IoT Security & Medical Devices, Oh My: 💩😵

Kevin Fu

Associate Professor
Computer Science & Engineering
University of Michigan

web.eecs.umich.edu/~kevinfu/
kevinfu@umich.edu

SPQR

Supported in part by NSF CNS-1330142. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

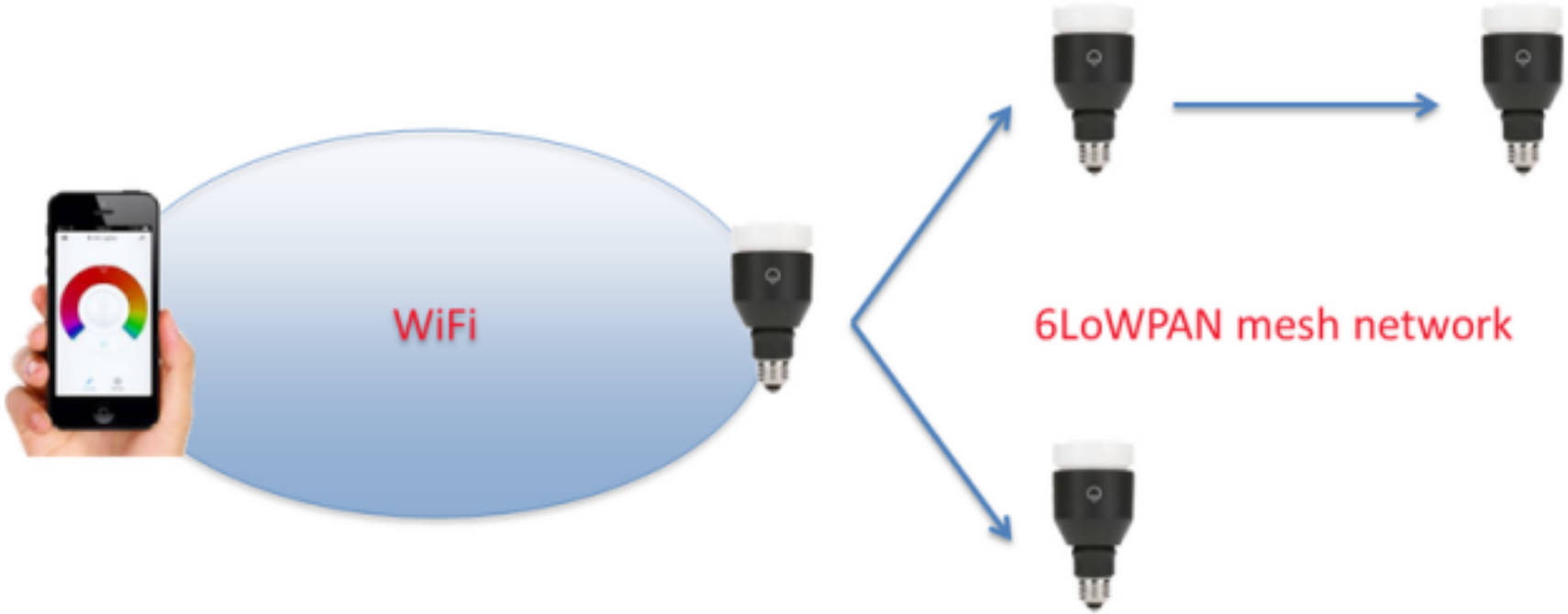
RISK ASSESSMENT / SECURITY & HACKTIVISM

Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords

More evidence the Internet of things treats security as an afterthought.

by **Dan Goodin** - July 7 2014, 3:20pm EDT

HACKING SMART HOME 90



Context

The New York Times

PRIVACY

Samsung Tweaks Television Policy Over Privacy Concerns

By **Nick Wingfield**

February 10, 2015 5:23 pm

After an outcry over privacy concerns, Samsung has clarified that some of its so-called smart televisions listen in on the conversations of viewers only if the viewers permit the devices to do so.

Samsung responded to an uproar that began after the company recently updated a privacy policy for its Internet-connected Smart TV line of sets. The new language implied that Samsung eavesdrops on its users, describing in one sentence a voice recognition capability that allows viewers to operate their televisions with verbal commands.

“Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition,” the sentence said.

Microsoft update mayhem delays German basketball game, costs team dear

17 minutes waiting proved to be just a bit too long

Erstwhile Microsoft boss Steve Ballmer likes a slam dunk, but still ...

31 Mar 2015 at 11:41, Jennifer Baker

What's the worst thing that could happen when your Windows update takes longer than expected? Ask the Paderborn Finke Baskets, a German pro basketball team who got relegated thanks to Windows' sluggish performance.

FDA issues recall of 465,000 St. Jude pacemakers to patch security holes

Heart patients will have to visit their doctors to have their pacemakers patched for the "voluntary" recall -- but there are risks.

By Charlie Osborne for Zero Day | August 30, 2017 -- 10:31 GMT (03:31 PDT) | Topic: Security

Important Cybersecurity Advisory

Information About Cybersecurity Firmware Update for Accent™/ Anthem™, Accent MRI™, Assurity™/ Allure™, and Assurity MRI™ devices

28 August, 2017

Dear Doctor,

We are advising you of the availability of new pacemaker firmware (a type of software) that is intended to address the risk of unauthorized access to our pacemakers that utilize radio frequency (RF) communications (i.e., Accent™/ Anthem™, Accent MRI™, Assurity™/ Allure™, and Assurity MRI™). This firmware update provides an additional layer of security against unauthorized access to these devices that further reduces the potential for a successful cybersecurity attack.

BOINGBOING / CORY DOCTOROW / 7:48 AM WED

Powerful Russian Orthodox cleric summoned to spritz computers with holy water to fight ransomware

Carson Block has a new short, and his reasoning is super creepy

LINETTE LOPEZ
10H

Muddy Waters, the firm founded by noted short-seller Carson Block, is short St. Jude Medical Inc.

The stock is down almost 7% on the news.

The firm says it's shorting St. Jude because its pacemakers are faulty and susceptible to cyberattacks.

St. Jude stock tumbles as report questions company's cybersecurity

Short seller says half of firm's revenue may be at stake; St. Jude said report "absolutely untrue."

By Joe Carlson (http://www.startribune.com/joe-carlson/271816721/) Star Tribune

AUGUST 25, 2016 — 9:03PM

~$1 billion drop
August 2016

THE HILL

Researchers: Evidence St. Jude report might not be accurate

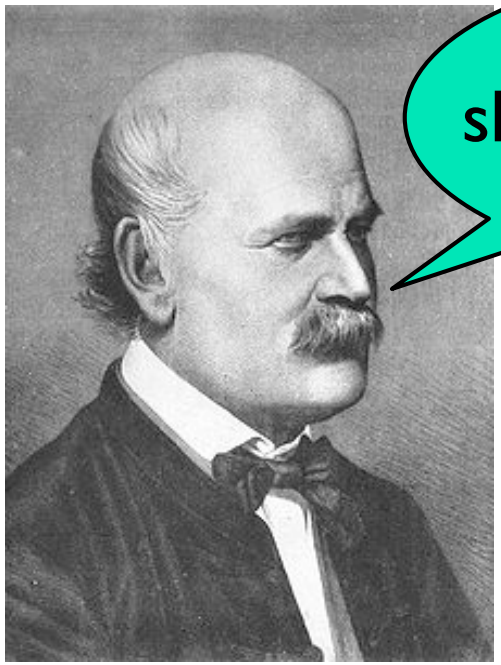
By Joe Uchill - 08/30/16 03:43 PM EDT

A prominent medical-device security expert tried to reproduce a purported hack of St. Jude Medical pacemakers and came to what a university press release called “strikingly different conclusions.”

University of Michigan associate professor Kevin Fu, along with the Archimedes Center for Medical Device Security that he heads, tried to recreate a “crash attack” listed in a controversial report released last week. What they found was evidence that the report is in error.

Semmelweis to Software Sepsis

1. Implantable medical devices should be trustworthy
2. Improved security will enable medical device innovation



Physicians should their wash hands.

Doctors are gentlemen and therefore their hands are always clean.

Dr. Ignaz Semmelweis
1818-1865

Dr. Charles Meigs
1792-1869

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

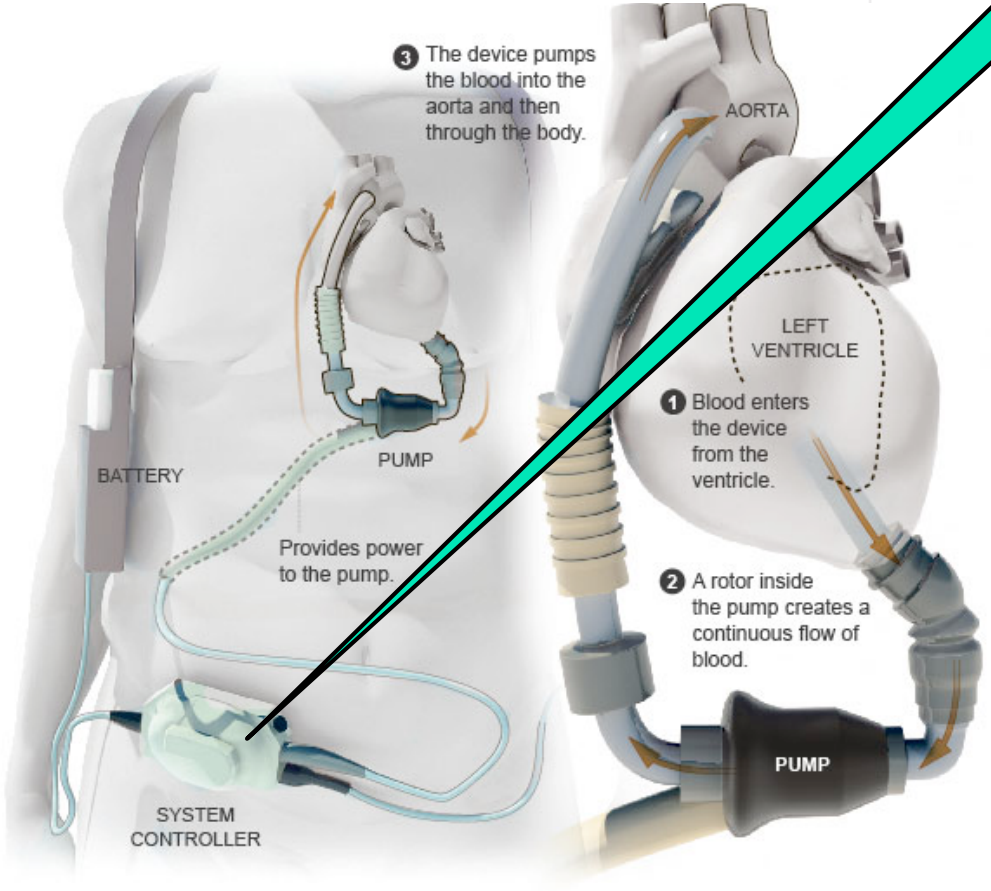
Benefits of Medical Device Software

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

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]

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]

First Internal Pacemaker

FDA approved ICD

Networking + Wireless !

1926

1960

1978

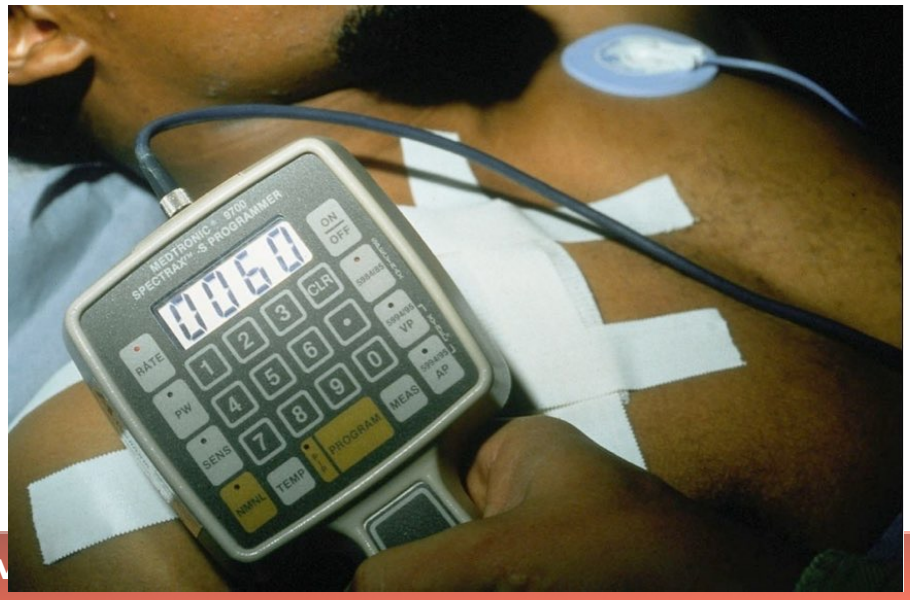
1985

2006

First Pacemaker

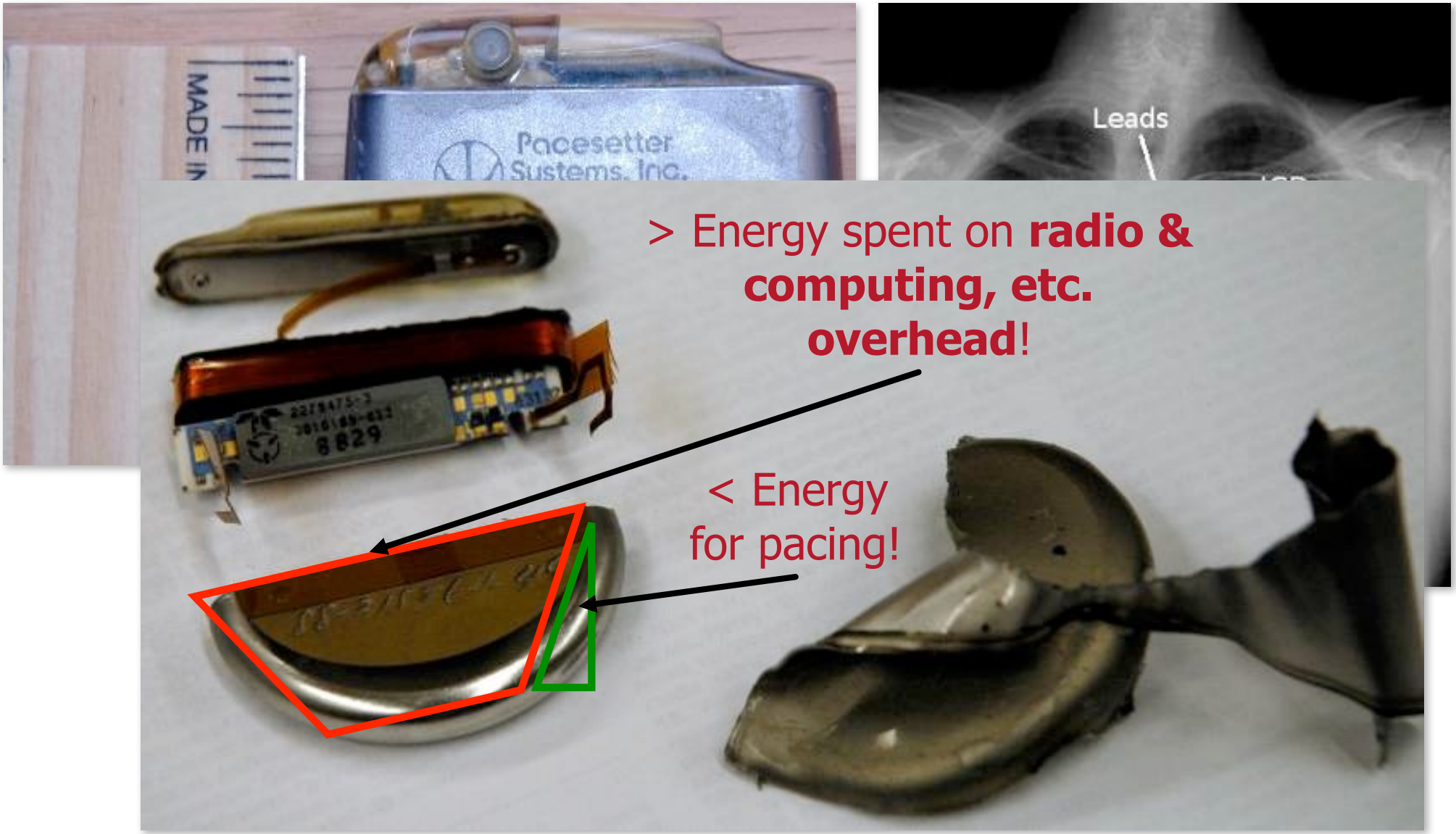
First Cochlear Implant Surgery

Wireless Blood Glucose Monitor



Photos from: Medtronic

Pacemakers: Regulate heartbeat



Wireless medical devices:

great benefits.

subtle inconvenient risks.

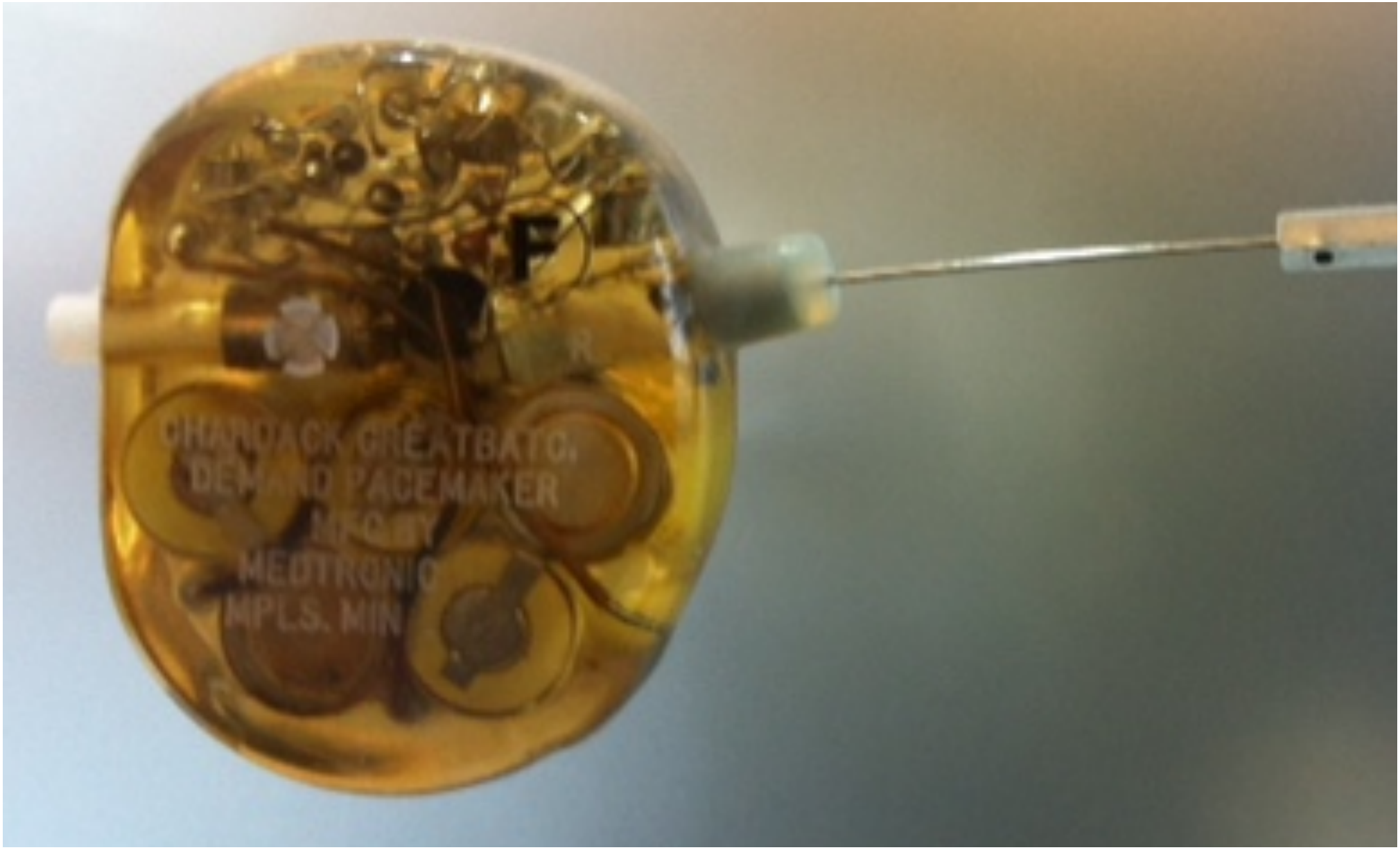
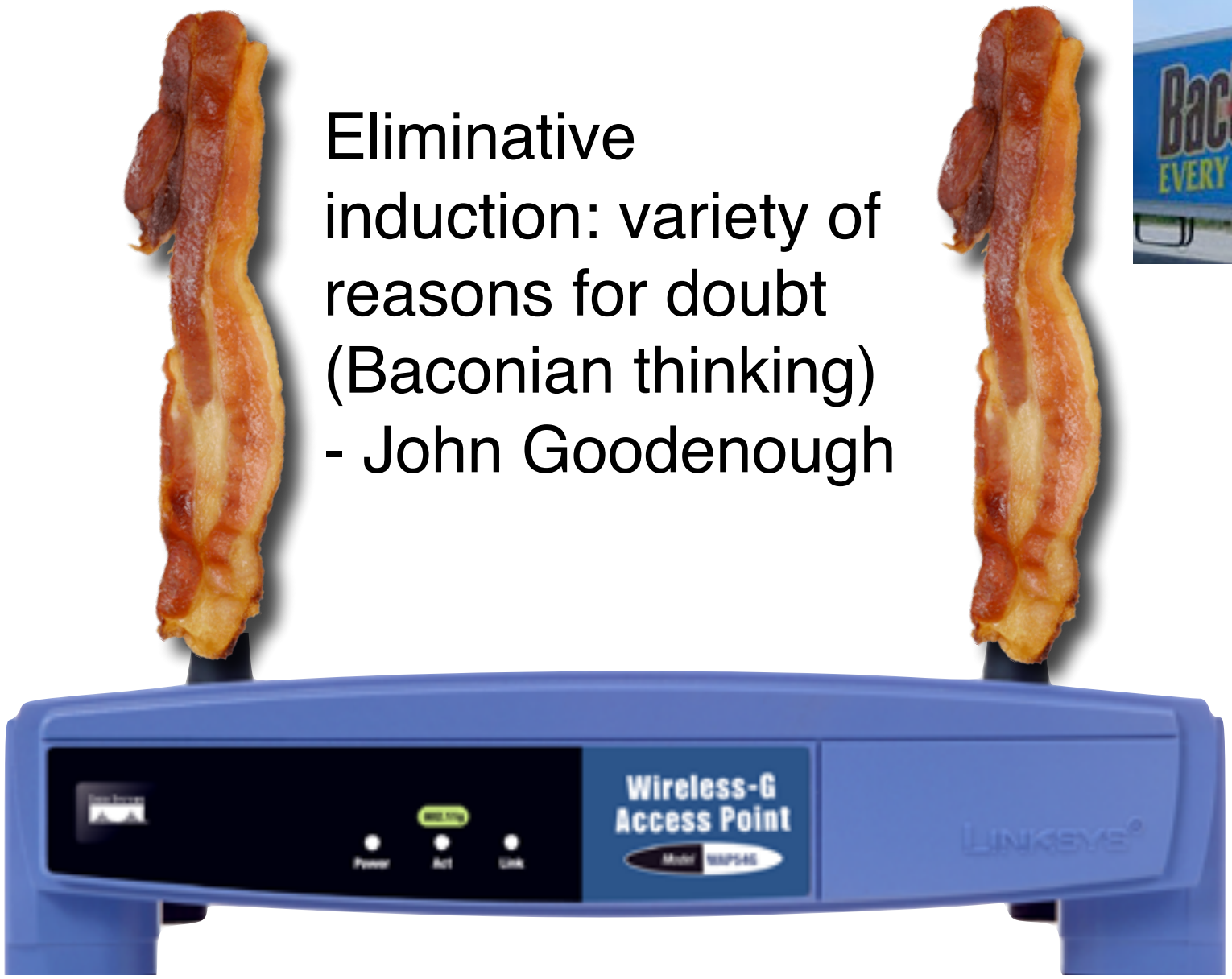


Photo by Kevin Fu @ Medtronic museum

Wireless Makes Everything Better?



Eliminative induction: variety of reasons for doubt (Baconian thinking)
- John Goodenough

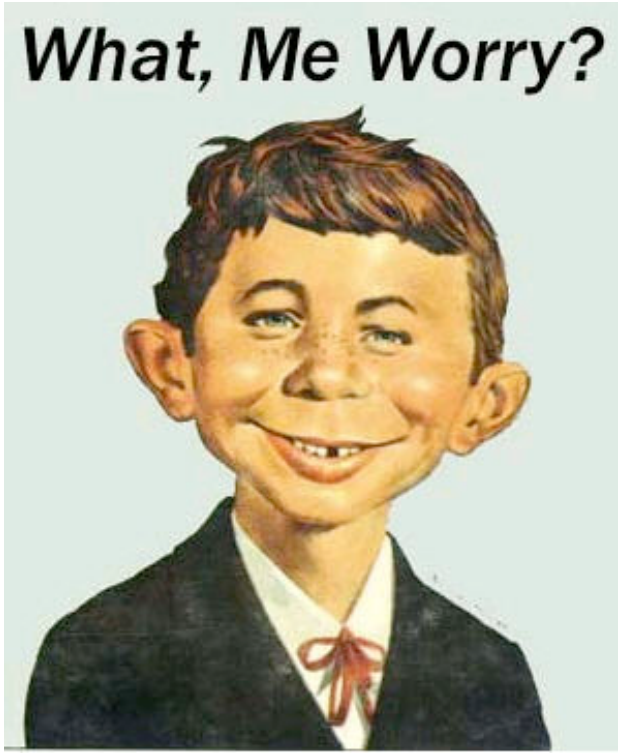
[Photos: uncyclopedia.wikia.com/wiki/Bacon & Cisco & bacondujour.blogspot.com]

"Safe, secure, and reliable **wireless medical device** systems require... focus on wireless performance, **security**, and EMC."
-Don Witters, FDA CDRH

Wireless Securi

- **Wireless security issues**
  - Open architecture
  - Multiple combinations of technology
  - Rogue wireless users
  - Health Insurance Portability and Accountability Act (HIPAA) issues
- **Wireless security considerations**
  - Authentication – to ensure authorized users
  - Encryption – to secure sensitive data and wireless links

What about **Internet**-related risks?



"These days, **everything is much safer**. It is easier to navigate thanks to modern technical instruments and the **Internet**."

-Captain Schettino, Captain of **Costa Concordia**

Shipwreck as seen from space.

Credit: DigitalGlobe

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

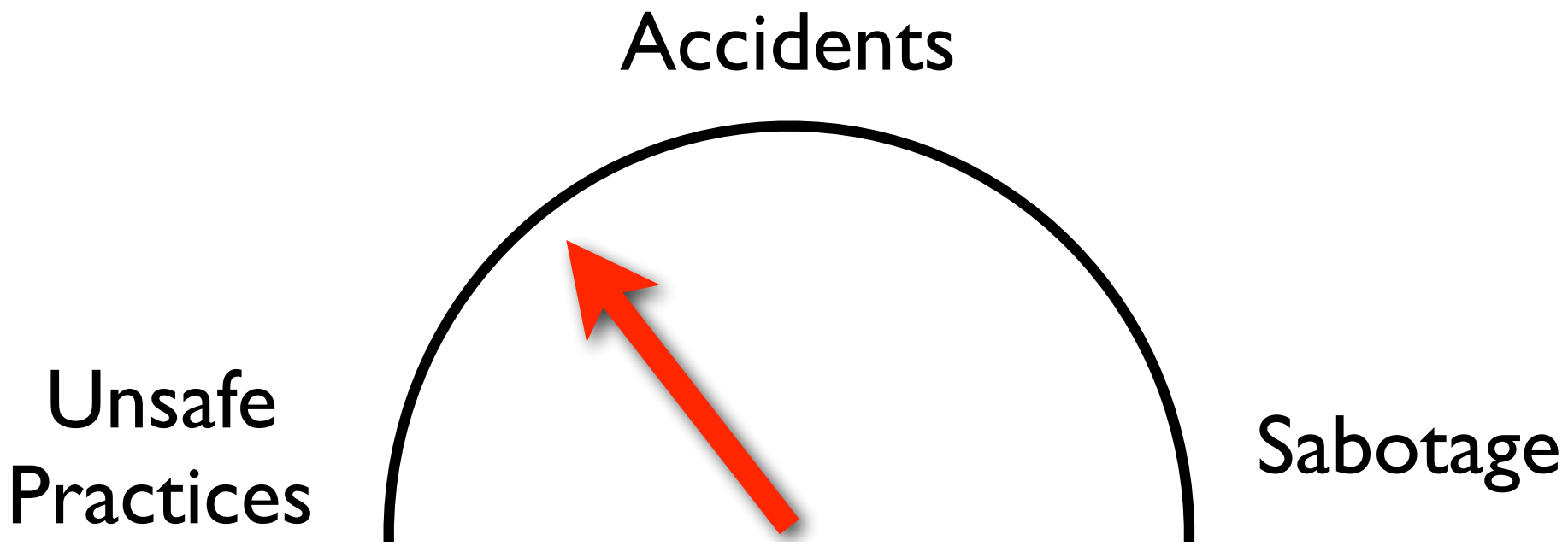
- Cannot be tested thoroughly

(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]

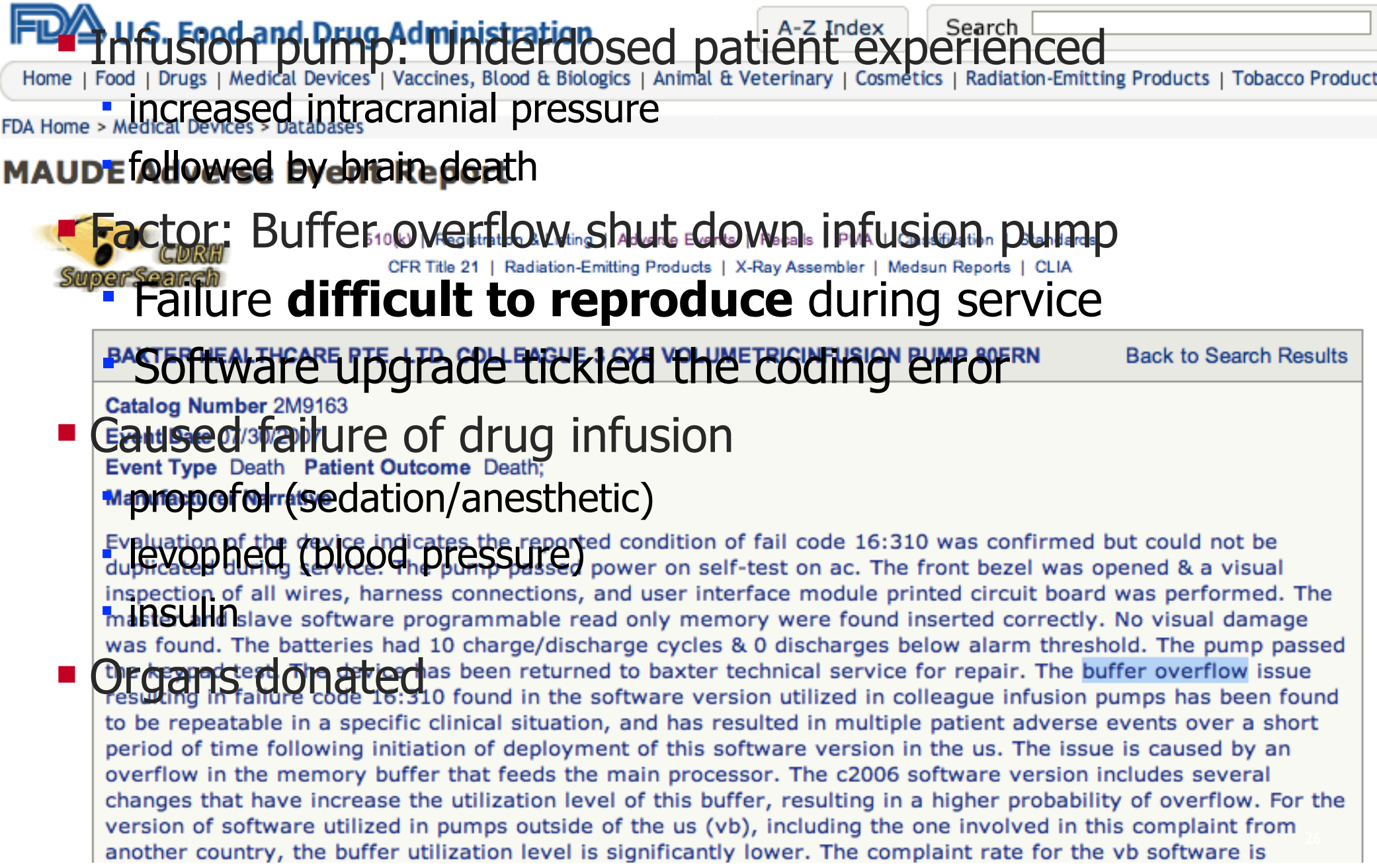
Accumulative Risks of…



Threat-o-meter

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
- Organs donated



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

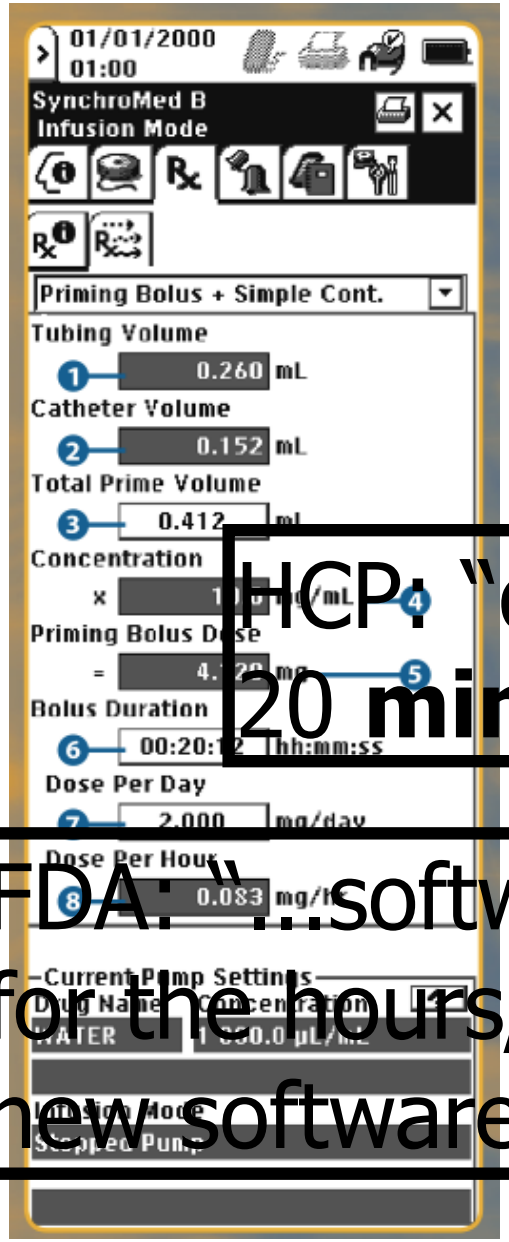
[US Recall News]

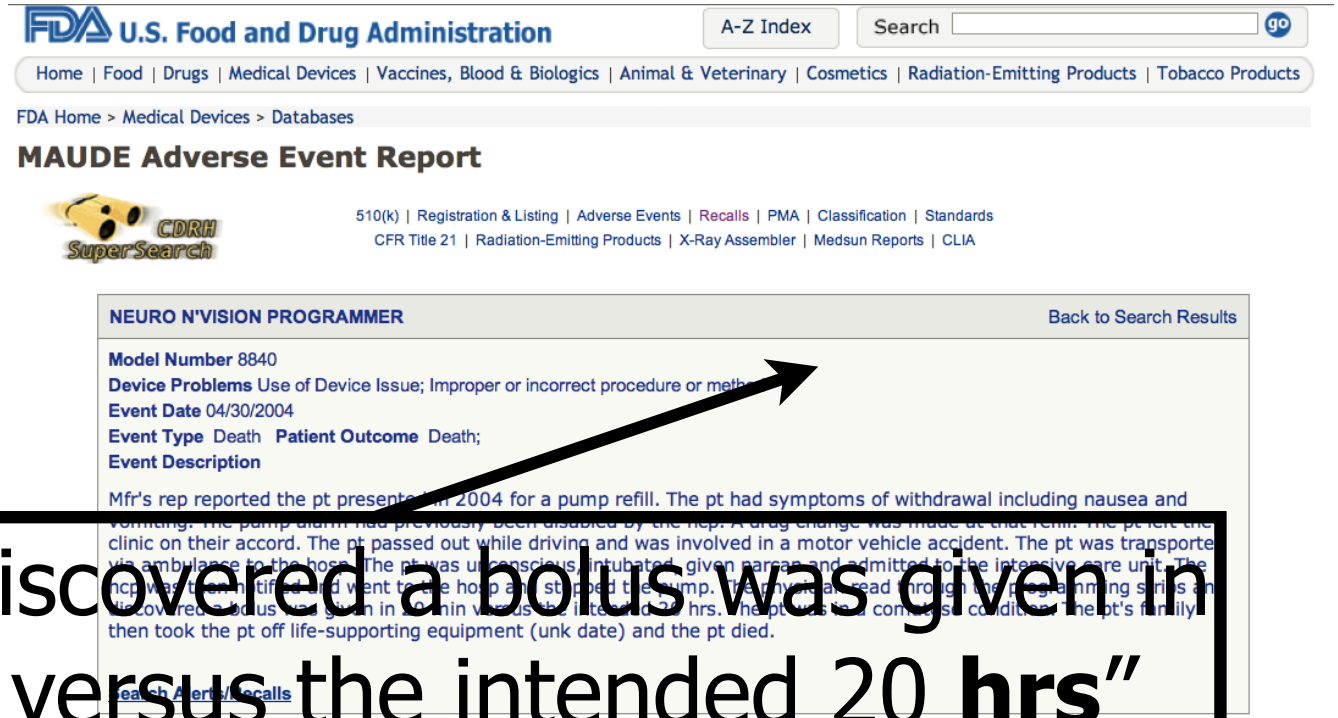
Pump+SW Problems=Deadly Cocktail

- "… 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]

User Interface: Timing is Everything





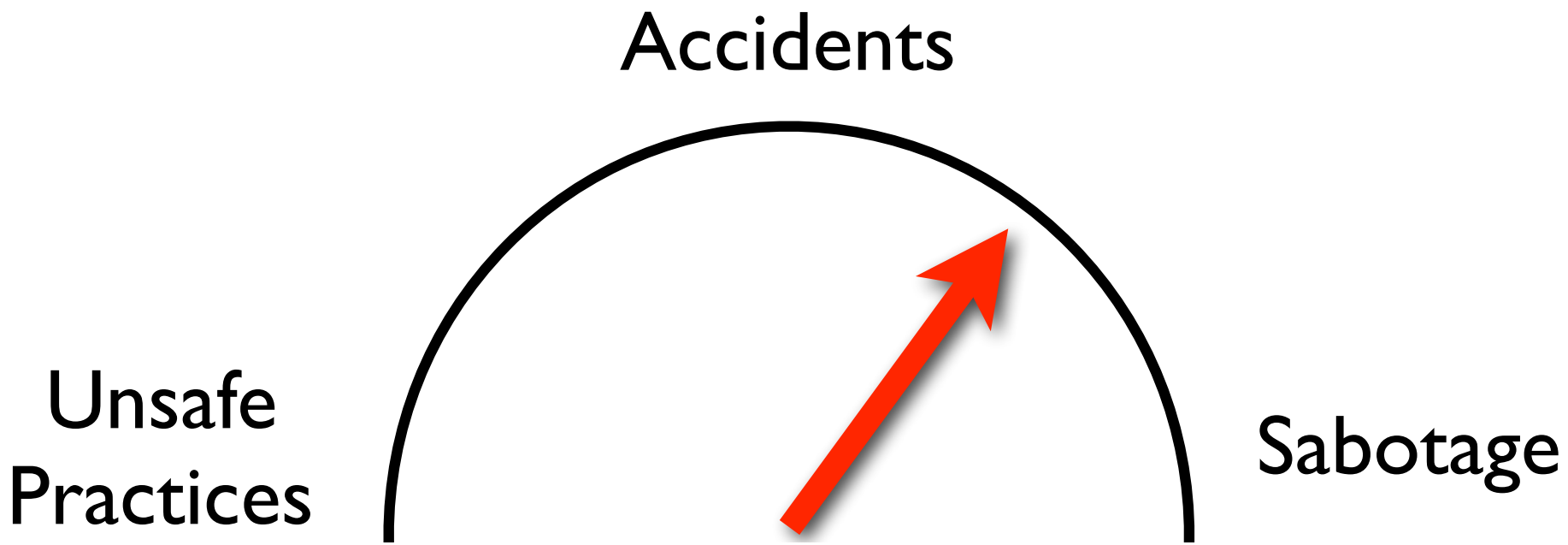
HCP: "discovered a bolus was given in 20 **min** versus the intended 20 **hrs**"

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

[Photos: Medtronic]

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

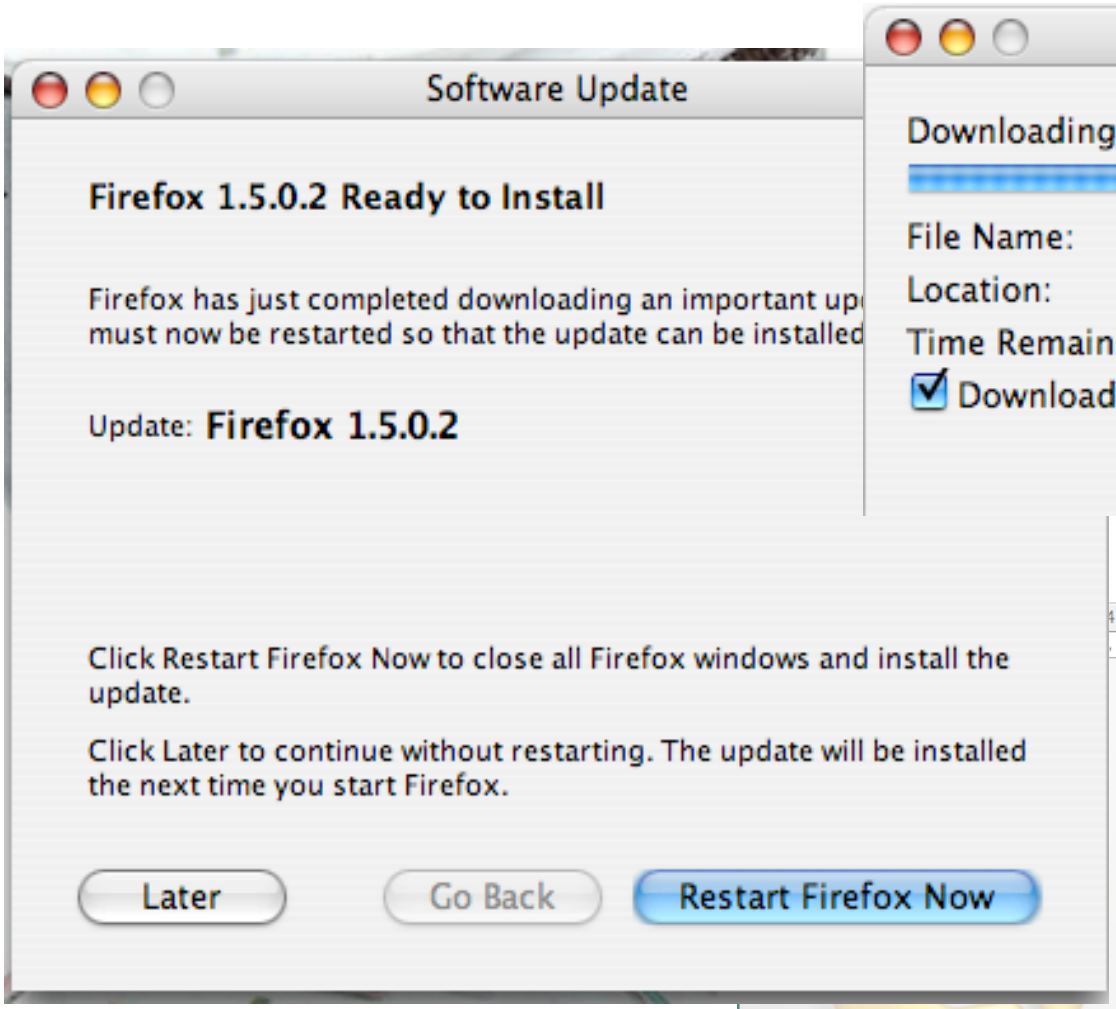
Accumulative Risks of…

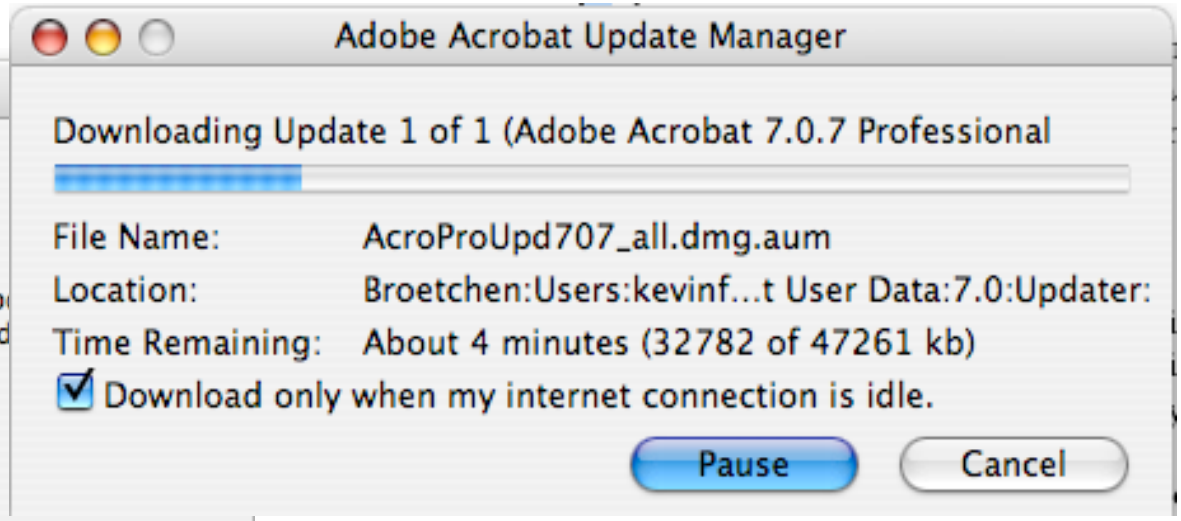


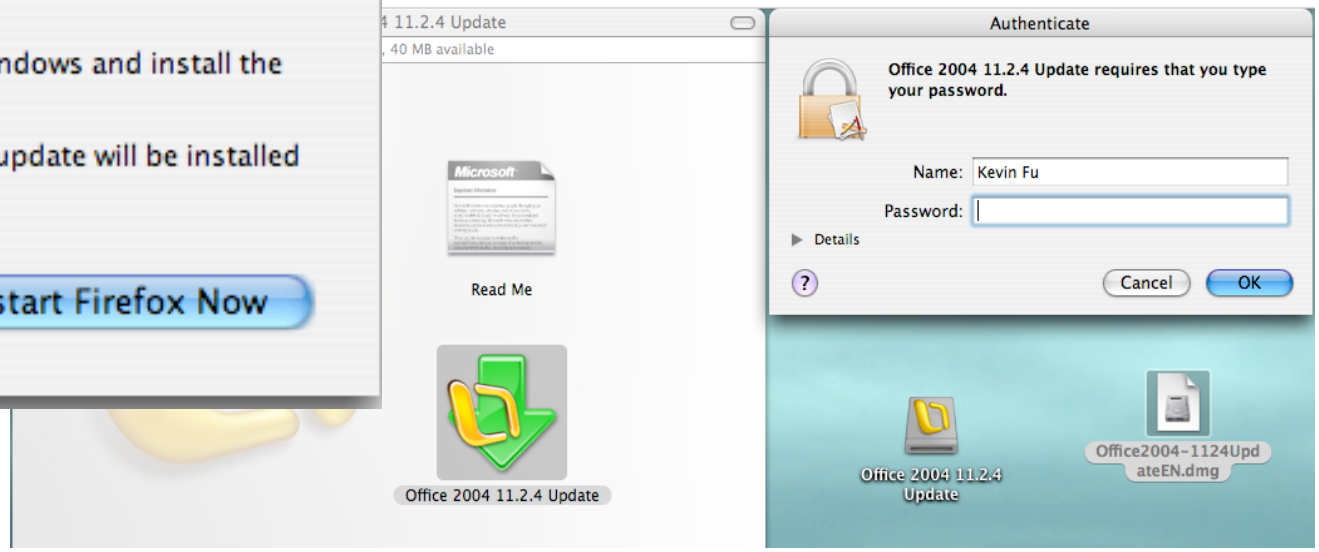
Threat-o-meter

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

WHAT?

What does end of support mean to customers?

It means you should take action. After April 8, 2014, there will be no new security updates, non-security hotfixes, free or paid assisted support options or online technical content updates.

Running Windows XP SP3 and Office 2003 in your environment after their end of support date may expose your company to potential risks, such as:

- **Security & Compliance Risks** - - Unsupported and unpatched environments are vulnerable to security risks. This may result in an officially recognized control failure by an internal or external audit body, leading to suspension of certifications, and/or public notification of the organization's inability to maintain its systems and customer information.
- **Lack of Independent Software Vendor (ISV) & Hardware Manufacturers support** — A recent industry report fro ap inn Wi of

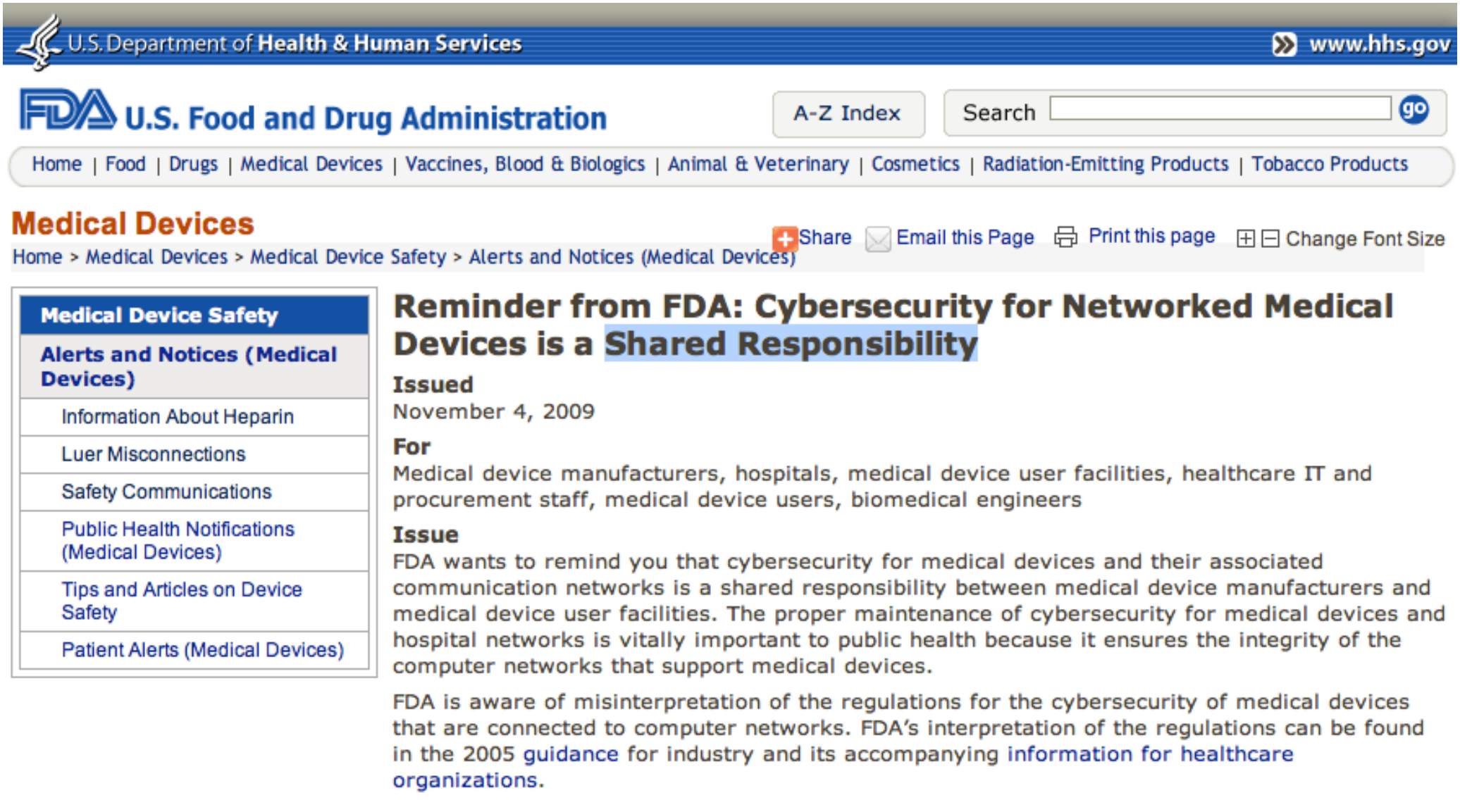
Get cu more fle security virtualiz rs d PC

Products Released	Lifecycle Start Date	Mainstream Support End Date	Extended Support End Date	Service Pack Support End Date
Windows XP Embedded	1/30/2002	1/11/2011	1/12/2016	10/22/2004
Windows XP Professional	12/31/2001	4/14/2009	4/8/2014	8/30/2005
Windows XP Service Pack 1	8/30/2002	Not Applicable	Not Applicable	10/10/2006

To help you get started in deploying a modern PC today, download the Microsoft Deployment Toolkit.
Download Free tool now.

How will Microsoft help customers?

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.

FDA Cybersecurity Guidance

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

---

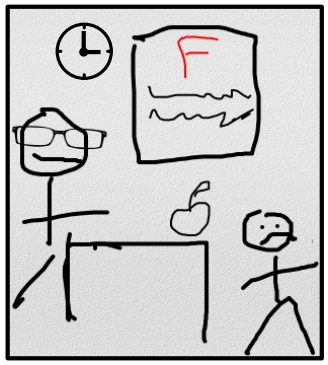
Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

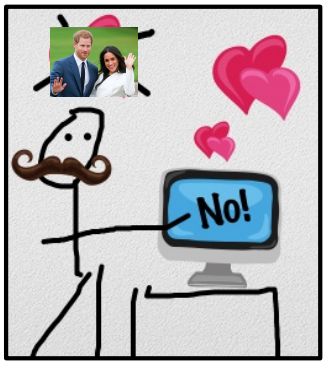
The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

Homework prevents me from passing class.



eHarmony prevents me from getting dates.



FDA rules prevent software updates.

BULLSHIT.

Get with the program.

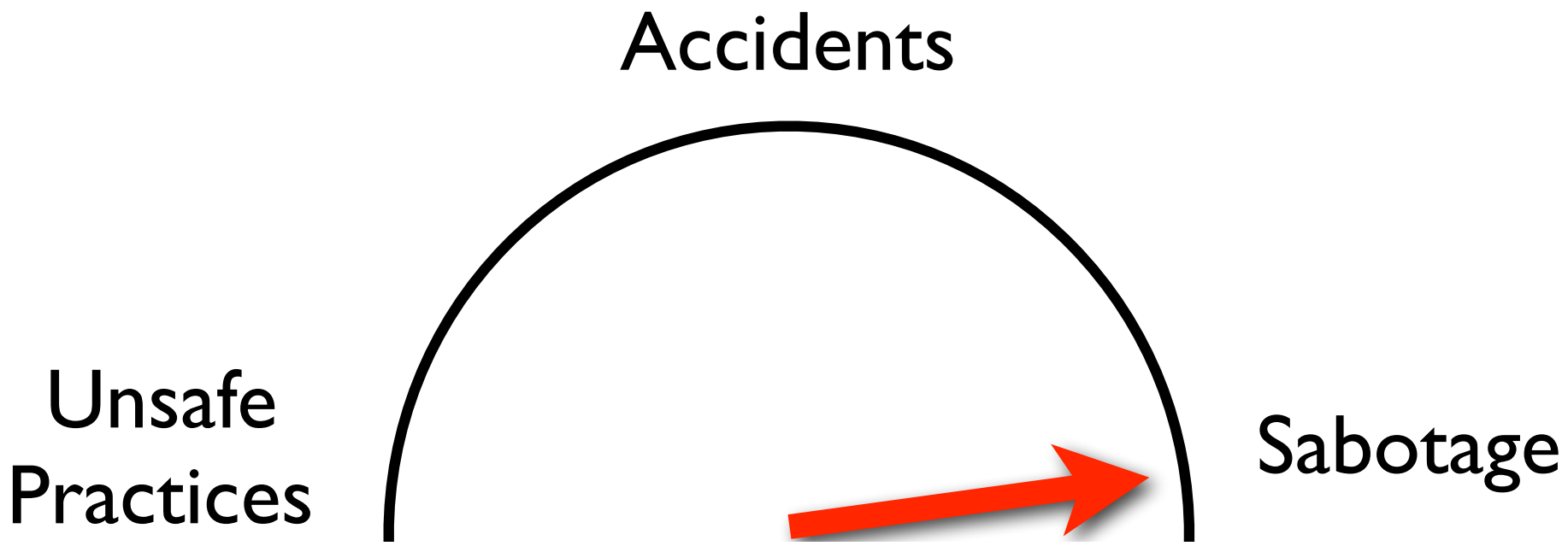
Distribute software updates regularly to address known vulnerabilities in Windows XP.

blog.secure-medicine.org

Managerial issues:
Diffusion of responsibility

Who's covered when
Secure Health IT hits the fan?

Foreseeable Cybersecurity Risks...



Foreseeable risk-o-meter

Short History: Medical Devices & SW

- Therac-25 analysis by Leveson & Clark in IEEE Computer, 1993.
- Defibrillator cybersecurity by Halperin et al. in IEEE Symposium on Security & Privacy, 2008.
- Insulin pump analysis, 2011 [several]

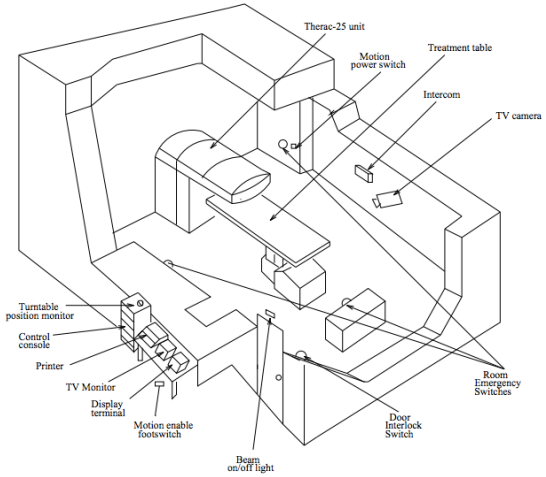


Figure 5: A typical Therac-25 facility after the final CAP.

Photos: Leveson, Fu

Short History: Medical Devices & SW

- Therac-25 analysis
  [Leveson & Clark, IEEE Computer, 1993]
- Defibrillator cybersecurity
  [Halperin et al., IEEE Symposium on Security & Privacy, 2008.]
- Insulin pump analysis, 2011 [several]
- Defib jamming defense
  [Gollakota et al., ACM SIGCOMM 2011]
- Pacemaker hack reproduced
  [Barnaby Jack, BlackHat 2012]
- WattsUpDoc defense
  [Clark et al., USENIX HealthTech 2013]

Photos: Leveson, Fu

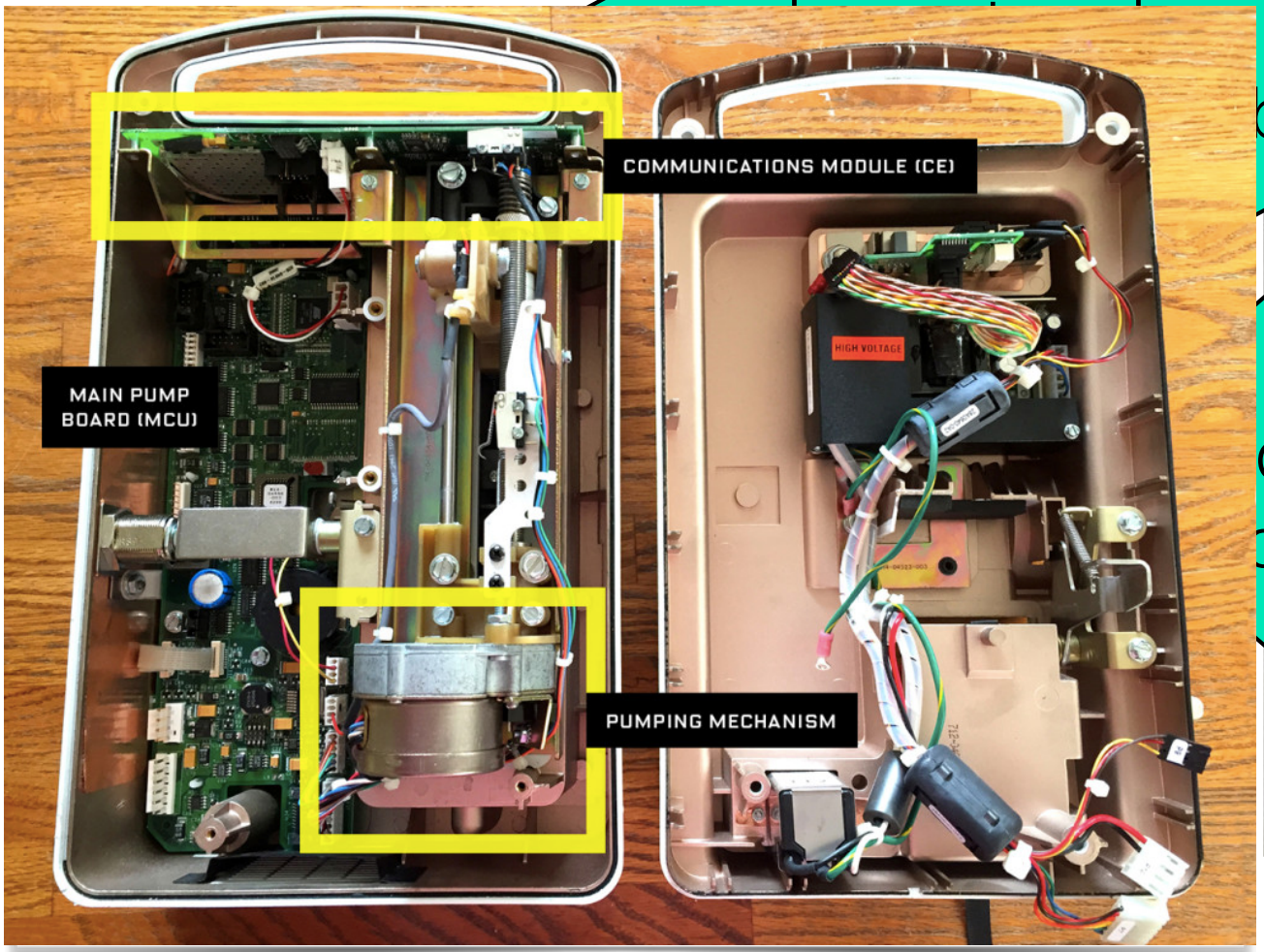
Short History: Medical Devices & SW

- Hospira Infusion Pump V[illegible]abilities [Billy Rios and more]

Wireless

[illegible]ble

Hard-
[illegible]ded local
[illegible]ccounts!



Photos: Wired

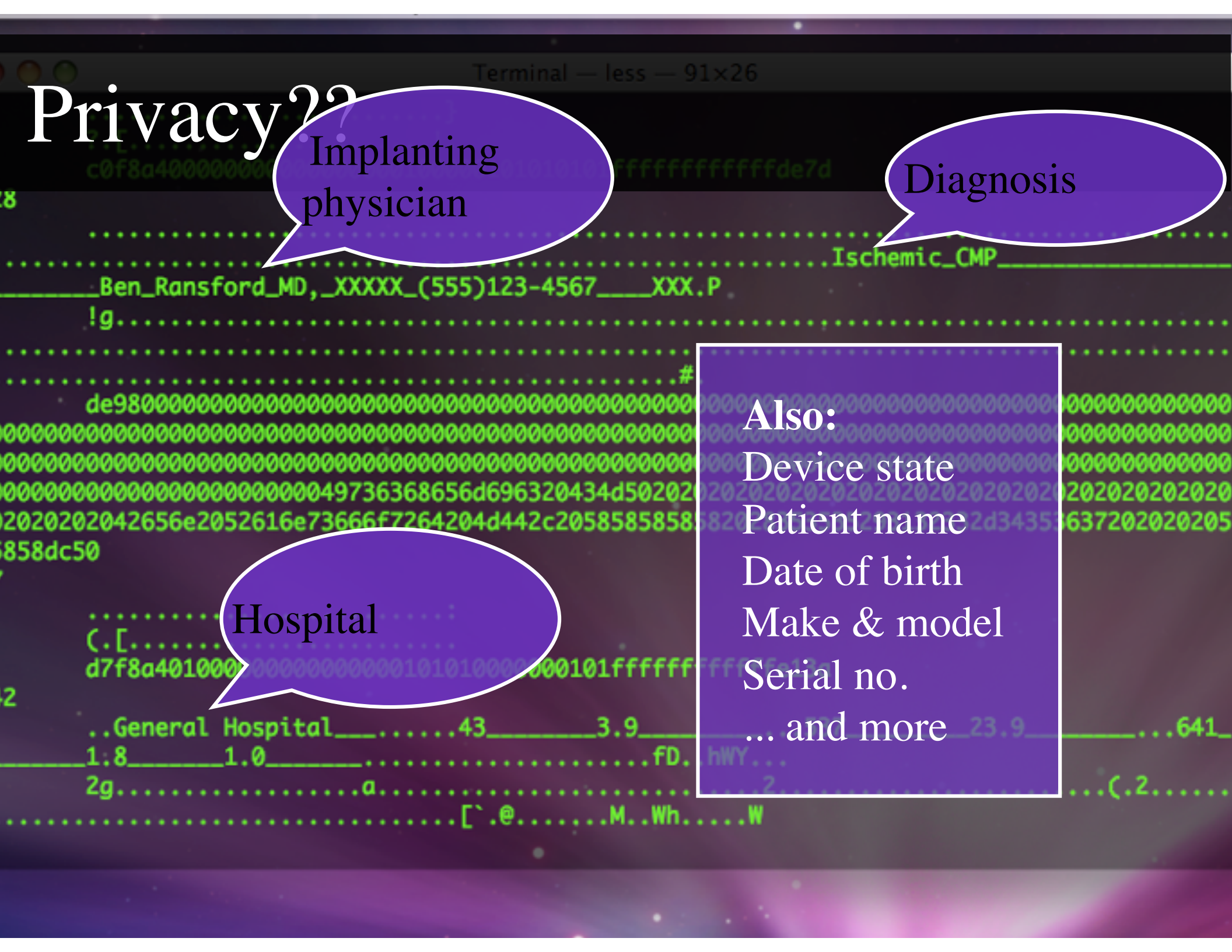
Implantation of Defibrillator

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

Device Programmer

Home monitor

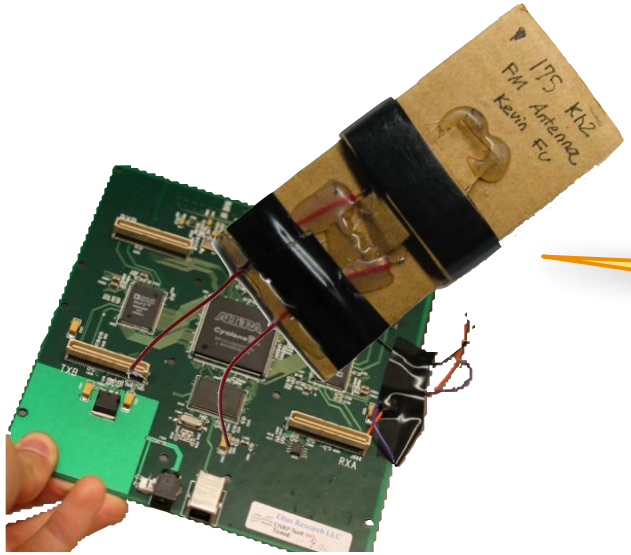
Photos: Medtronic; Video: or-live.com

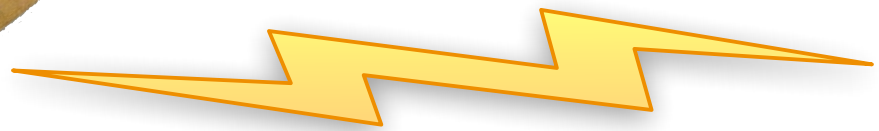

Privacy??
Implanting physician
Diagnosis
Ischemic_CMP
Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
Hospital
Also:
Device state
Patient name
Date of birth
Make & model
Serial no.
... and more

Wirelessly Induce Fatal Heart Rhythm

- 402-405 MHz MICS band, nominal range several meters
- Command shock sends 35 J in ~1 msec to the T-wave
- Designed to induce ventricular fibrillation
- No RF amplification necessary

(Risks mitigated a long time ago)





[Halperin et al., IEEE Symposium on Security & Privacy 2008]

Video and Exercise

- Design an authentication system for pacemakers

- Requirements
  - Patient outcomes must improve: safety and effectiveness
  - Security
  - Privacy

- What are the engineering tensions and challenges?
- How can we solve?

AED Firmware Replacement

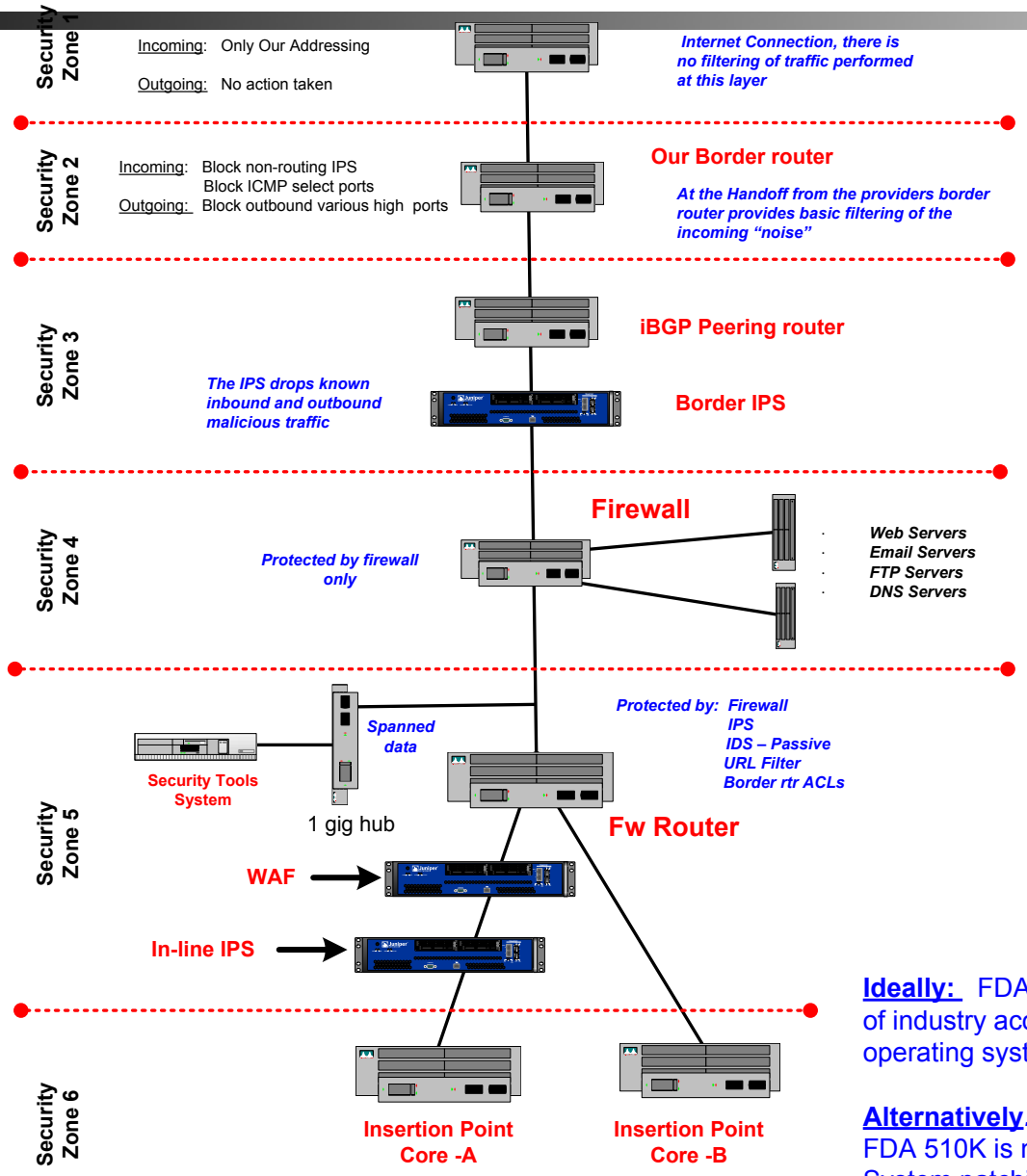
- Device accepts unauthentic firmware updates
- How do risks change when AEDs become wireless with Internet-based software updates?

DEVICE COMPROMISED

Hospitals & Malware

[Photo: Medical Real Estate Advisors and Kevin Fu]

Hospitals Stuck With Windows XP



General System Counts

Systems with AV……6398
Printers……..2074
Medical equipment…**905**
Misc……2460

Total Devices:……..11837

OS Makeup – Medical

Windows 95……..1
Windows 98 ……15
Windows 2000……..23
Windows CE……..9
Windows Vista……0
Windows XP……..600
Windows XP SP1…..0
Windows XP SP2….15
Windows XP SP3…..1

Total…….. 664

Last security patch: 2007

Average Time to Infection

Clinical Systems , 510K, no AV..: **12 days**
Systems running AV/Patches…..: **300+ days**

Ideally: FDA 510K is updated to include a requirement for the provision of industry accepted security controls for devices utilizing embedded operating systems or other controllers associated with a medical device

Alternatively: The FDA issues a clear statement to the community that FDA 510K is not jeopardized by permitting Anti-Virus or Operating System patching to the supporting systems associated with a certified medical device

[Courtesy: Mark Olson, BIDMC Boston]

Factory-installed malware?

More common than you might think

- Vendors with USB drives
- Vendors repairing infected machines
- Product assembly line

Shoot P0wn Foot w/ Software Update

Safe Browsing

Diagnostic page for www.viasyshealthcare.com

Advisory provided by Google

What is the current listing status for www.viasyshealthcare.com?

This site is not currently listed as suspicious.

Part of this site was listed for suspicious activity 1 time(s) over the past 90 days.

What happened when Google visited this site?

Of the 291 pages we tested on the site over the past 90 days, 19 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2012-06-24, and the last time suspicious content was found on this site was on 2012-06-13.

Malicious software includes 38 trojan(s), 3 scripting exploit(s).

Malicious software is hosted on 4 domain(s), including nikjju.com/, lilupophilupop.com/, koklik.com/.

This site was hosted on 1 network(s) including AS26651 (CAREFUSION).

Has this site acted as an intermediary resulting in further distribution of malware?

Over the past 90 days, www.viasyshealthcare.com did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?

No, this site has not hosted malicious software over the past 90 days.

Next steps:

- Return to the previous page.
- If you are the owner of this web site, you can request a review of your site using Google Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Updated 2 hours ago

Phone: 800.231.2466, ext 1
Email: support.vent.us@carefusion.com

EnVe

[Photo: Care Fusion, Niels Provos]

Waiter, there's a virus in my SW!

MAUDE Adverse Event Report: BAXA CORPORATIONBAXA EM2400 COMPOUNDER

FDA Home ⊙ Medical Devices ⊙ Databases

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

BAXA CORPORATION BAXA EM2400 COMPOUNDER Back to Search Results

Event Type Malfunction

Event Description

The (b) (6) pharmacy department uses a baxa em2400 compounder to make tpn's and other admixtures. Recently the compounder was infected with a virus. The virus has been contained on the em2400 compounder. It is unknown what effect this virus should have on the operating of the software. (b) (6) information systems department together with the pharmacy has requested that baxa provide a microsoft security patch to prevent this infection from occurring again. Baxa is unwilling to allow these patches to be applied to the baxa em2400. Instead baxa has recommend that we place a router with the functionality for a firewall between the compounder and the network (b) (4) as protection. In a single case, this may be a possible solution. (b) (6)'s manager indicates that if this was the routine solution, (b) (6) would then have to procure and maintain over 1000 routers institution wide. That approach is not sustainable by (b) (6) nor the marketplace. I am interested to hear about fda's requirement for medical devices to have security patches that protect the device from contamination.

Search Alerts/Recalls

Don't worry sir, they don't eat much!

MAUDE Adverse Event Report: BAXA CORP.EXACTA-MIX 2400

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 | TPLC

BAXA CORP. EXACTA-MIX 2400 Back to Search Results

Model Number EM 2400
Event Date 02/26/2010
Event Type Other
Manufacturer Narrative

The em2400 compounder is designed to not be connected directly to the facility network, but should be installed behind a firewall that provides a protected subnet for the device. The device should be used only in accordance with its intended use and not for email, internet access, file sharing or other non-approved use. The device is designed to only reach out to the facility's network to collect text-based pat files, back up device databases or to issue a print job. The em2400 compounder is hosted on a (b)(4)-based embedded operating system and has been verified and validated only with the software, operating system and patches that were installed by baxa. Thus, any changes to the original, validated image, including installation of antivirus software, nullifies the validated state and could; therefore, constitute off-label use of this device. In addition, baxa does not regularly install operating system updates or patches, generally published by (b)(4), on this device. The online help file, preventing cyber attacks technical paper, specifies baxa's policies relating to product security and provides instructions for safeguarding baxa devices. If a device becomes infected, baxa technical support will send a replacement and assist the customer with proper facility network installation. Baxa has not received any reports of pt injury or illness as a result of this issue.

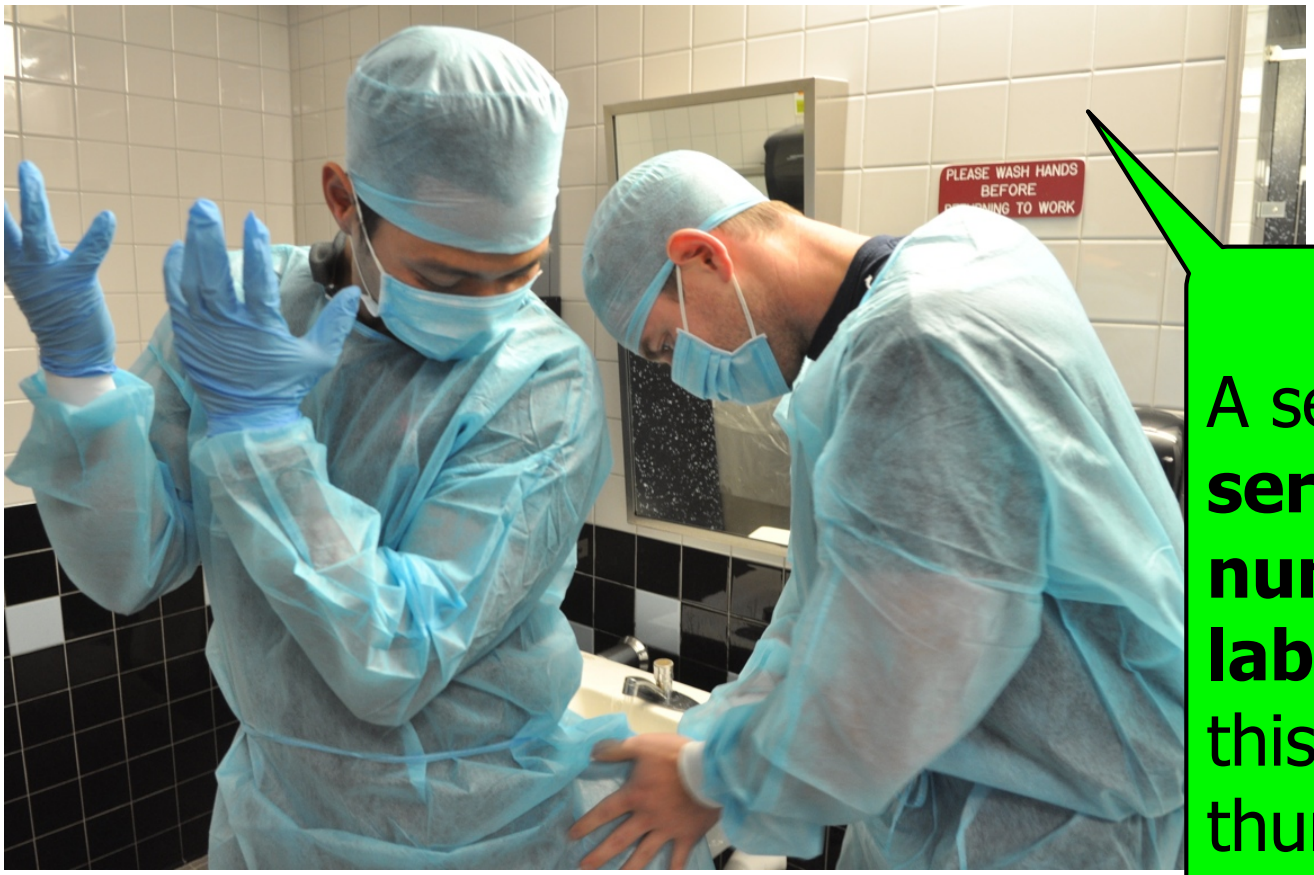
Event Description

Baxa received a letter from the fda on 04/08/2010 in reference to report number mw5014956. The report states that an em2400 compounder was infected with a virus. The customer requested that baxa provide a (b)(4) security patch to prevent the infection from occurring again. Upon receipt of the mw letter, the complaint database was reviewed to determine if an associated complaint was received by baxa prior to this report. No prior complaint was found. Therefore, a complaint was initiated to further investigate this issue. This mdr is being filed per baxa corporation's procedure to submit an mdr for all medwatch forms submitted.

Doctors…therefore always secure

As you are aware, on December 23rd an unknown **virus was found in the MacLab/CardioLab** system. [We] worked late into Christmas Eve in order to keep the infected MacLabs isolated. As a proactive measure and to prevent our patients from inappropriate release of protected healthcare information the hospital immediately blocked our access to the internet. Today [it was] announced that they have traced the virus path from [a] nursing workstation. Apparently pictures were uploaded from a USB drive to yahoo.

Sterile Technique or Software Sepsis?



A senior faculty member **serially infected a number of cath and EP lab systems,** and solved this problem by plugging thumb drives into a fellow's laptop to erase the malware he was spreading.

-Dr. Anonymous

OPEN ACCESS Freely available online

PLoS one

Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance

D
K
1
S
r

Regulators and manufacturers should carefully weigh the **premarket evaluation of security and privacy** elements of their devices and systems, and to design postmarket systems that enable effective collection of cybersecurity threat indicators for medical devices.

Methods: We used three comprehensive, publicly available databases maintained by the Food and Drug Administration (FDA) to evaluate recalls and adverse events related to security and privacy risks of medical devices.

Results: Review of weekly enforcement reports identified 1,845 recalls; 605 (32.8%) of these included computers, 35 (1.9%) stored patient data, and 31 (1.7%) were capable of wireless communication. Searches of databases specific to recalls and adverse events identified only one event with a specific connection to security or privacy. Software-related recalls were relatively common, and most (81.8%) mentioned the possibility of upgrades, though only half of these provided specific instructions for the update mechanism.

Conclusions: Our review of recalls and adverse events from federal government databases reveals sharp inconsistencies with databases at individual providers with respect to security and privacy risks. Recalls related to software may increase security risks because of unprotected update and correction mechanisms. To detect signals of security and privacy problems that adversely affect public health, federal postmarket surveillance strategies should rethink how to effectively and efficiently collect data on security and privacy problems in devices that increasingly depend on computing systems susceptible to malware.

Citation: Kramer DB, Baker M, Ransford B, Molina-Markham A, Stewart Q, et al. (2012) Security and Privacy Qualities of Medical Devices: An Analysis of FDA

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

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

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.

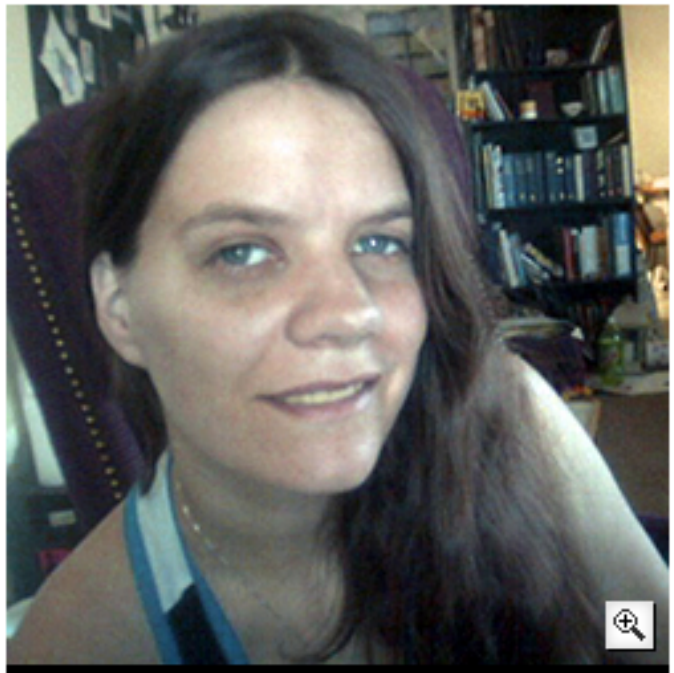
Discuss
COMMENTS (5)

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.

Bad People Do Exist: Vandals

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.

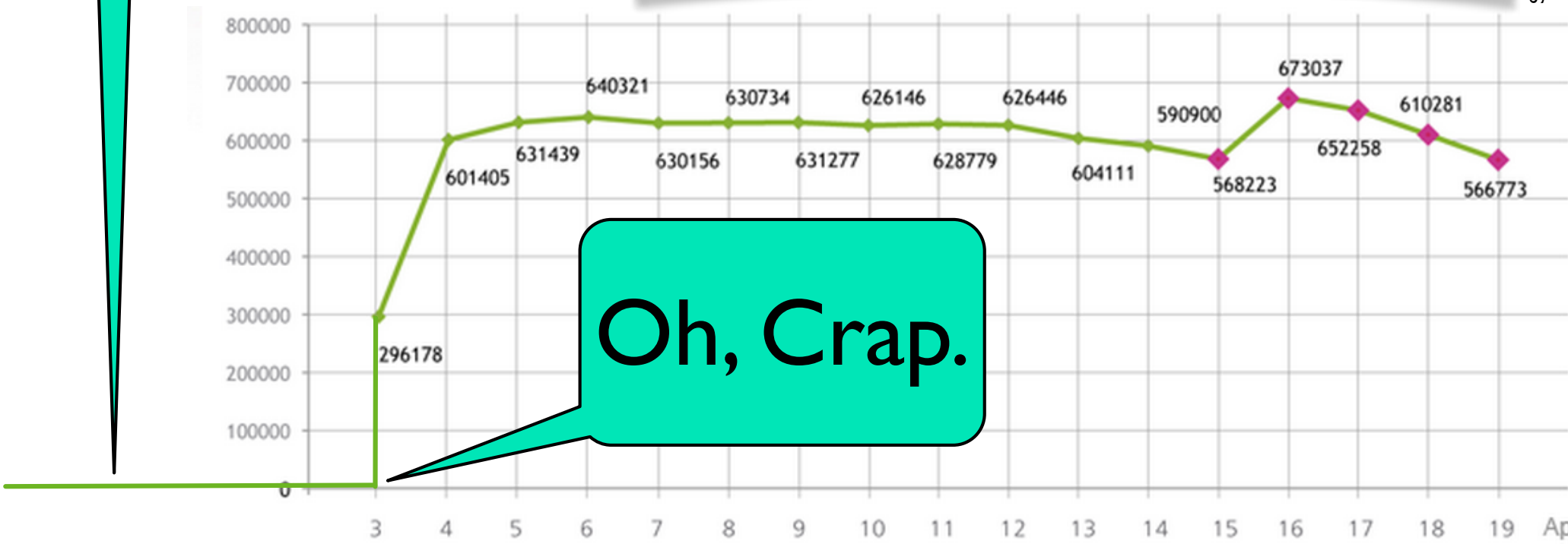
Lack of Exploits is Not Assurance

Pre-April 2012:
No Mac threats,
therefore never will be.

SECURITY | 4/20/2012 @ 5:28PM | 2,173 views

Antivirus Researchers Confirm: Flashback Still Infects More Than 500,000 Macs

Source: Andy Greenberg, Forbes



Oh, Crap.

19 Days in April 2012

Achoo!

The Weekly World News: world's only reliable journal

Security of 156 VA Med. Centers

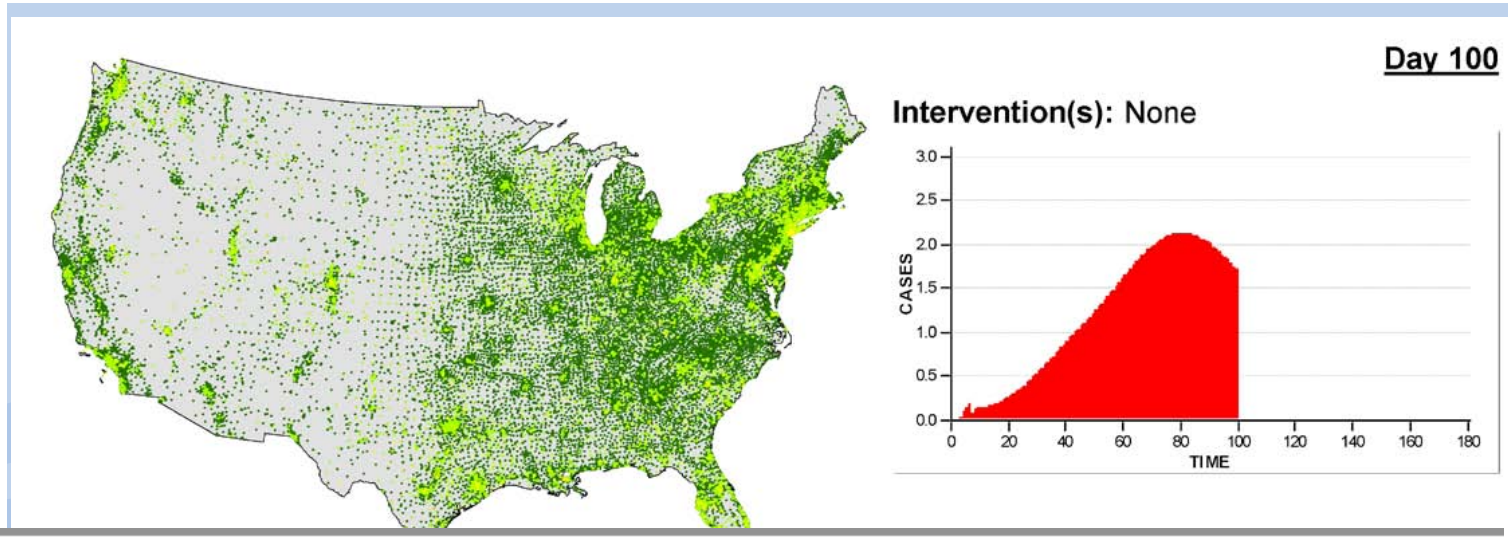
- Every **8 seconds**, the VA still finds usernames and **passwords** unprotected in networks

- VA has ~**600,000** connected computing devices, of which **50,000** are considered medical devices
- VA implemented VLANs with **3,270 different ACLs**

- Manual maintenance of ACLs prone to human error
- ACLs broke network security tools that detect intrusions

[Source: Lynette Sherrill, VA Field Security Office]

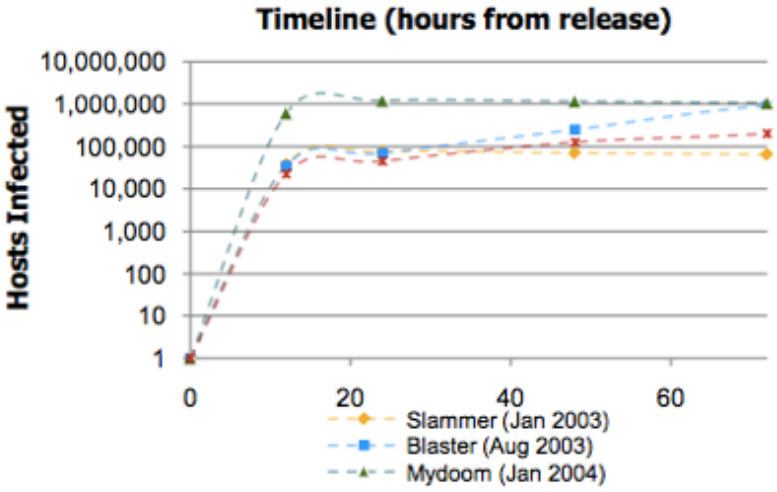
Disease to Malware:Days to Hours



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

DARPA

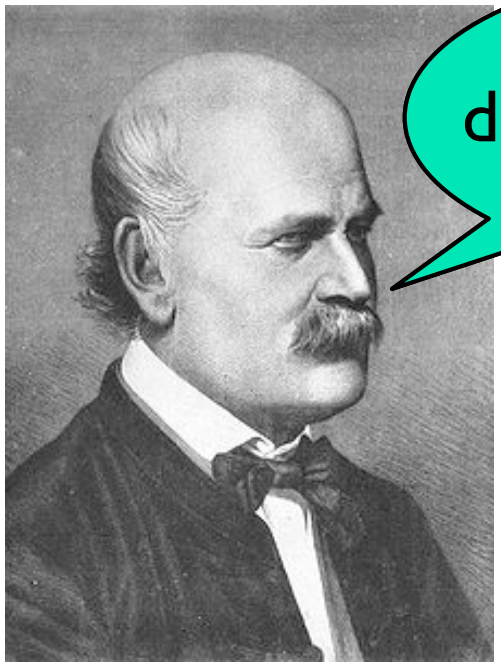
Dark Clouds on the Horizon: The Network is a *Vulnerability Amplifier*



Slide from Howie Shrobe and others

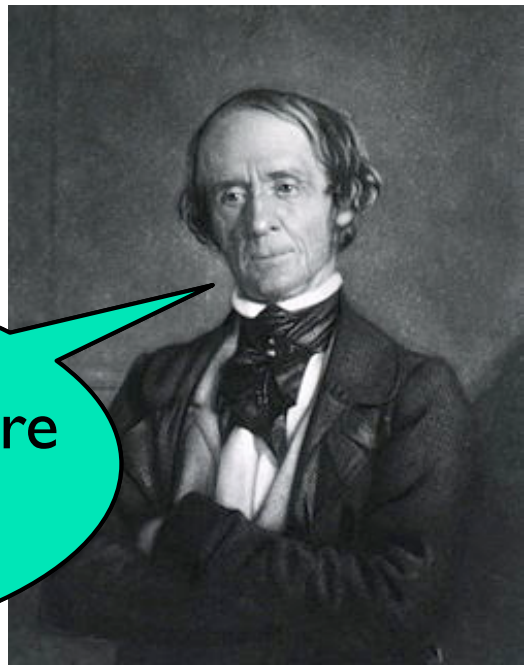
Semmelweis to Software Sepsis

1. Implantable medical devices should be trustworthy
2. Improved security will enable medical device innovation



Medical devices should be secure.

Doctors are gentlemen and therefore their computers are always secure.



Dr. Ignaz Semmelweis
1818-1865

Dr. Charles Meigs
1792-1869

←Ways Forward ↗

Security should be **designed** in

not **bolted** on

Pixie Dust to Solve Security…ugh

- What design controls address cybersecurity risks?
  - Using wireless? Radio? USB port? Networking? Cloud?
  - A manufacturer can not claim unawareness of security risks
- How often are **software updates** issued to customers?
  - Windows XP has several critical security flaws per year
  - Engineers need resource$ to regularly issue software updates
- **Oxymorons** that raise my eyebrows. Watch out for:
  - Windows XP security
  - Cloud security
  - Wireless security
  - Unbreakable cryptography
  - Firewall-based security
  - Proprietary security
  - Private networks

http://www.crypto.com/bingo/pr

What a Great Idea, Dear Engineer!

- Can't you just...
  - Add a password?
    (ignores emergency access)
  - Implement crypto?
    (part of sol'n, but red herring)
  - Mandate an isolated network? (two words: USB stick)
  - Install anti-virus?
    (tends to screw up machine)
  - Firewalls?
    (so you'r
- Sadly, technical sol'n tied to **non-technical** constraints:
  - Human factors, regulatory, management, economics, engineering, science, public health

Credit: demotivationalposters.org

Sarcasm Continued…

Credit: demotivationalposters.org

- Problems with arm chair security engineering:
  - **Ad hoc** approaches lack principled-based design
  - Many technical approaches ignore **human factors**
  - Security is an **emergent property** of a system
  - Need to use **system engineering** principles
  - **Component** solutions alone won't solve problem
  - Get the **security requirements** right first

Computing Research Beyond Ivory Tower
Helping the Community, Saving Lives

Creating safe, effective, and secure medical devices:

- **Detect computer malware on hospital medical devices by analyzing power outlets**
- **Device to test safety of recycled pacemakers saves lives in Ghana**

Patient in Ghana receives safely recycled pacemaker

Power outlet detects malware on drug compounder

Manufacturers visiting Center for Medical Device Security

Cybersecurity: A Foreseeable Risk

- Biggest risk at the moment:
  - ~~Hackers breaking into medical devices~~
  - Wide-scale **unavailability** of patient care
  - **Integrity** of medical sensors

- Gaps
  - Don't interrupt clinical workflow
  - Many security specialists focus on technical controls (ahem, **you**)
  - Many safety specialists focus on risk management (biomedical)
  - Trustworthy medical device software requires both

spqr.eecs.umich.edu • Prof. Kevin Fu • Medical Device Security

Post-388 Opportunities

- Courses
  - EECS475 Cryptography
  - EECS588 Grad security
  - PUBPOL750 Cyber Conflict
- Reading
  - RISKS Column
  - USENIX Security Symposium (student travel grants!)