoshi Kohno, Benjamin Ransford, and William H. Maisel. Clinically significant magnetic interference of implanted cardiac devices by portable headphones. *Heart Rhythm Journal*, 6(10):1432–1436, October 2009.
- Kevin Fu. Inside risks, reducing the risks of implantable medical devices: A prescription to improve security and privacy of pervasive health care. *Communications of the ACM*, 52(6):25–27, June 2009.
- Mastooreh Salajegheh, Andres Molina, and Kevin Fu. Privacy of home telemedicine: Encryption is not enough. *Journal of Medical Devices*, 3 (2), April 2009. Design of Medical Devices Conference Abstracts.
- Tamara Denning, Kevin Fu, and Tadayoshi Kohno. Absence makes the heart grow fonder: New directions for implantable medical device security. In *Proceedings of USENIX Workshop on Hot Topics in Security (HotSec)*, July 2008.
- Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the 29th Annual IEEE Symposium on Security and Privacy*, pages 129–142, May 2008.
- Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, 7(1), January 2008.

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

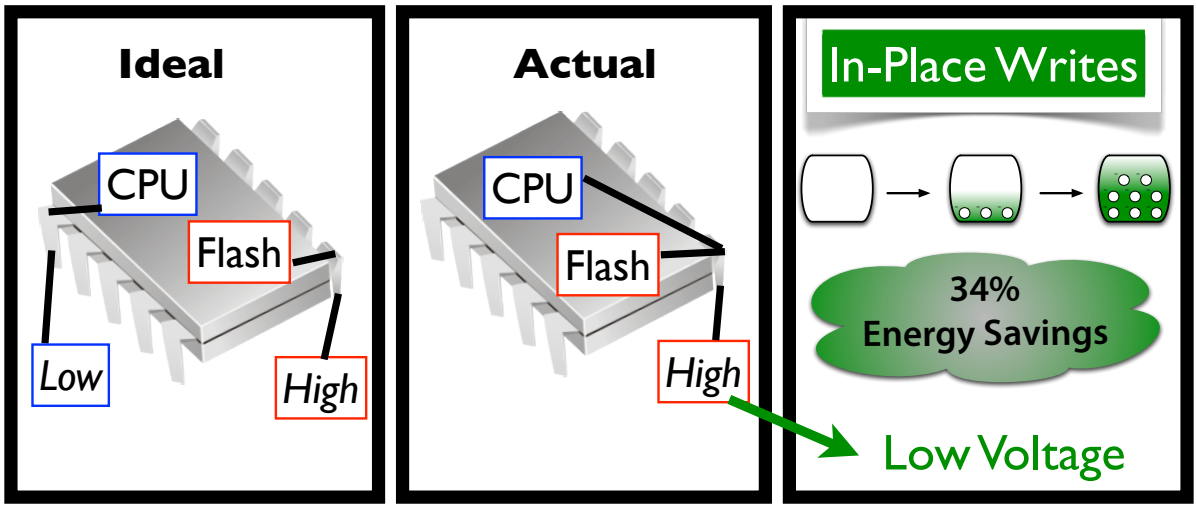
Extra Material

RFID-Scale Computing Platforms



http://spqr.cs.umass.edu/moo/

Smarter Storage for Low-Power Devices

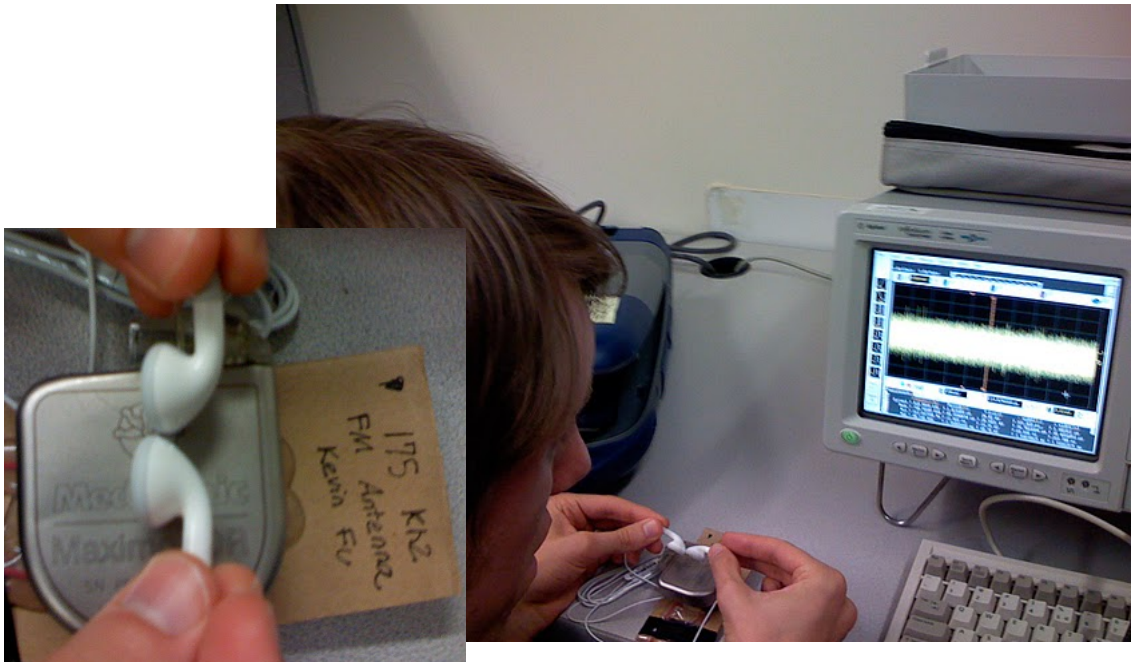


http://spqr.cs.umass.edu/half-wits/

[Salajegheh et al. USENIX FAST 2011]

Headphones Can Disrupt Implanted Heart Devices

by JOSEPH SHAPIRO



["Clinically Significant Magnetic Interference of Implanted Cardiac Devices by Portable Headphones" by Lee et al. Heart Rhythm Journal 6(10), October 2009.]