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?

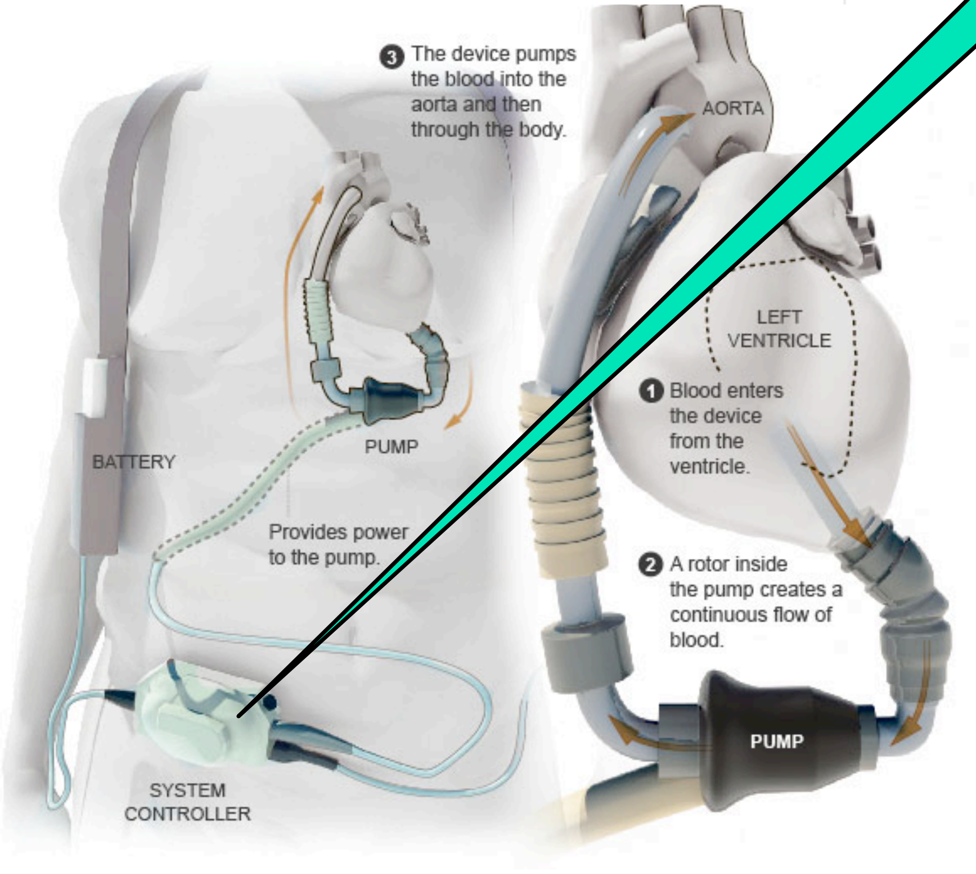
Benefits of Medical Device Software

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


3 The device pumps the blood into the aorta and then through the body.
AORTA
LEFT VENTRICLE
1 Blood enters the device from the ventricle.
2 A rotor inside the pump creates a continuous flow of blood.
PUMP
BATTERY
PUMP
Provides power to the pump.
SYSTEM CONTROLLER

Computer

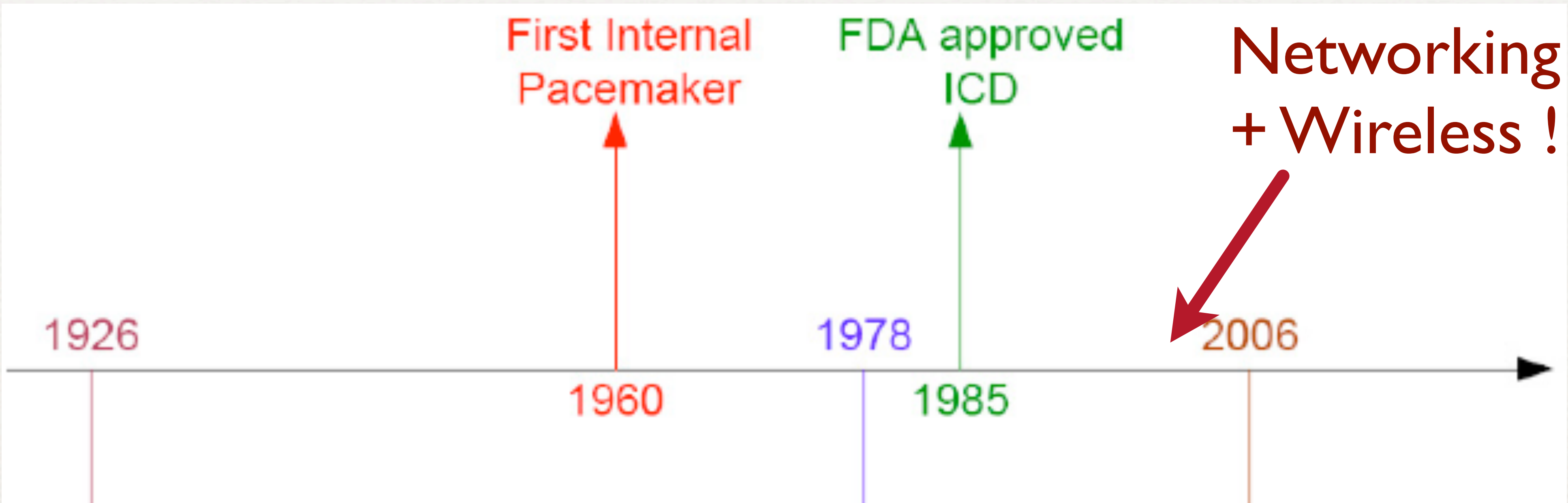
"Recent reports show improvement over the earlier model mechanical hearts"

Source: NY Times, Thoratec

Without software,
many medical treatments
could not exist.

Medical Devices 101:

A 10-minute residency for the security & privacy researcher



First Internal Pacemaker

FDA approved ICD

Networking + Wireless !

1926

1960

1978

1985

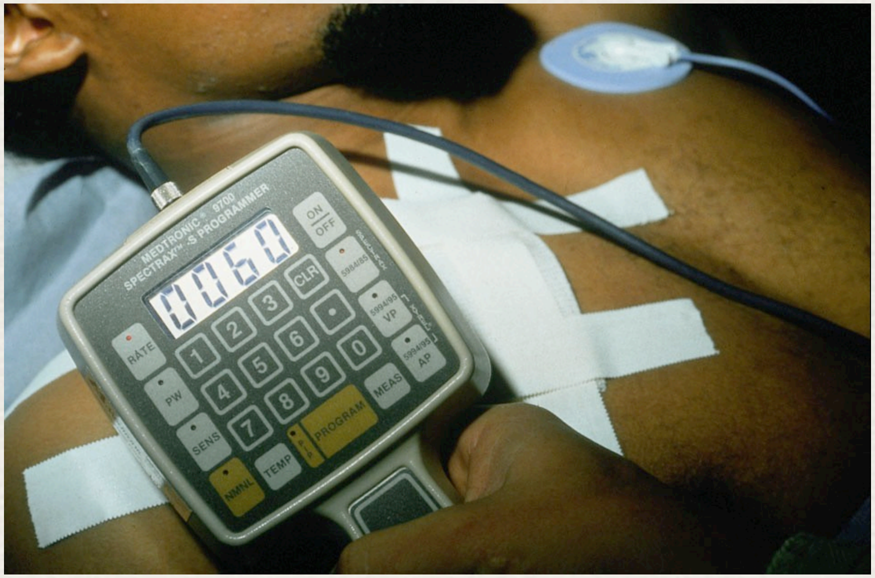
2006

First Pacemaker

First Cochlear Implant Surgery

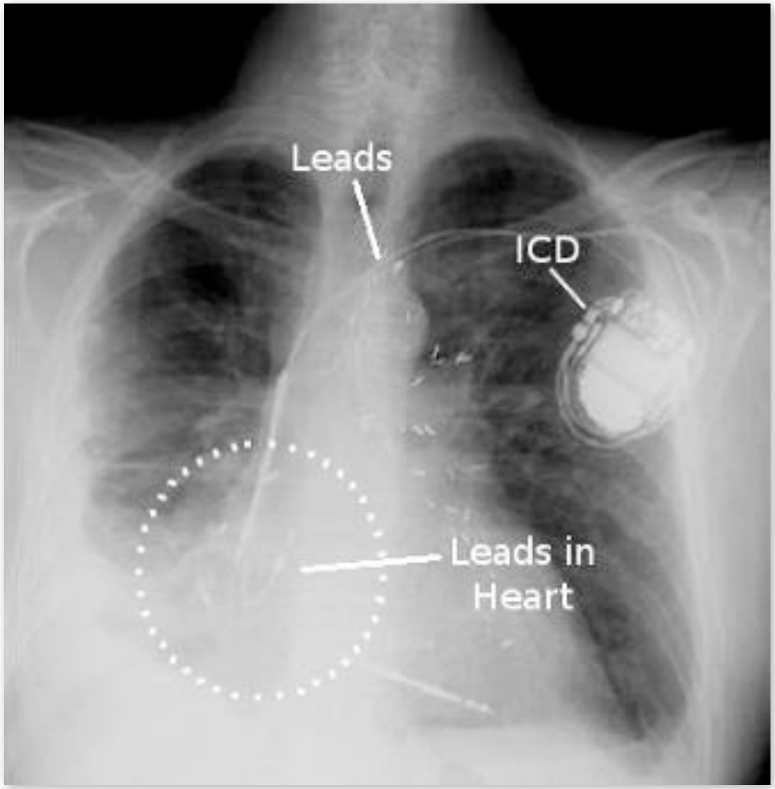
Wireless Blood Glucose Monitor

Principles And Techniques Of Cardiac Pacing. c. 1970; Page 6.

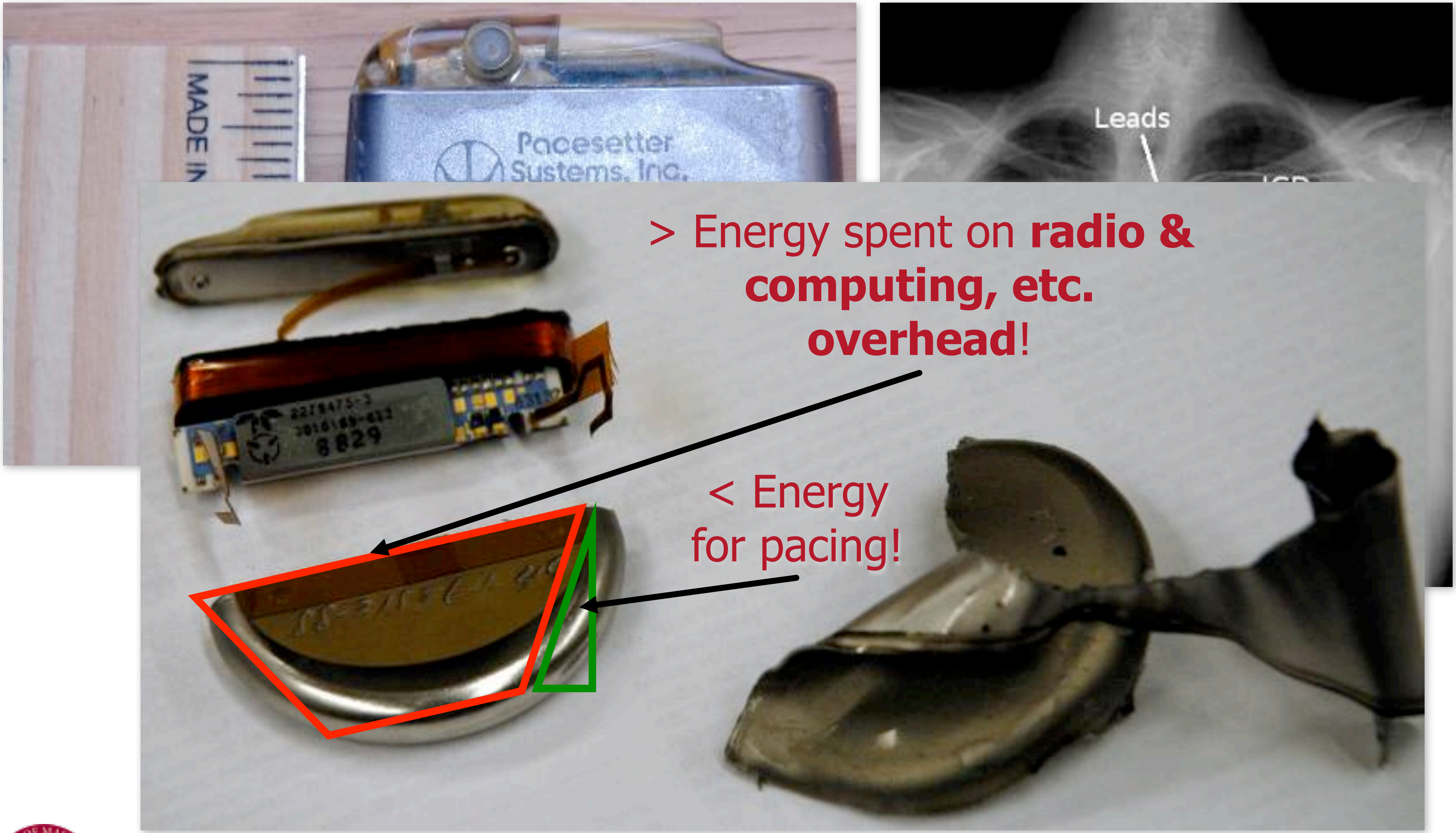


Photos from: Medtronic

Pacemakers: Regulate heartbeat



Pacemakers: Regulate heartbeat

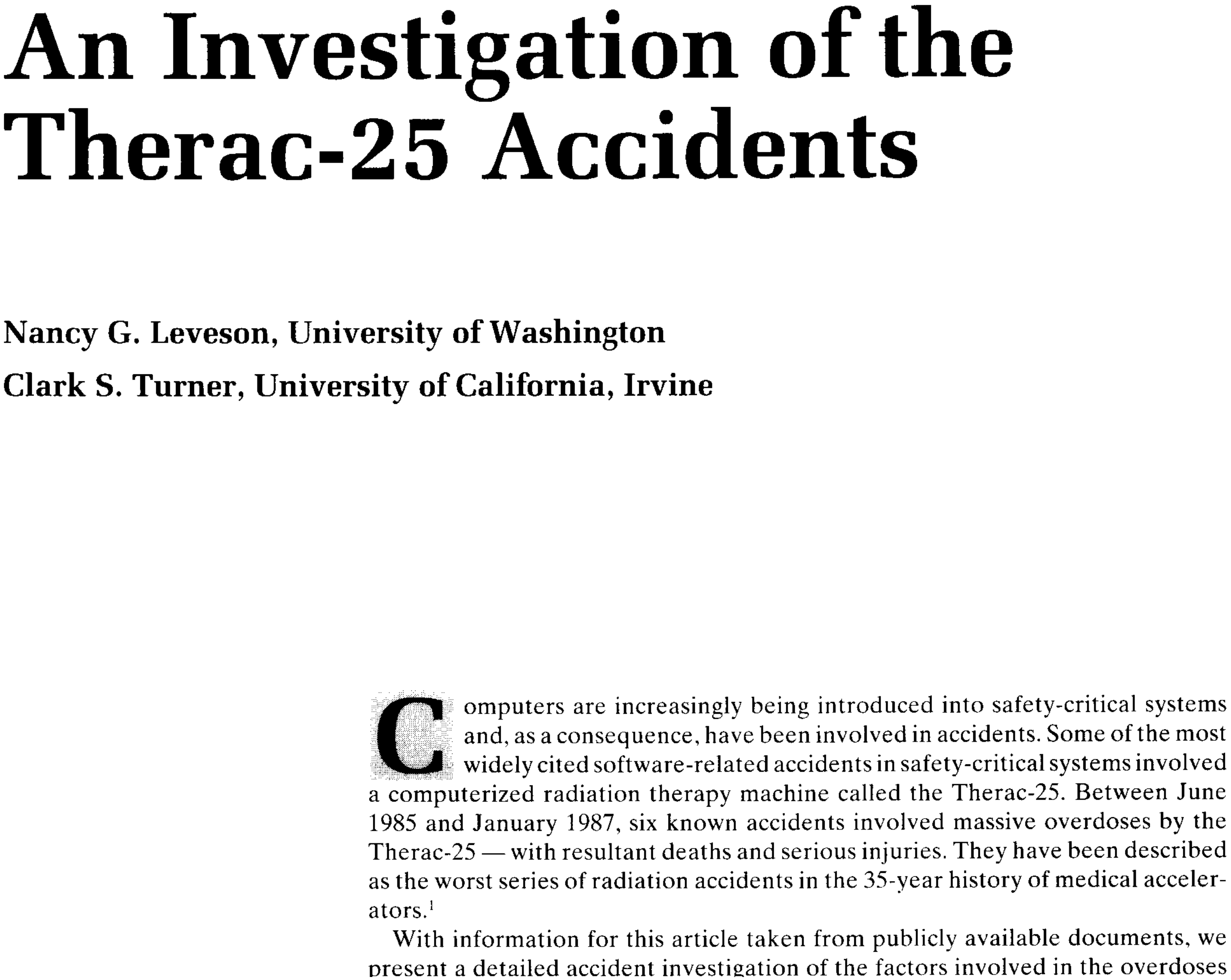


> Energy spent on **radio & computing, etc. overhead**!

< Energy for pacing!

Medical Device Failures

IEEE Computer 1993



An Investigation of the Therac-25 Accidents

Nancy G. Leveson, University of Washington

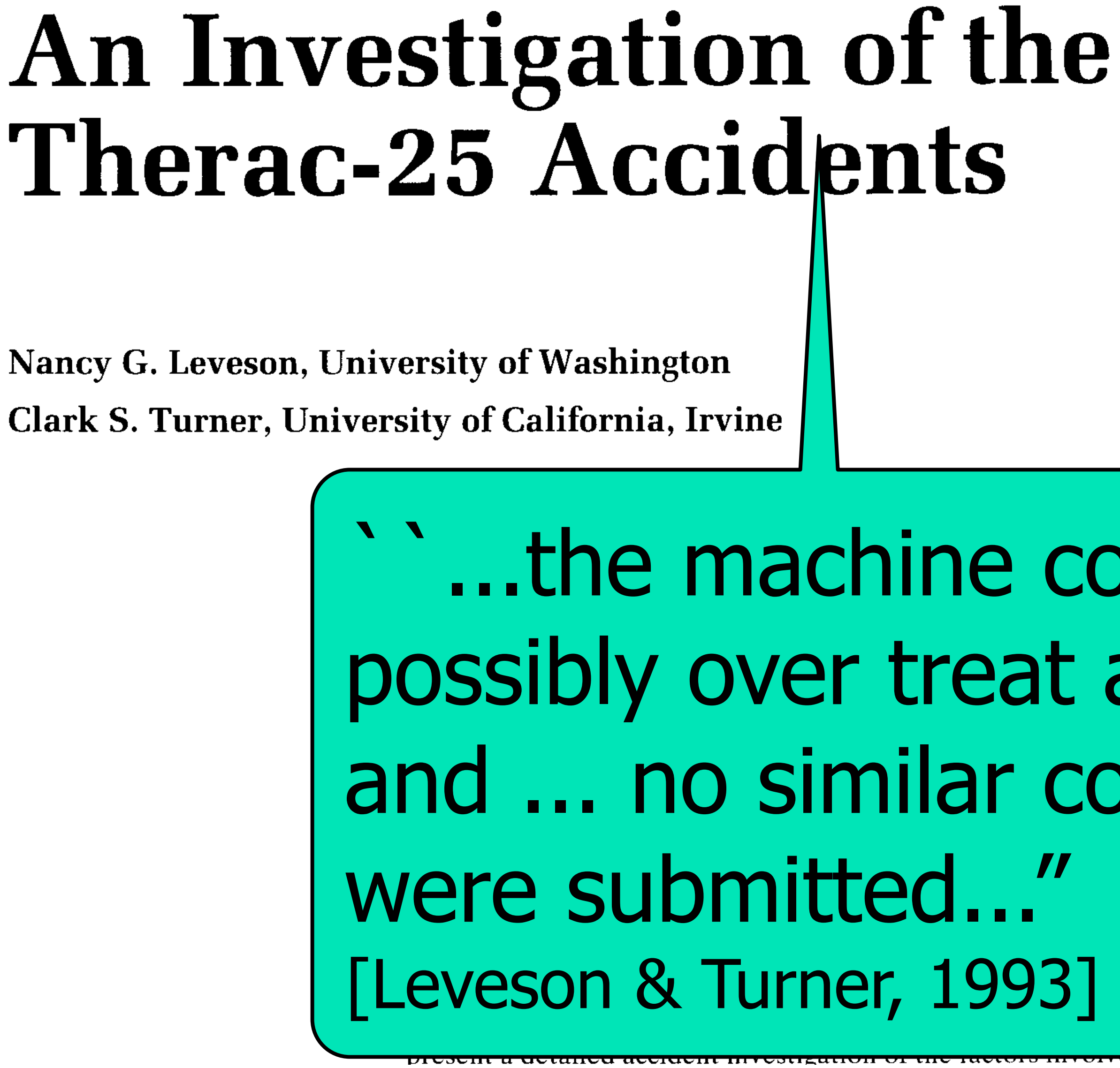
Clark S. Turner, University of California, Irvine

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

Medical Device Failures

IEEE Computer 1993



An Investigation of the Therac-25 Accidents

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

present a detailed accident investigation of the factors involved in the overdoses

``...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

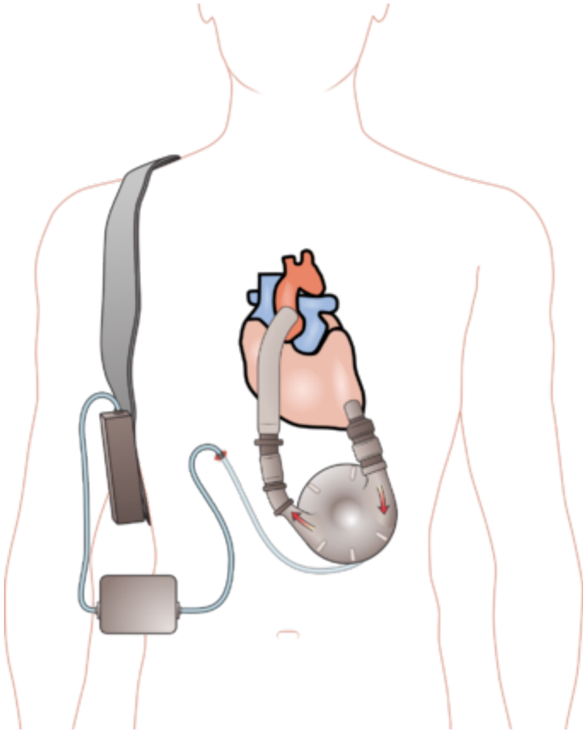
[Sources: Bliznakov et al. 2006, Faris 2006, Maisel et al. 2002, Wallace & Kuhn 2001, Computer history museum, eurogramer.net, wikipedia, businesspundit.com, imdb.com, coverbrowser.com, thefilmtalk.com]

(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**.”

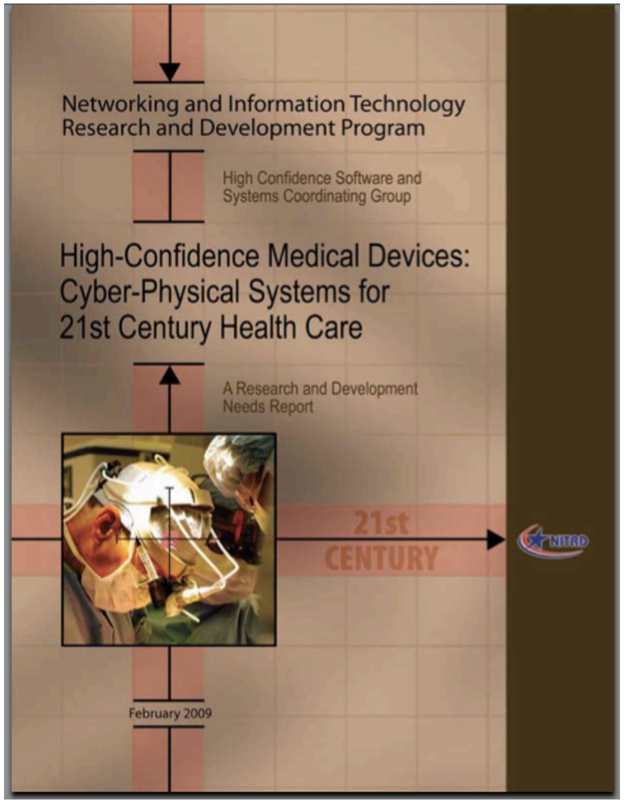
  -David Feigal
  Fmr. Director, FDA Center for Devices and Radiological Health (CDRH)
  [Institute of Medicine Meeting 2, June 2010:
  Public Health Effectiveness of the FDA 510(k) Clearance Process]

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**."



Networking and Information Technology
Research and Development Program

High Confidence Software and
Systems Coordinating Group

High-Confidence Medical Devices:
Cyber-Physical Systems for
21st Century Health Care

A Research and Development
Needs Report

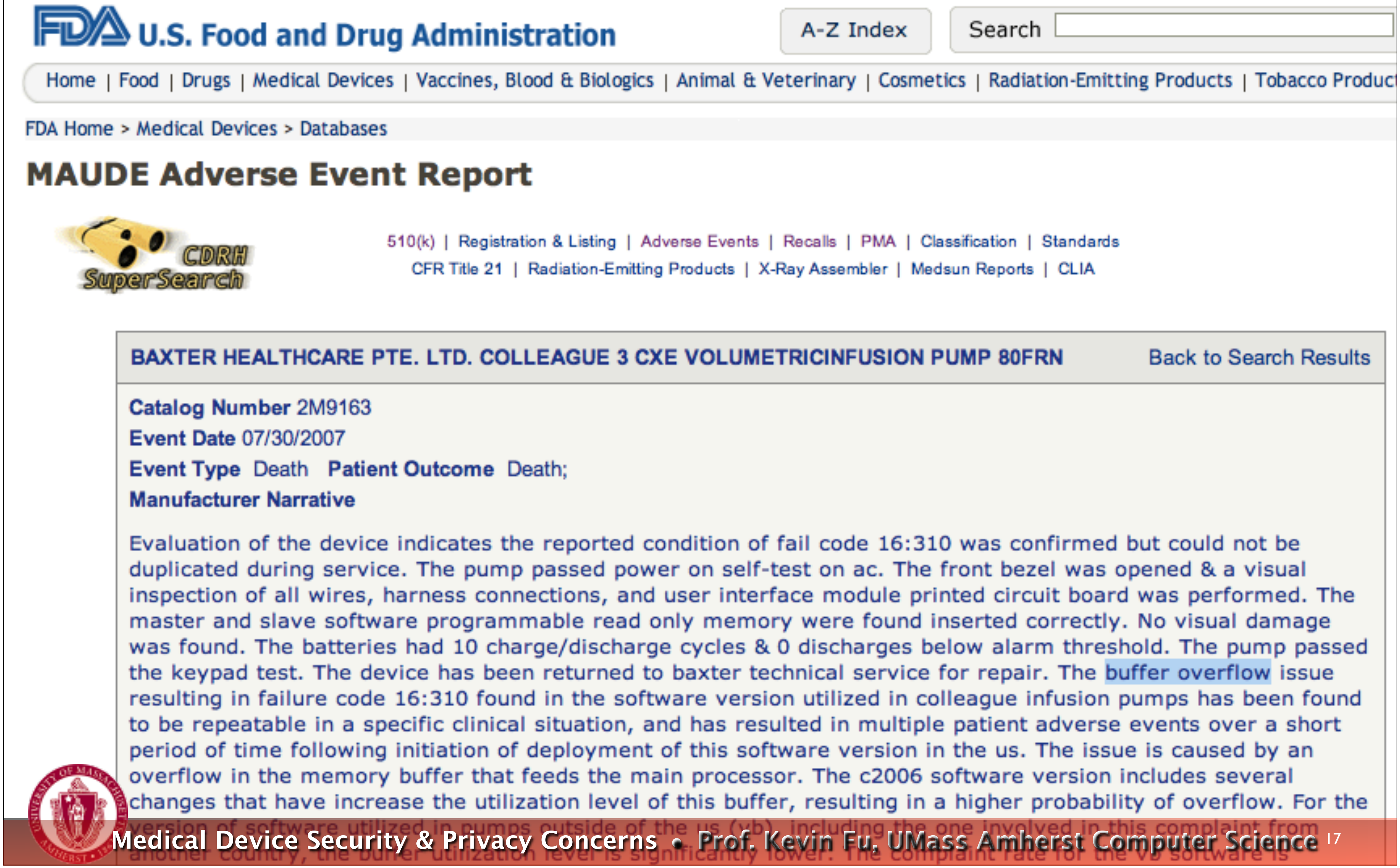
21st
CENTURY

NITRD

February 2009

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

Implementation Errors


FDA 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 Produc
FDA Home > Medical Devices > Databases
CDRH SuperSearch
510(k) | Registration & Listing | Adverse Events | Recalls | PMA | Classification | Standards
CFR Title 21 | Radiation-Emitting Products | X-Ray Assembler | Medsun Reports | CLIA
Back to Search Results

MAUDE Adverse Event Report

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

Catalog Number 2M9163

Event Date 07/30/2007

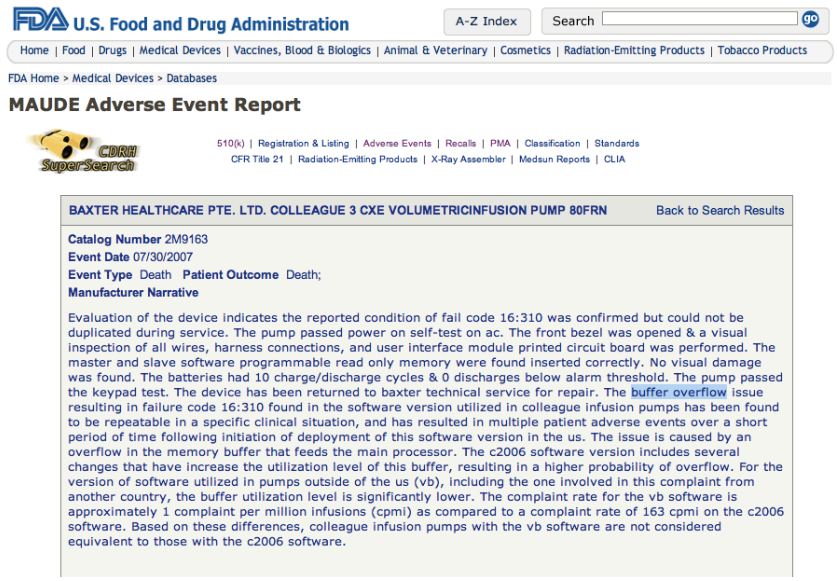
Event Type Death **Patient Outcome** Death;

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 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

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


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
FDA Home > Medical Devices > Databases
CDRH SuperSearch
510(k) | Registration & Listing | Adverse Events | Recalls | PMA | Classification | Standards
CFR Title 21 | Radiation-Emitting Products | X-Ray Assembler | Medsun Reports | CLIA
Back to Search Results

MAUDE Adverse Event Report

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

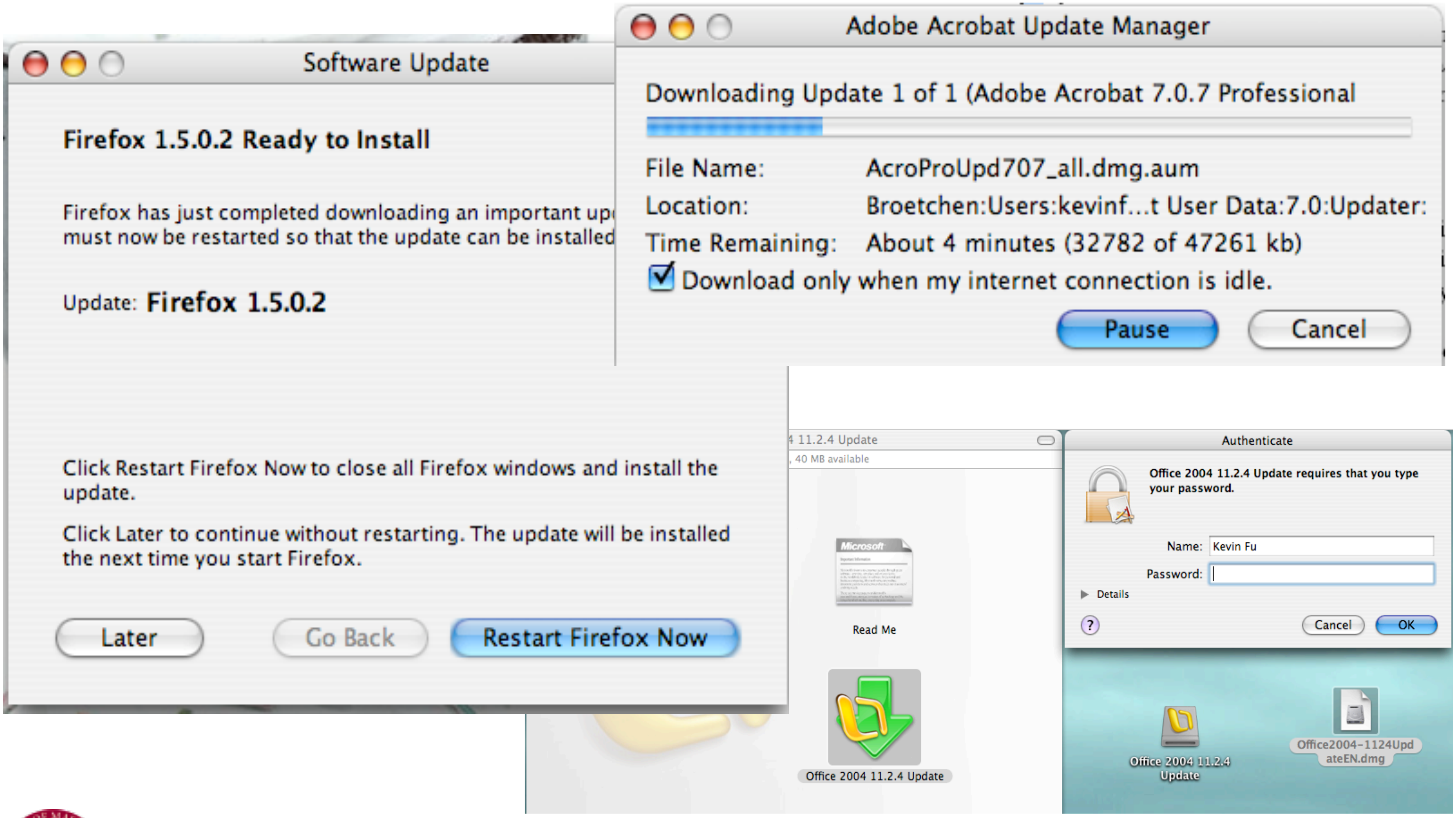
Evaluation of the device indicates the reported condition of fail code 16:310 was confirmed but could not be duplicated during service. The pump passed power on self-test on ac. The front bezel was opened & a visual inspection of all wires, harness connections, and user interface module printed circuit 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 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.

Emerging issues for information security and privacy

Managerial issues:

Diffusion of responsibility

Dirty Secrets: SW Maintenance



Software Update

Firefox 1.5.0.2 Ready to Install

Firefox has just completed downloading an important up
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.

Adobe Acrobat Update Manager

Downloading Update 1 of 1 (Adobe Acrobat 7.0.7 Professional

File Name: AcroProUpd707_all.dmg.aum

Location: Broetchen:Users:kevinf...t User Data:7.0:Updater:

Time Remaining: About 4 minutes (32782 of 47261 kb)

☑ Download only when my internet connection is idle.

4 11.2.4 Update

, 40 MB available

Authenticate

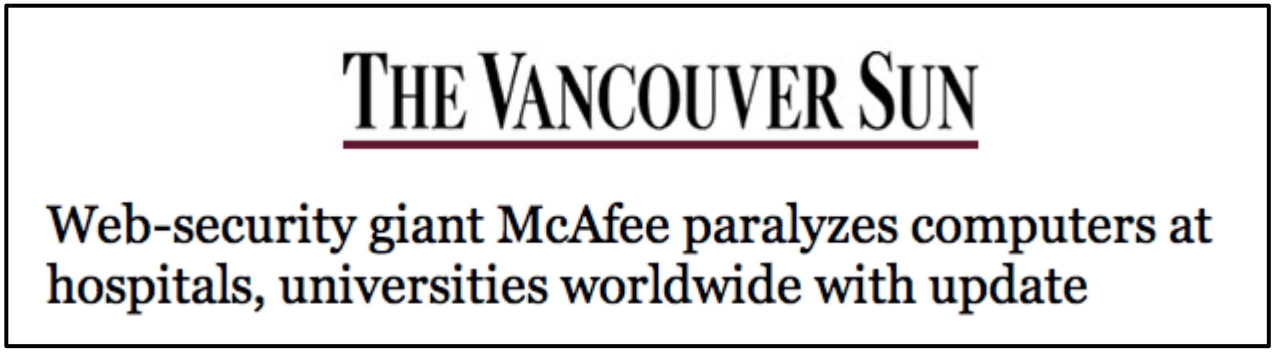
Office 2004 11.2.4 Update requires that you type your password.

Name: Kevin Fu

Password:

Software Update Woes

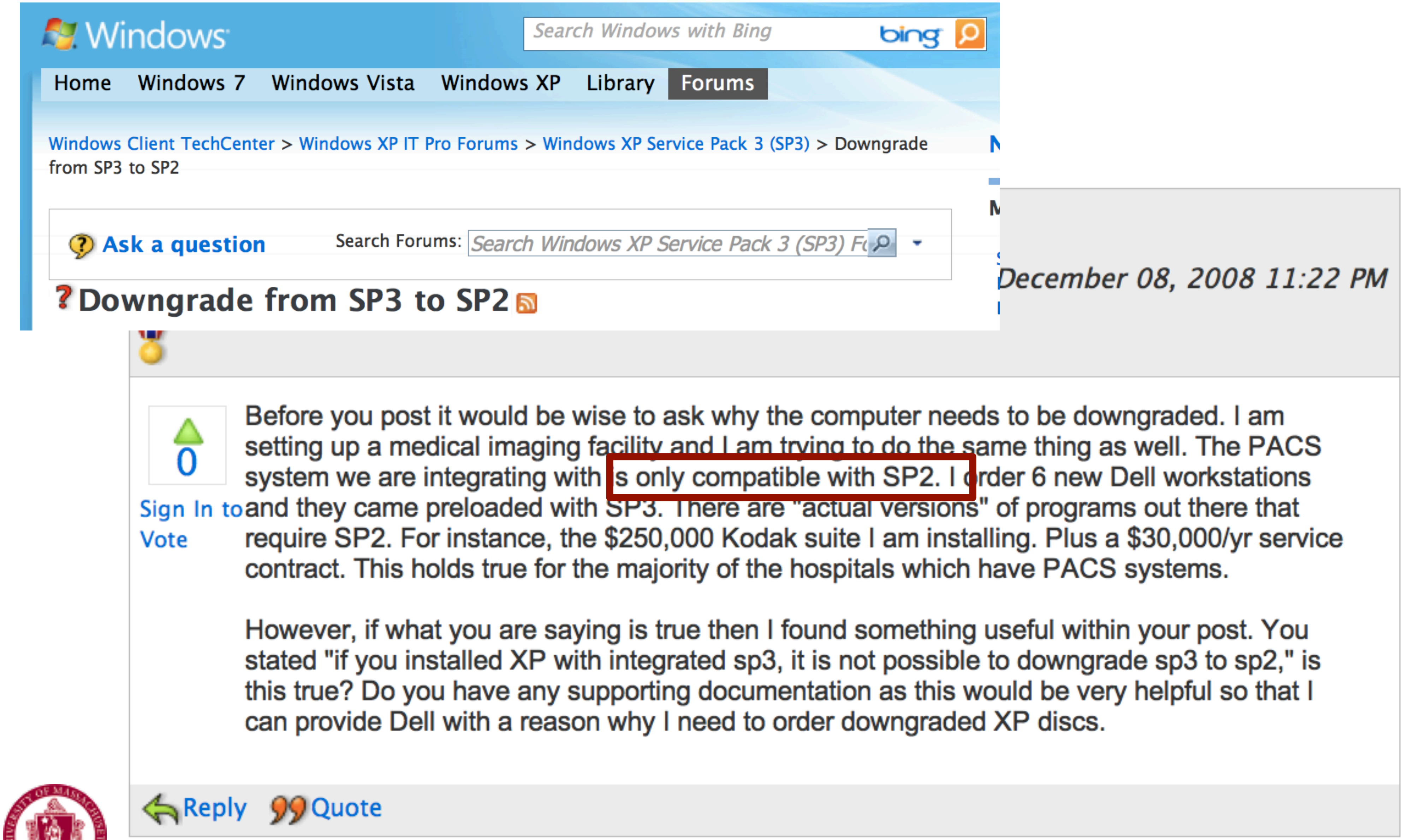
- Health Information Technology (HIT) devices globally rendered unavailable
- Cause: Automated software update went haywire
- Numerous hospitals were affected April 21, 2010
  - Rhode Island: a third of the hospitals were forced ``to postpone elective surgeries and stop treating patients without traumas 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



Windows Client TechCenter > Windows XP IT Pro Forums > Windows XP Service Pack 3 (SP3) > Downgrade from SP3 to SP2

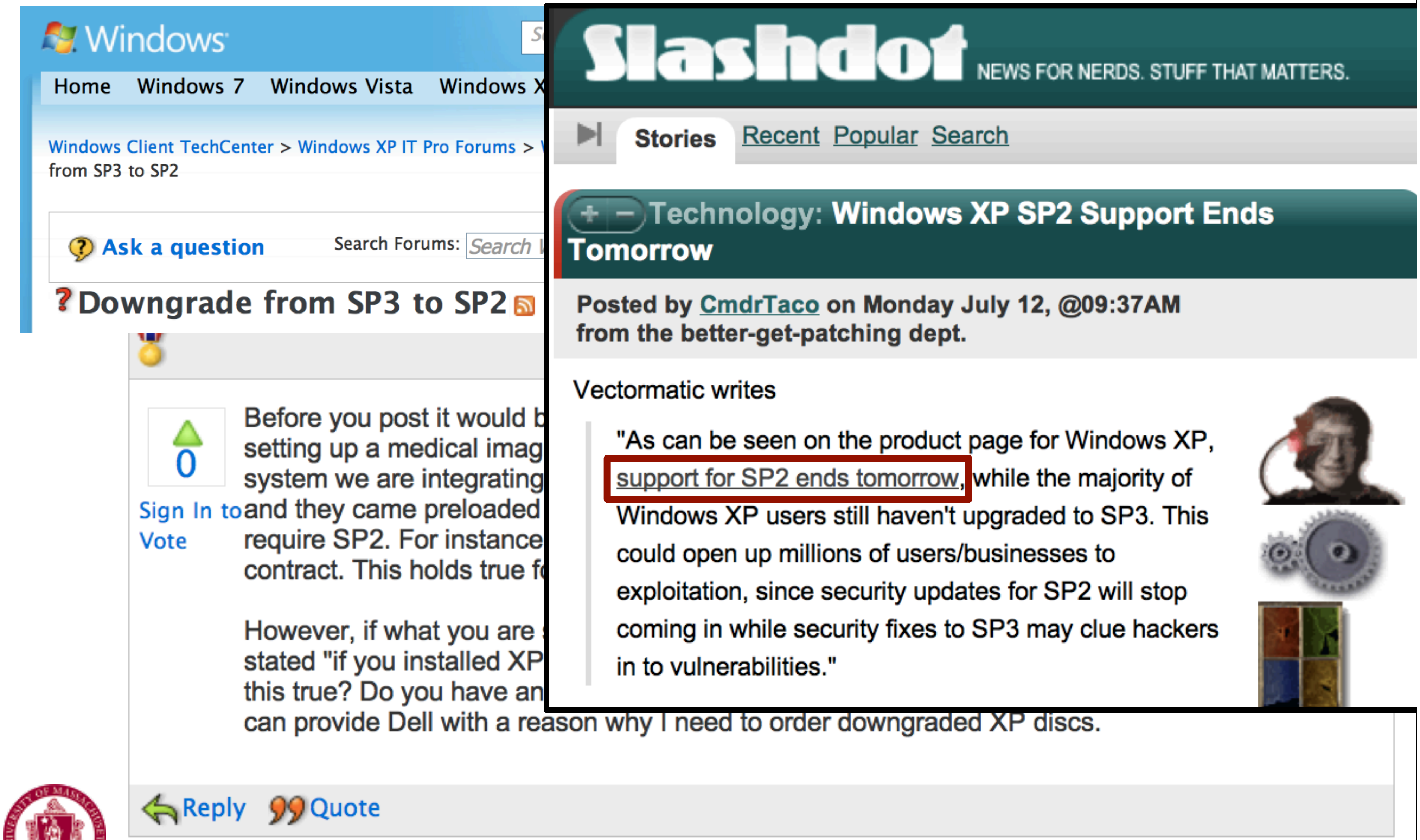
Downgrade from SP3 to SP2

December 08, 2008 11:22 PM

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



? Downgrade from SP3 to SP2

Before you post it would b
setting up a medical imag
system we are integrating
and they came preloaded
require SP2. For instance
contract. This holds true f

However, if what you are
stated "if you installed XP
this true? Do you have an
can provide Dell with a reason why I need to order downgraded XP discs.

Technology: Windows XP SP2 Support Ends Tomorrow

Posted by CmdrTaco on Monday July 12, @09:37AM
from the better-get-patching dept.

Vectormatic writes

> "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."

Not It! Olly Olly Oxen Free!

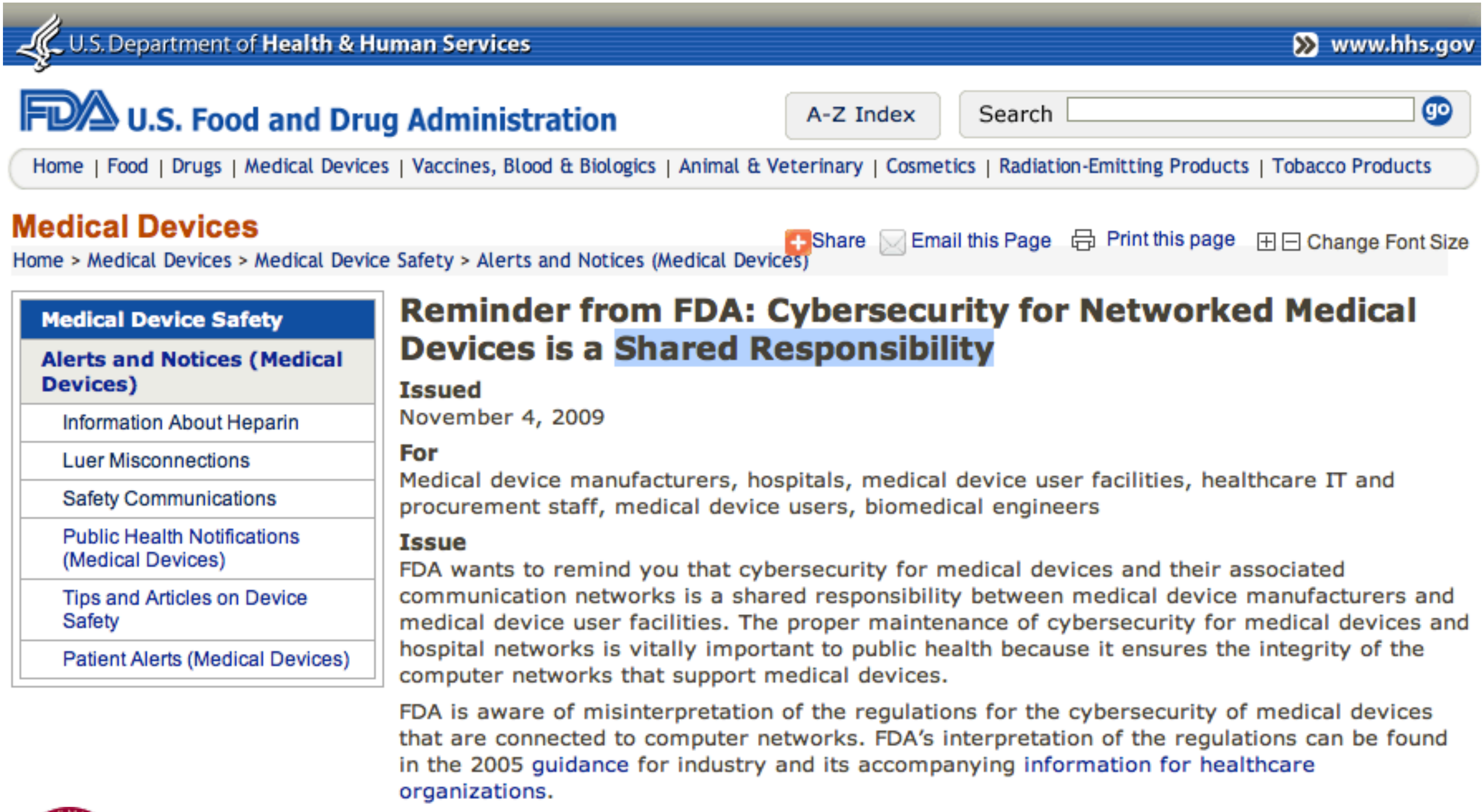
- Security falls outside the purview of the Food and Drug Administration, [**FDA** spokeswoman Karen Riley] said, unless mandated measures taken to protect data end up causing problems.

  …

  "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
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.

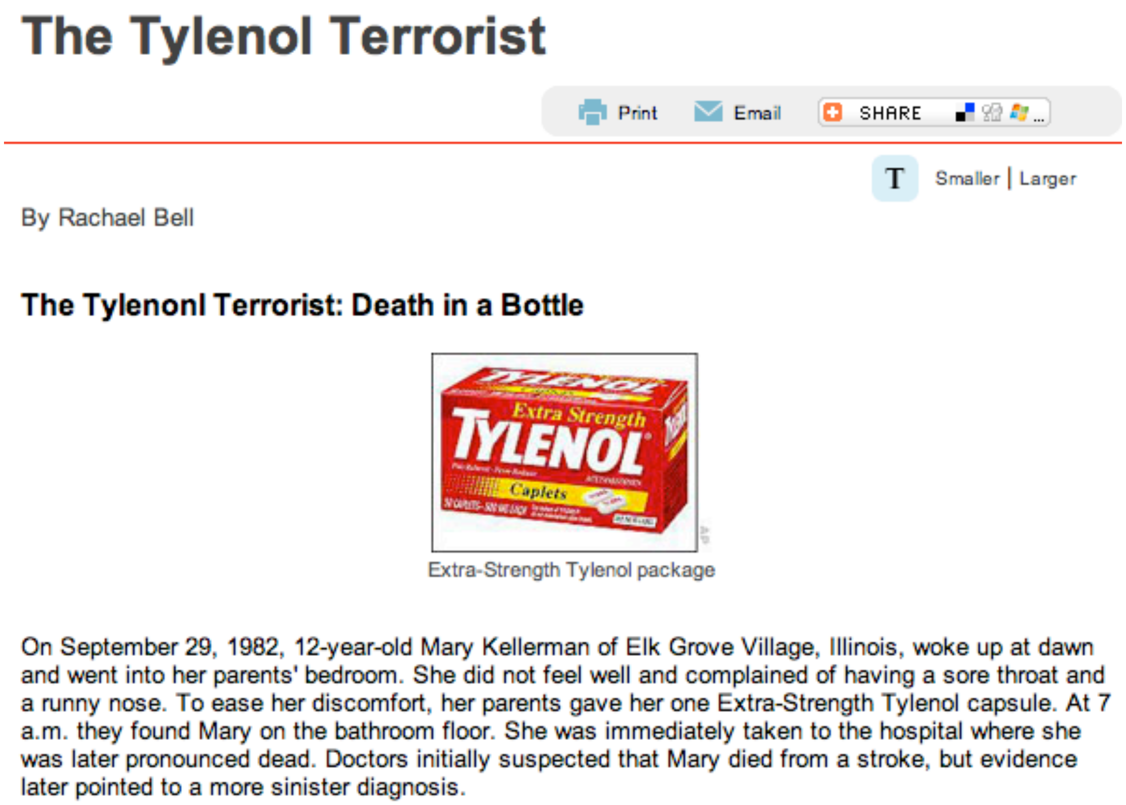
Managerial issues:

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

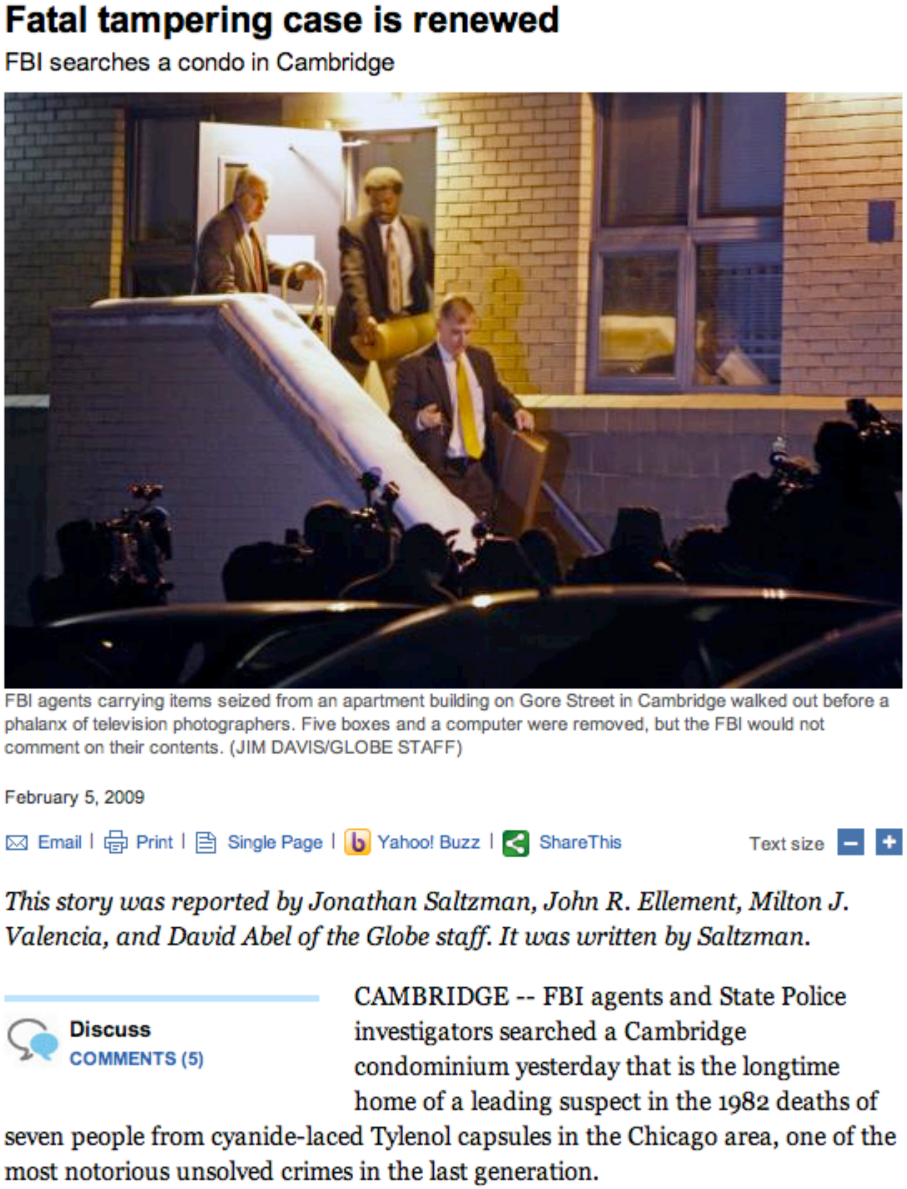
By Rachael Bell

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

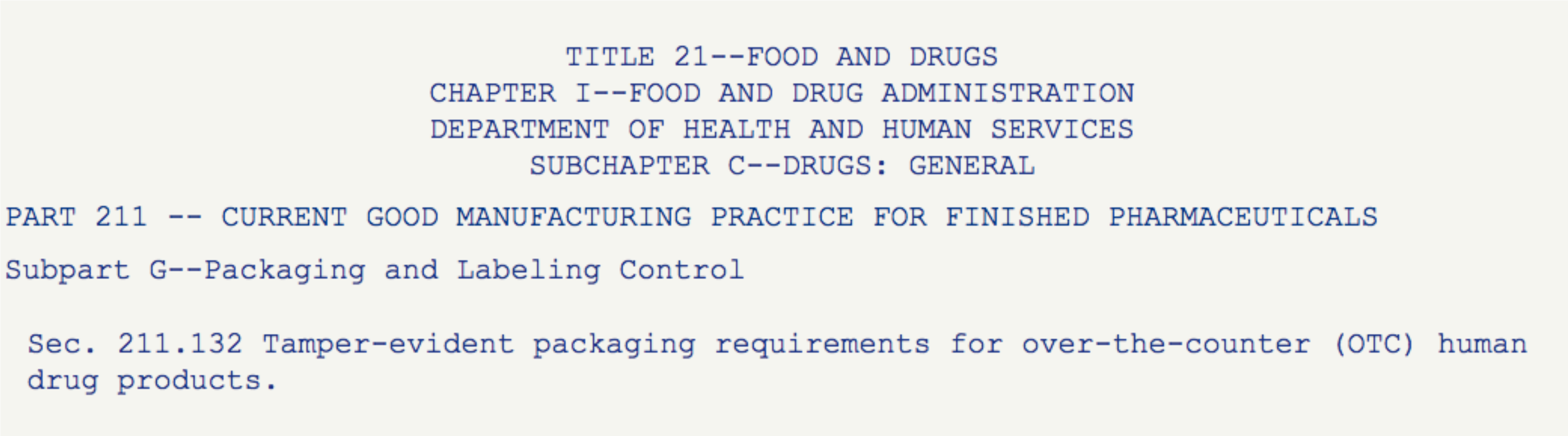
Email | Print | Single Page | Yahoo! Buzz | ShareThis Text size − +

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.

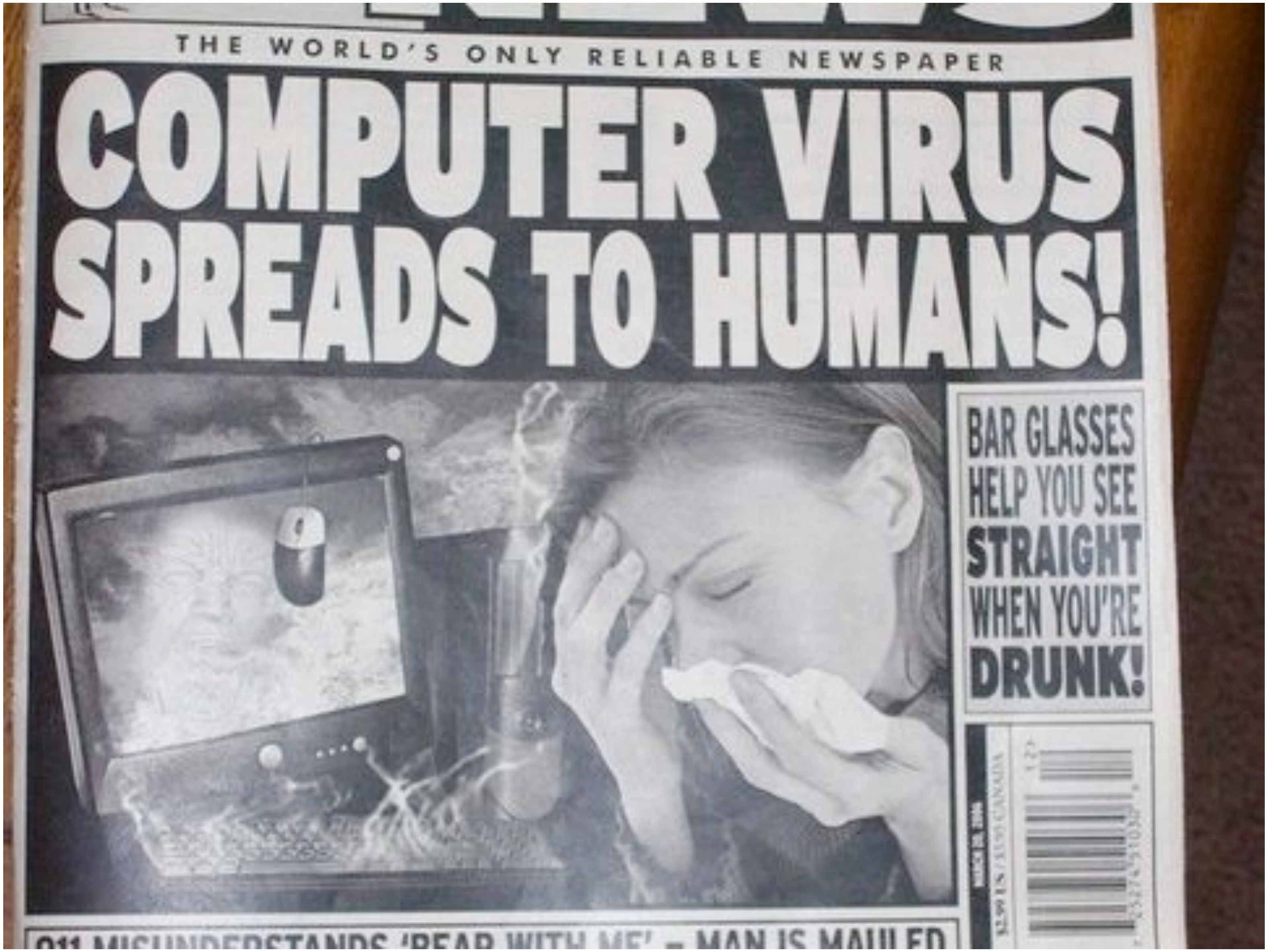
(a)General. The Food and Drug Administration has the authority under the Federal Food, Drug, and Cosmetic Act (the act) to establish a uniform national requirement for tamper-evident packaging of OTC drug products that will **improve the security** of OTC drug packaging

Administrative issues:

Insufficient software/security expertise available to FDA

Technical issues

Achoo!



THE WORLD'S ONLY RELIABLE NEWSPAPER

COMPUTER VIRUS SPREADS TO HUMANS!

BAR GLASSES HELP YOU SEE STRAIGHT WHEN YOU'RE DRUNK!

$2.99 US / $3.59 CANADA

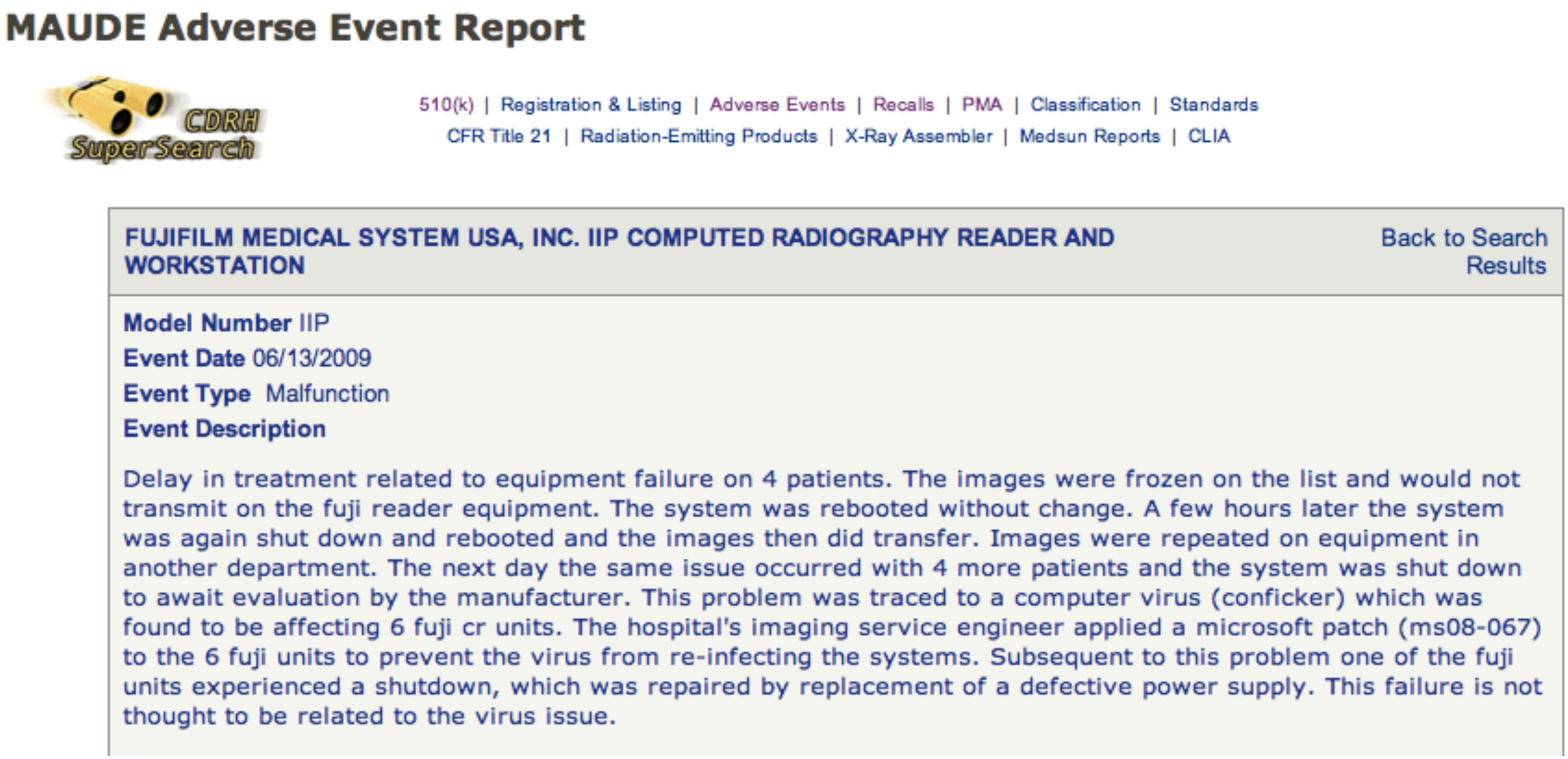
911 MISUNDERSTANDS 'BEAR WITH ME' – MAN IS MAULED

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

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

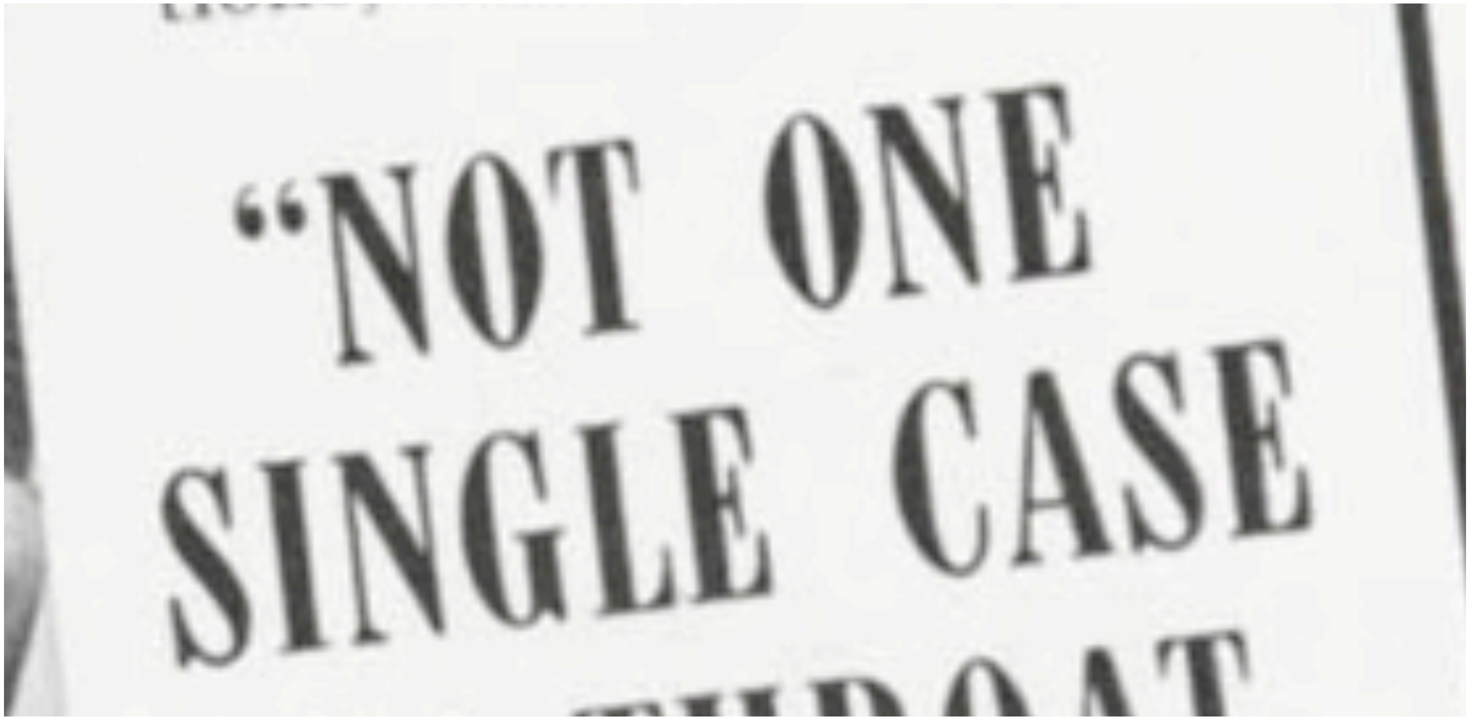
Back to Search Results

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.

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

Information Assurance or Bliss?



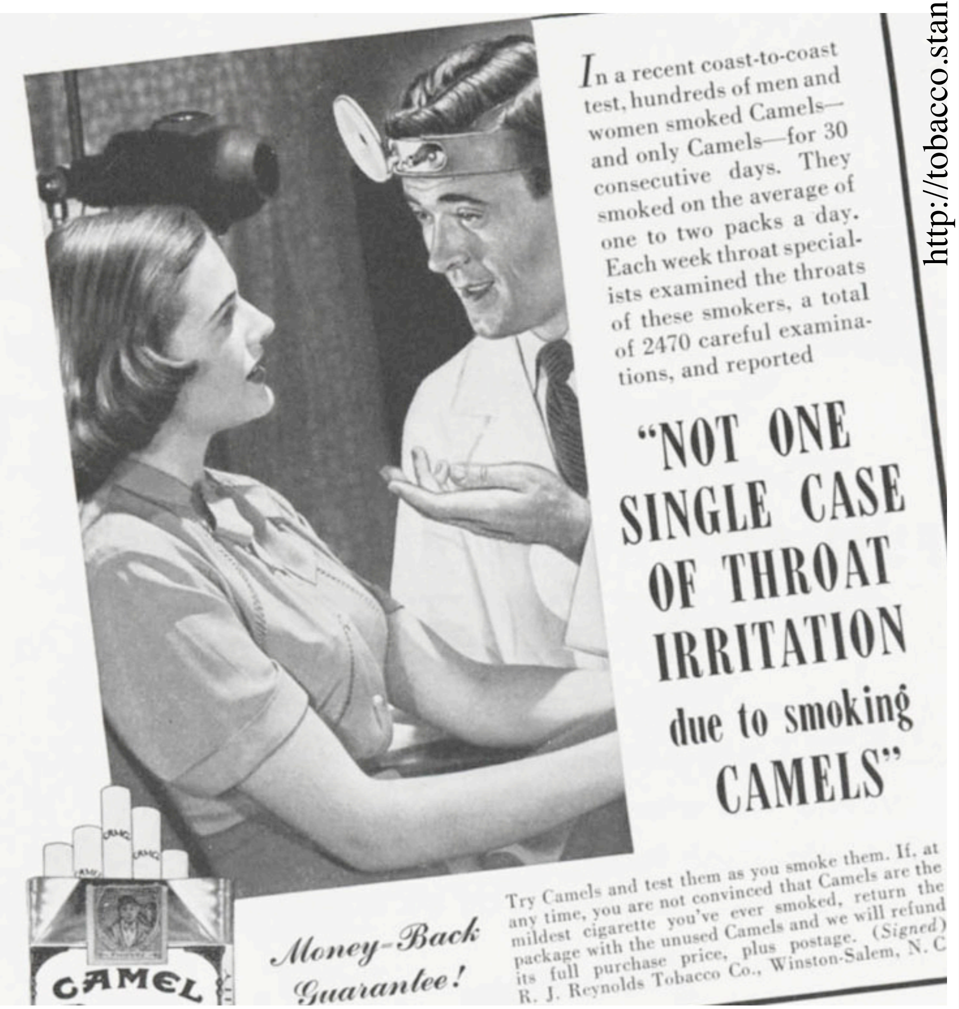
“NOT ONE SINGLE CASE THROAT

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]



In a recent coast-to-coast test, hundreds of men and women smoked Camels—and only Camels—for 30 consecutive days. They smoked on the average of one to two packs a day. Each week throat specialists examined the throats of these smokers, a total of 2470 careful examinations, and reported

“NOT ONE SINGLE CASE OF THROAT IRRITATION due to smoking CAMELS”

Money-Back Guarantee!

Try Camels and test them as you smoke them. If, at any time, you are not convinced that Camels are the mildest cigarette you've ever smoked, return the package with the unused Camels and we will refund its full purchase price, plus postage. (*Signed*) R. J. Reynolds Tobacco Co., Winston-Salem, N. C

http://tobacco.stanford.edu/

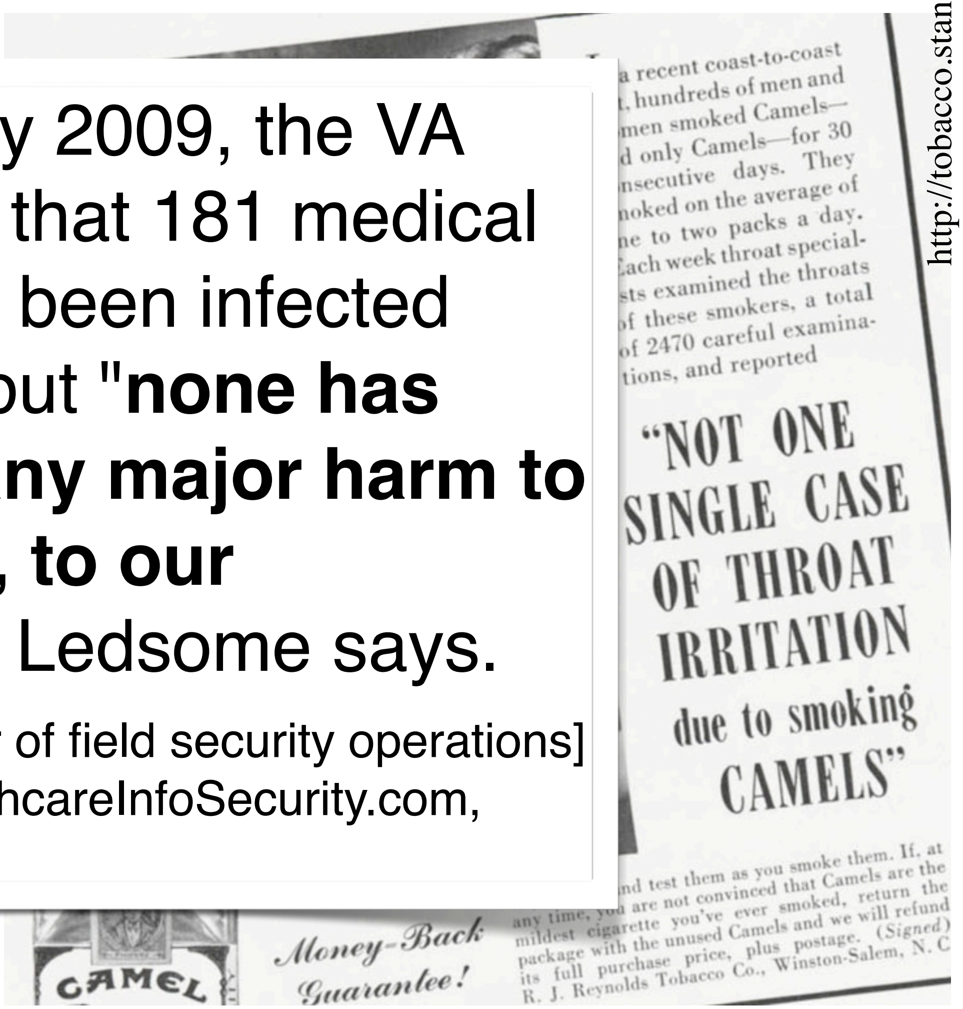
Information Assurance or Bliss?

“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]



a recent coast-to-coast
, hundreds of men and
men smoked Camels—
d only Camels—for 30
nsecutive days. They
noked on the average of
ne to two packs a day.
Each week throat special-
sts examined the throats
of these smokers, a total
of 2470 careful examina-
tions, and reported

“NOT ONE SINGLE CASE OF THROAT IRRITATION due to smoking CAMELS”

nd test them as you smoke them. If, at any time, you are not convinced that Camels are the mildest cigarette you've ever smoked, return the package with the unused Camels and we will refund its full purchase price, plus postage. (Signed) R. J. Reynolds Tobacco Co., Winston-Salem, N. C.

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

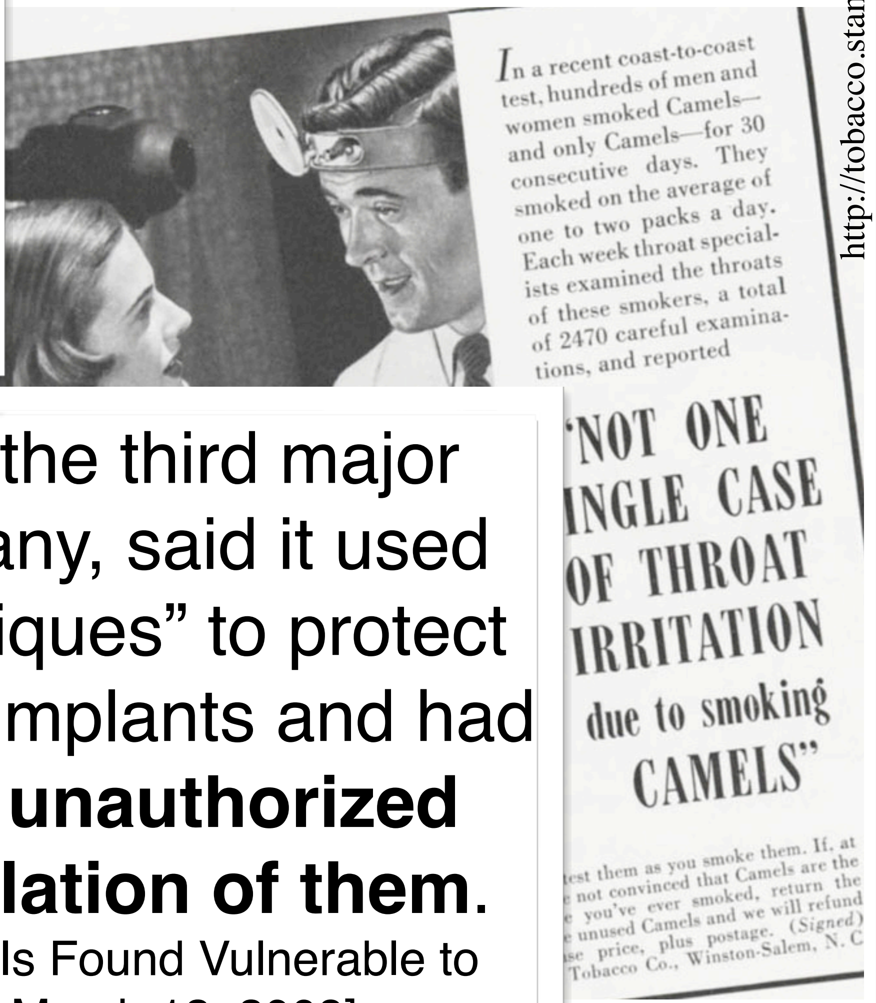
[B. Feder, "A Heart Device Is Found Vulnerable to Hacker Attacks" NY Times, March 12, 2008]

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]

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]



In a recent coast-to-coast test, hundreds of men and women smoked Camels—and only Camels—for 30 consecutive days. They smoked on the average of one to two packs a day. Each week throat specialists examined the throats of these smokers, a total of 2470 careful examinations, and reported

test them as you smoke them. If, at e not convinced that Camels are the e you've ever smoked, return the e unused Camels and we will refund ase price, plus postage. (*Signed*) Tobacco Co., Winston-Salem, N. C

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]

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**.

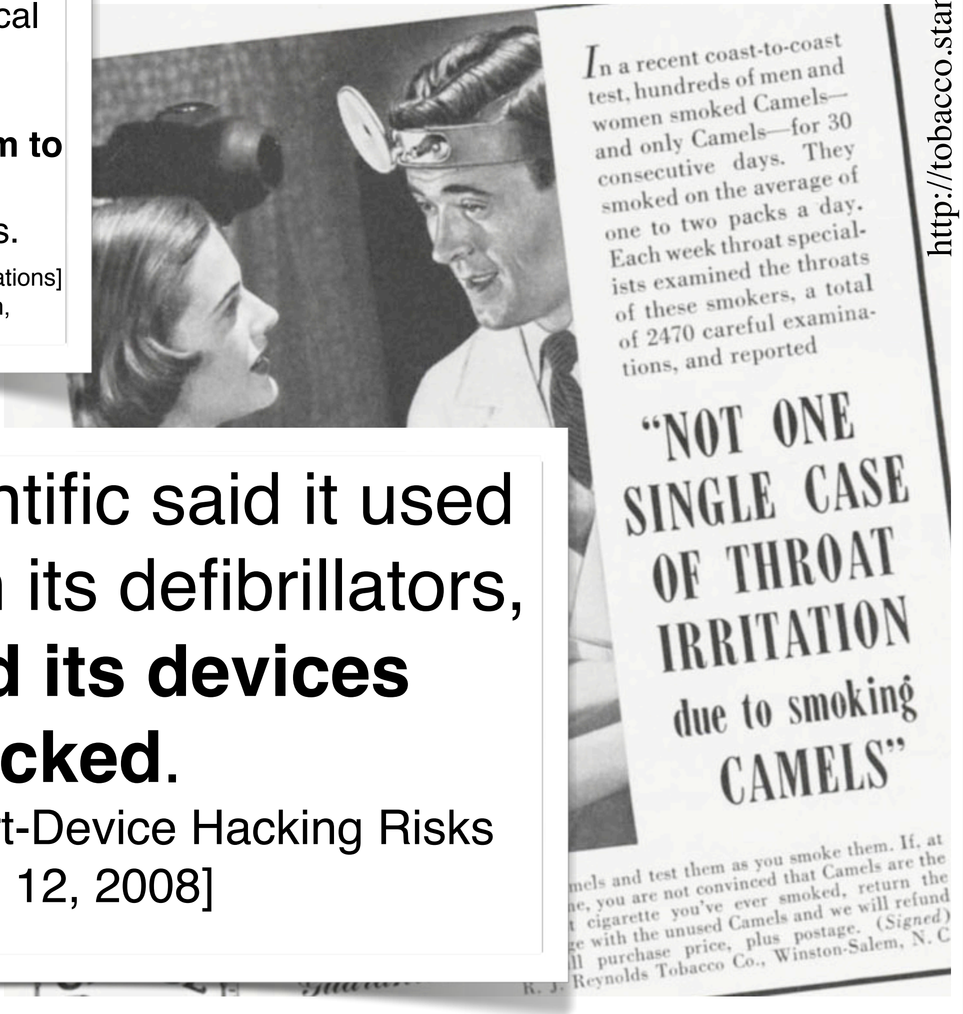
[B. Feder, “A Heart Device Is Found Vulnerable to Hacker Attacks” NY Times, March 12, 2008]

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]

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]



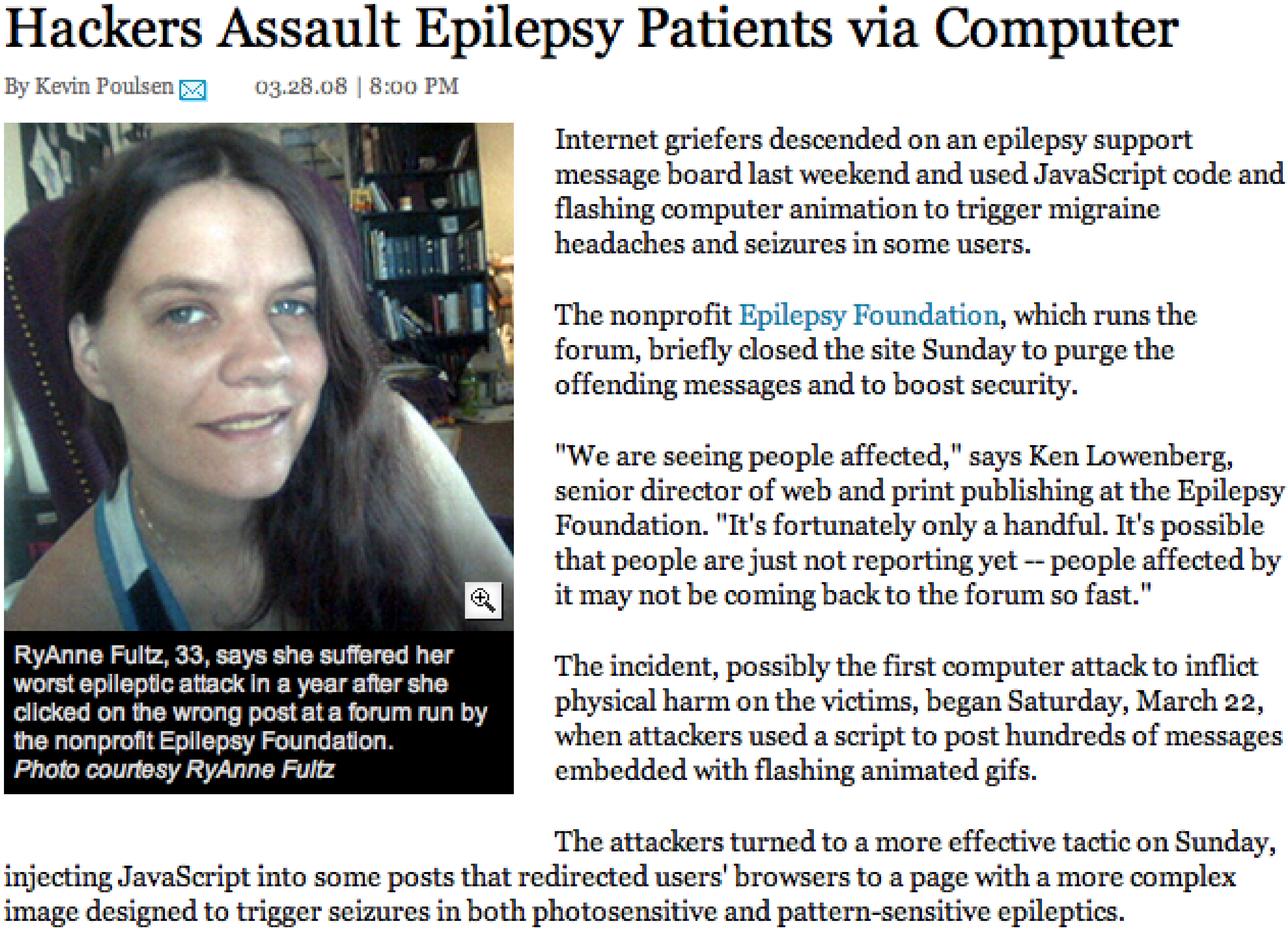
In a recent coast-to-coast test, hundreds of men and women smoked Camels—and only Camels—for 30 consecutive days. They smoked on the average of one to two packs a day. Each week throat specialists examined the throats of these smokers, a total of 2470 careful examinations, and reported

“NOT ONE SINGLE CASE OF THROAT IRRITATION due to smoking CAMELS”

mels and test them as you smoke them. If, at
ne, you are not convinced that Camels are the
t cigarette you’ve ever smoked, return the
ge with the unused Camels and we will refund
ll purchase price, plus postage. (Signed)
R. J. Reynolds Tobacco Co., Winston-Salem, N. C

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.

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

BOBBY SMITH, M.D.
You're, I think, probably about ready to
test the device for effectiveness. Is that

Photos: Medtronic; Video: or-live.com

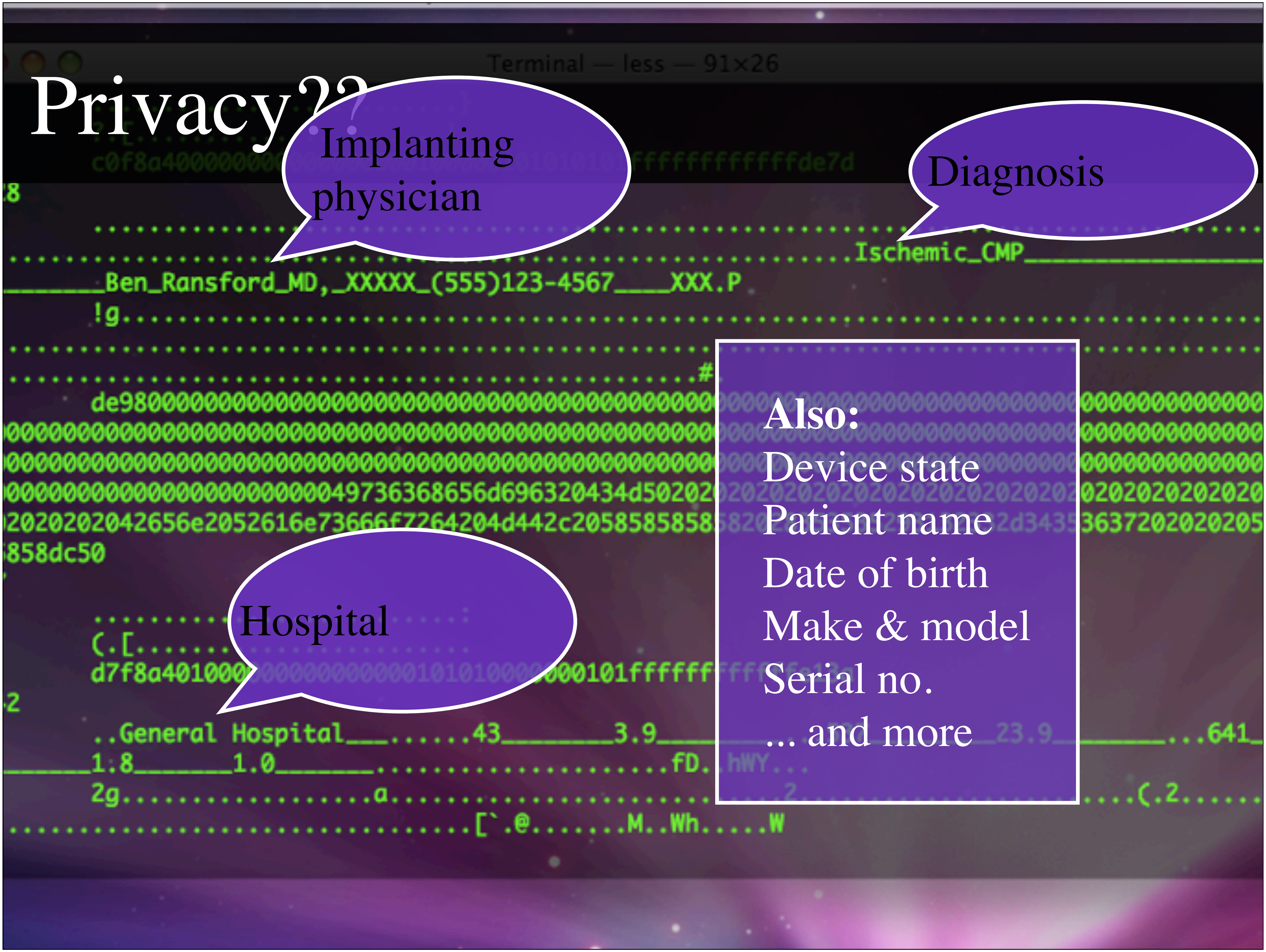
Implantation Scenario

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

Home monitor

Photos: Medtronic; Video: or-live.com

Privacy??

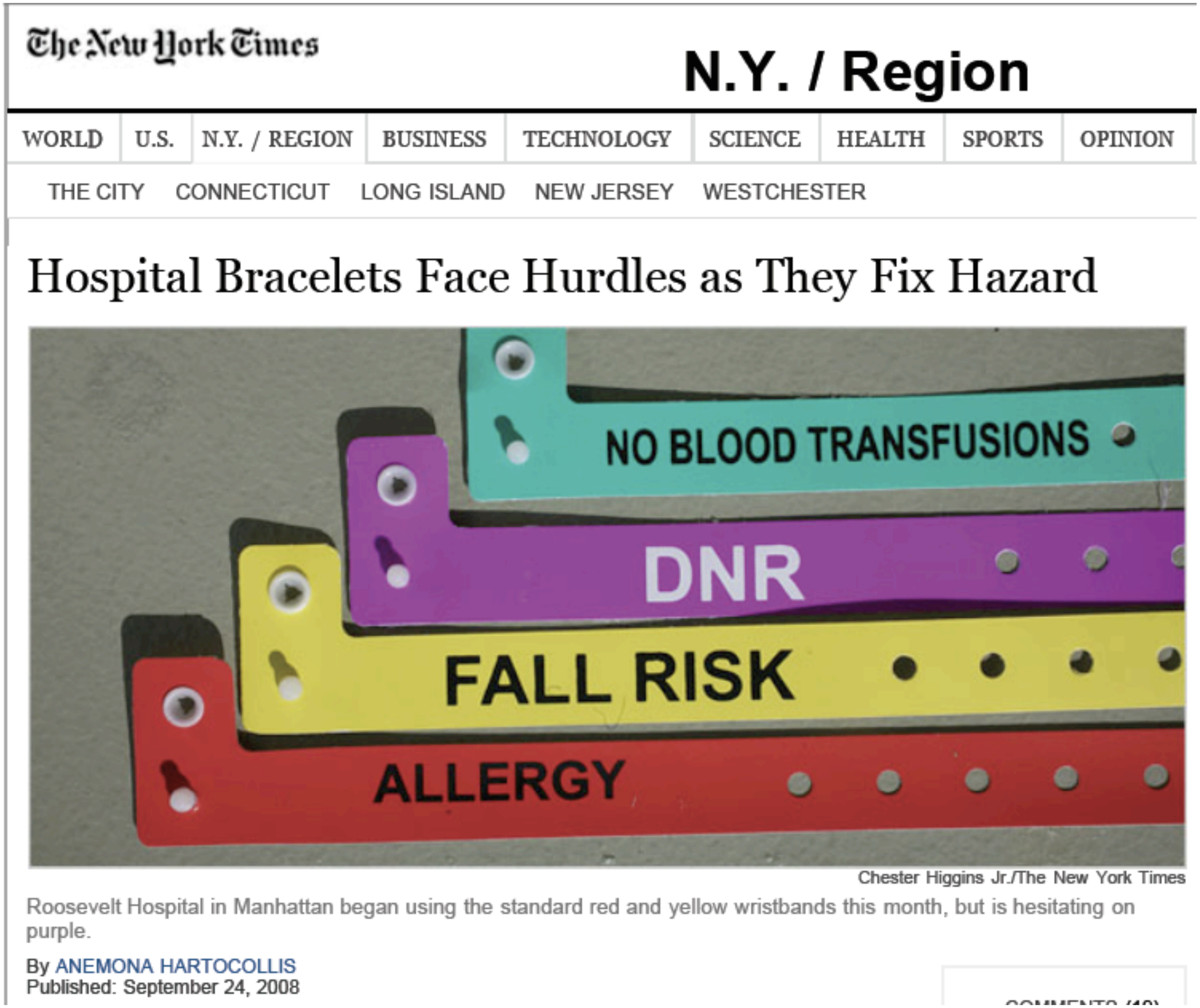


```
c0f8a40000000000                01010101ffffffffffffde7d
:8
     ...........................................................................
.................................................................Ischemic_CMP____________
______Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
     !g.............................................................................
...............................................................................
...................................................#.
     de980000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000497363686564696320434d502020202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c2058585858582                    2d3435363720202020205
858dc50

     .........                 ........
     (.[.......              ..................
     d7f8a401000000000000000001010100000000101ffffffffff
2
     ..General Hospital___......43________3.9____                 23.9________...641_
______1.8_______1.0_______.......................fD..hWY...
     2g...................a..................................2.......................(.2......
................................[`.@.......M..Wh.....W
```

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

Wardrobe Malfunctions



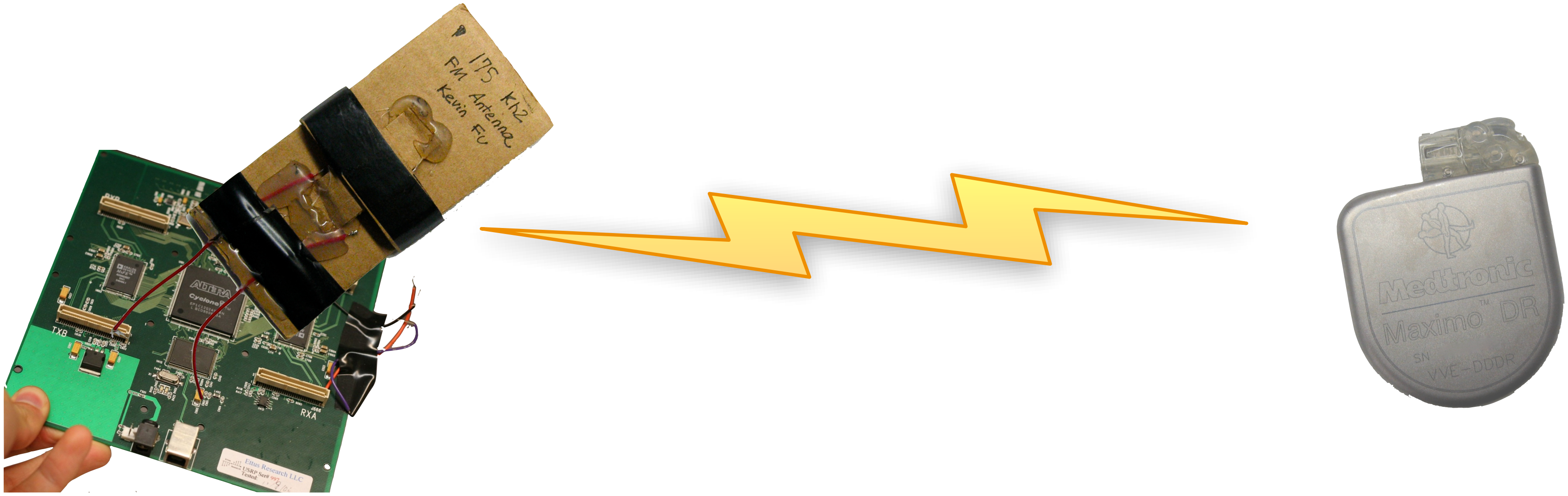
Hospital Bracelets Face Hurdles as They Fix Hazard

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]

Technical issues

Vulnerabilities are in plain sight.

When will risk become a tangible threat?

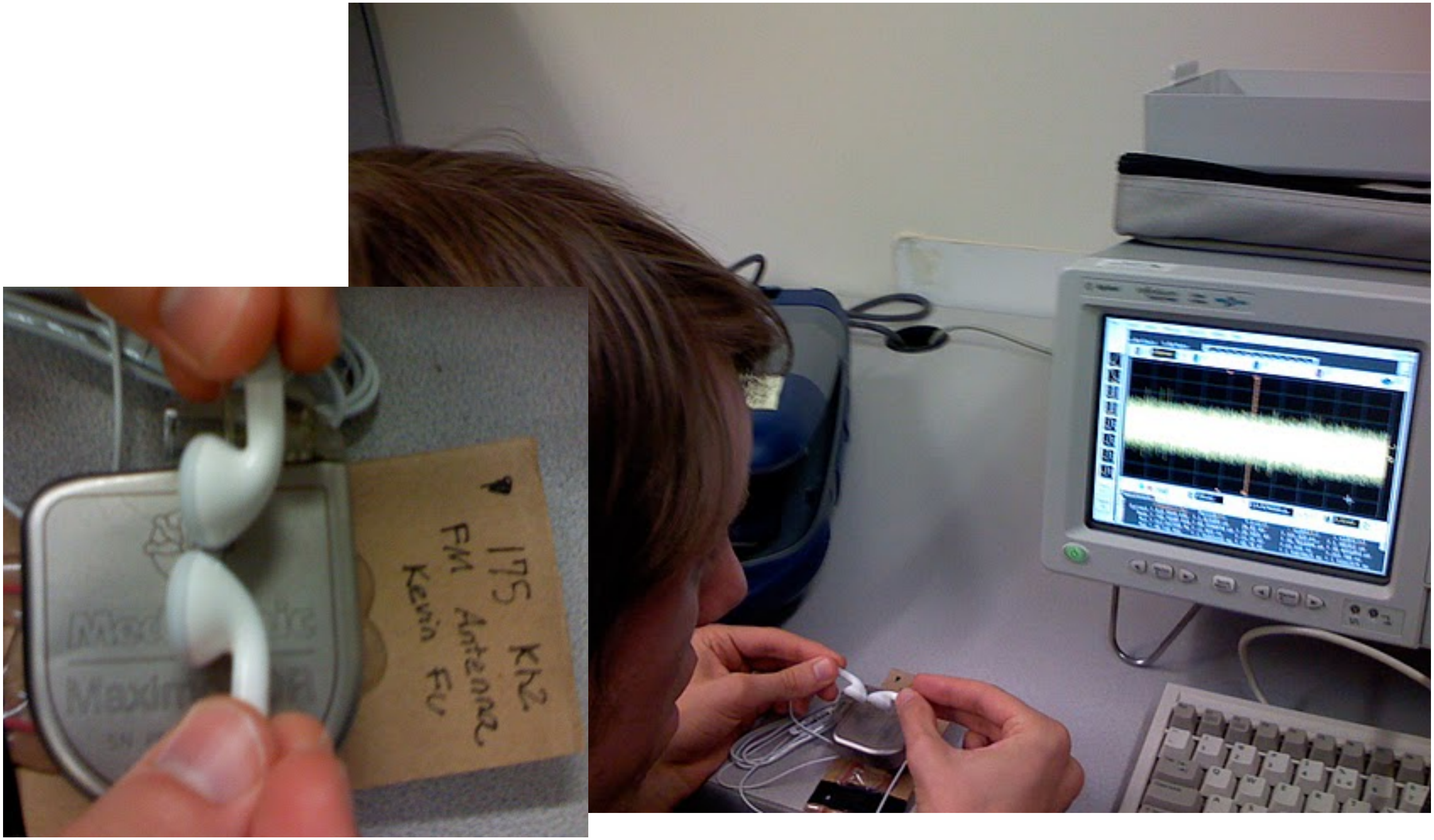
← Ways Forward? ↗

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

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.]

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

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

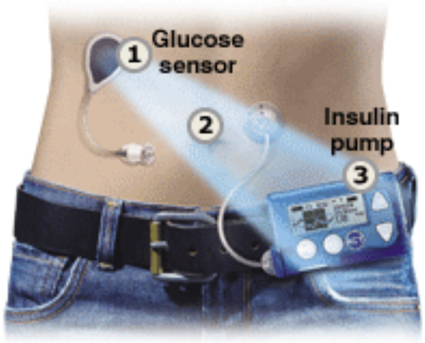
OPEN
MEDICAL
DEVICE
RESEARCH
LIBRARY

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

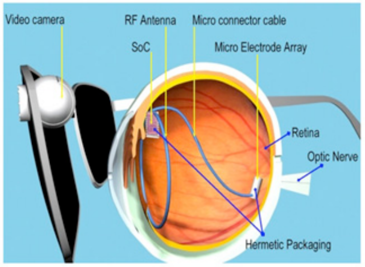
But not without fully understanding trustworthy computing



Insulin pump

Artificial pancreas

Neurostimulators



Artificial vision

Obesity control

Programmable
Vasectomy

Photos: Medgadget

Further Reading

- 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. To appear.
- 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. To appear.
- 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