



# Medical Device Security: The First 164 Years

**Prof. Kevin Fu, Ph.D.**

Associate Professor, Director  
Archimedes Center for Medical Device Security  
University of Michigan, EECS  
TROOPERS 2014, Heidelberg, Germany

<http://secure-medicine.org/>

[kevinfu@umich.edu](mailto:kevinfu@umich.edu)



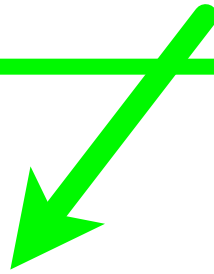
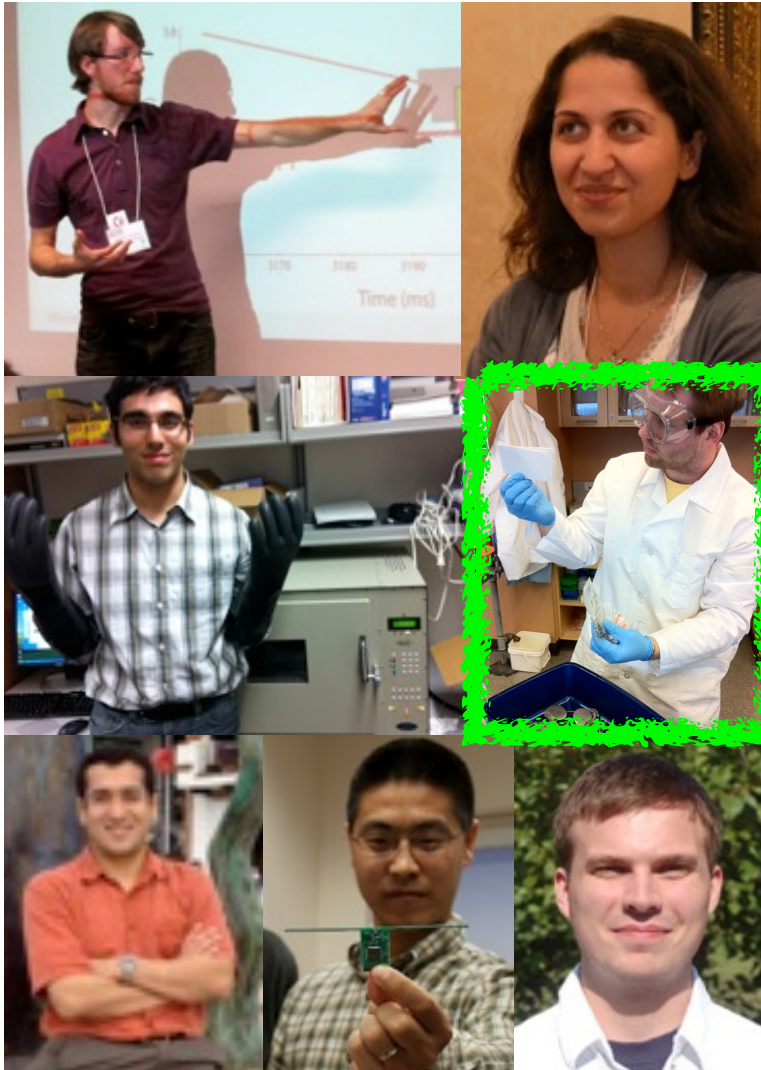
Supported in part by NSF  
CNS-1330142 and the numbers  
4101-9700-2532-1187-2157.  
Any opinions, findings, and  
conclusions expressed in this  
material are those of the authors  
and do not necessarily reflect  
the views of NSF.

# The **S** Today's slice of research **R** Lab

Graduate Students

(Security & Privacy Research Lab)

Undergraduate REUs



Pre-UGrad



# 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, Harvard Med School
- Prof. Dawn Song, UC Berkeley Computer Science Div.

- Research assistants

- Shane Clark, Benessa Defend, Tamara Denning, Denis Foo Kune, 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

# Background & Disclosures

---

- Director, Security & Privacy Research Group @ Univ. Michigan EECS
- Director, Archimedes Center for Medical Device Security
- Co-chair, AAMI Working Group on Medical Device Security
- Federal Advisory Committee member, NIST Information S&P Advisory Board
- Fmr. visiting scientist, U.S. Food and Drug Administration
- Recent research support from NSF, HHS, SRC, DARPA, MARCO, Underwriters Labs (UL), Medtronic, WelchAllyn
- 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. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of sponsors.



[Back to previous page](#)

## FDA, facing cybersecurity threats, tightens medical-device standards

By [Lena H. Sun](#) and [Brady Dennis](#), Updated: Thursday, June 13, 9:01 AM

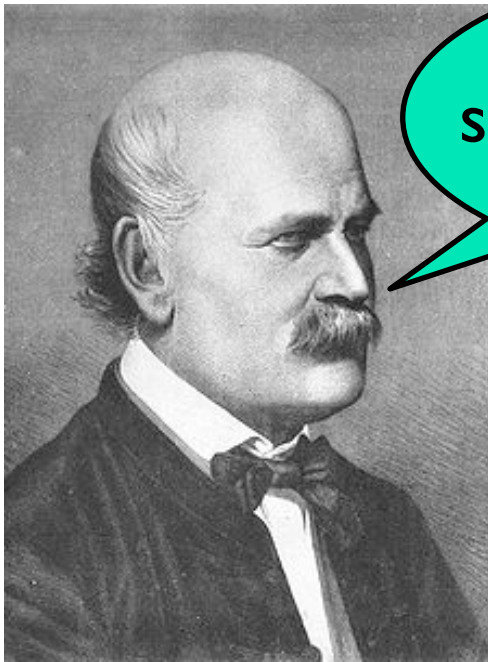
The Food and Drug Administration is tightening standards for a wide range of medical devices — from fetal monitors used in hospitals to pacemakers implanted in people — because of escalating concerns that the gadgets are vulnerable to cybersecurity breaches that could harm patients.

Increasingly, officials said, computer viruses and other malware are infecting equipment such as hospital computers used to view X-rays and CT scans as well as devices in cardiac catheterization labs. The security breaches cause the equipment to slow down or shut off entirely, complicating patient care. As more devices operate on computer systems that are connected to each other, the hospital network and the Internet, the potential for problems rises dramatically, they said.



# 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?**

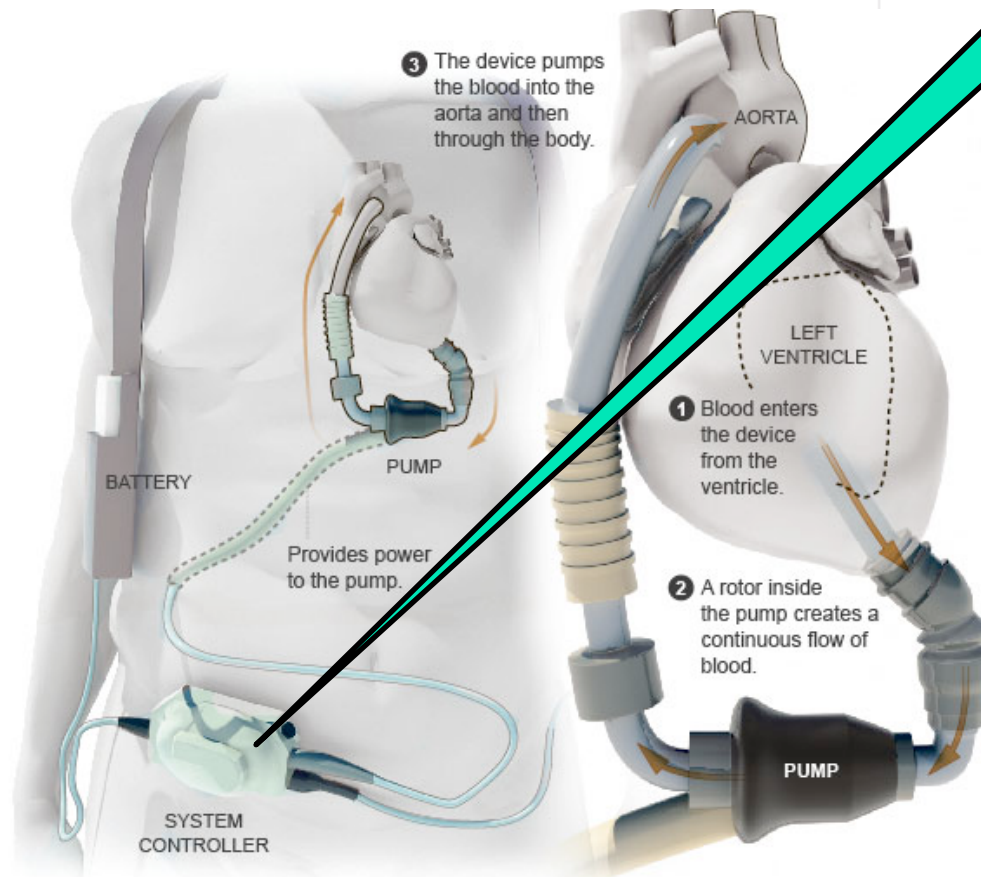
# Benefits of Medical Device Software

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



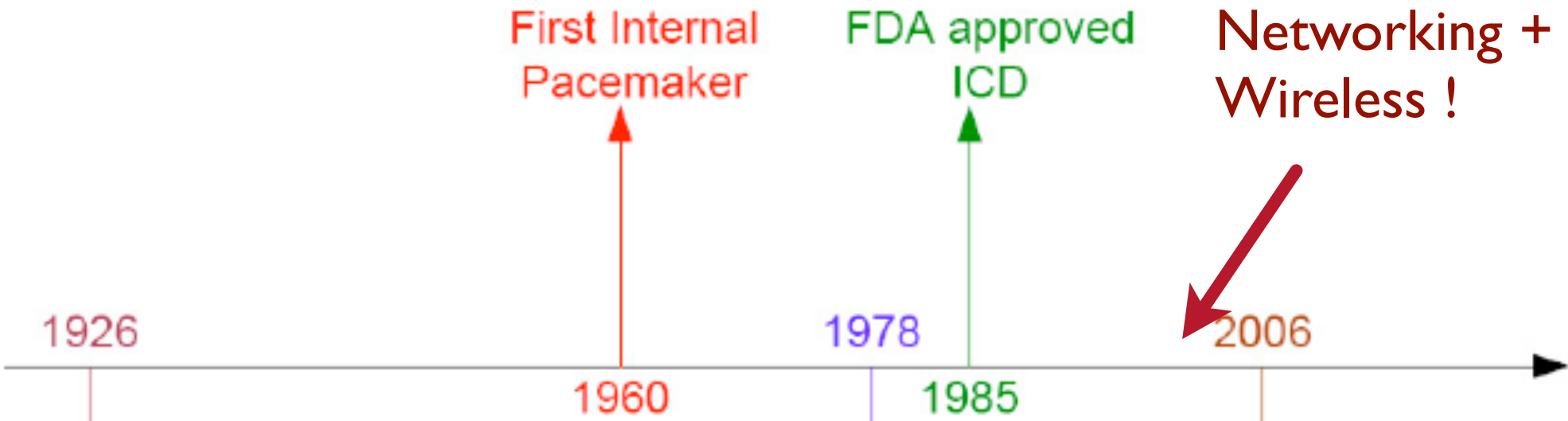
**Without software,  
many medical treatments  
could not exist.**

# Medical Devices 101:

## A 10-minute residency



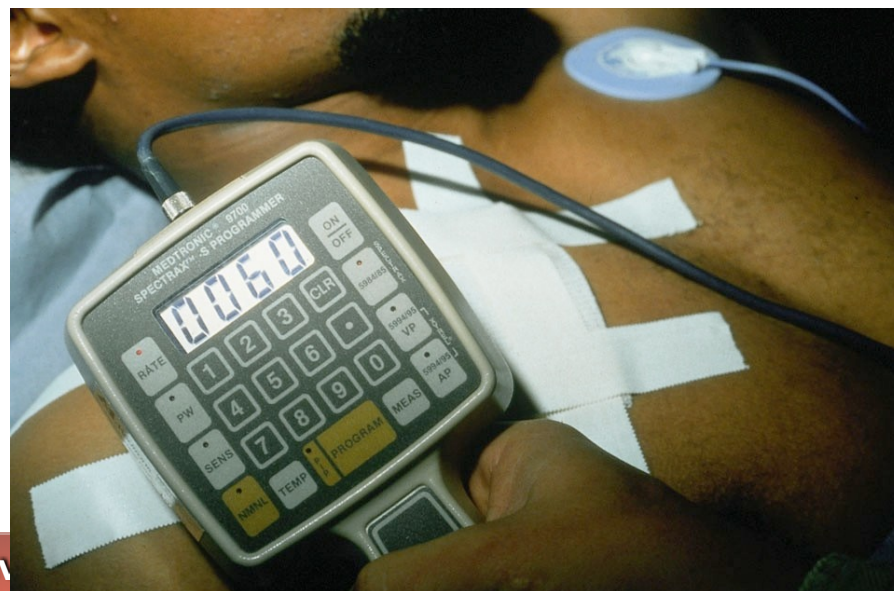
“Nurse, get on the Internet, go to SURGERY.COM, scroll down and click on ‘Are you totally lost?’ icon.”



First Pacemaker



First Cochlear Implant Surgery



Wireless Blood Glucose Monitor

Photos from:  
Medtronic

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

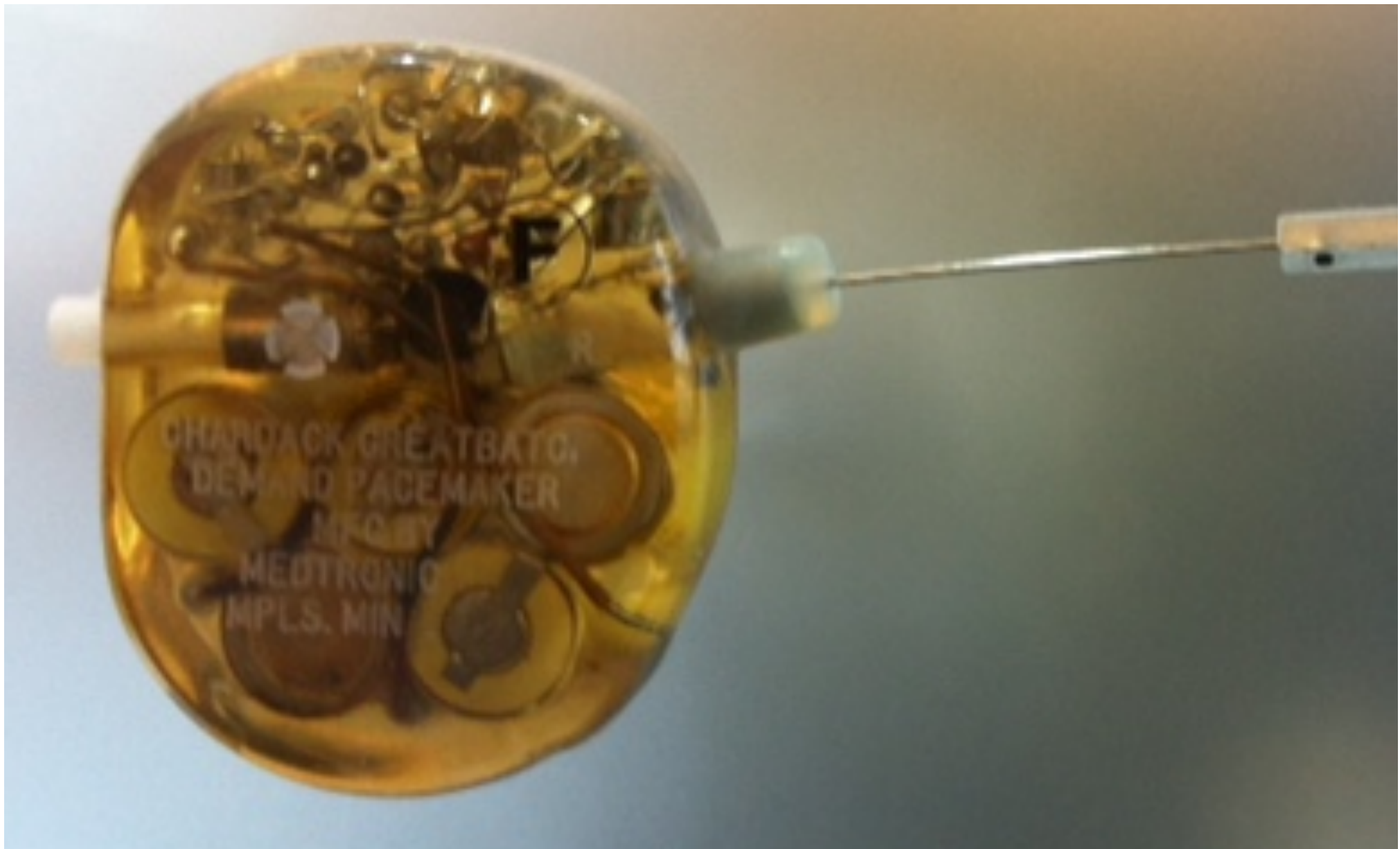
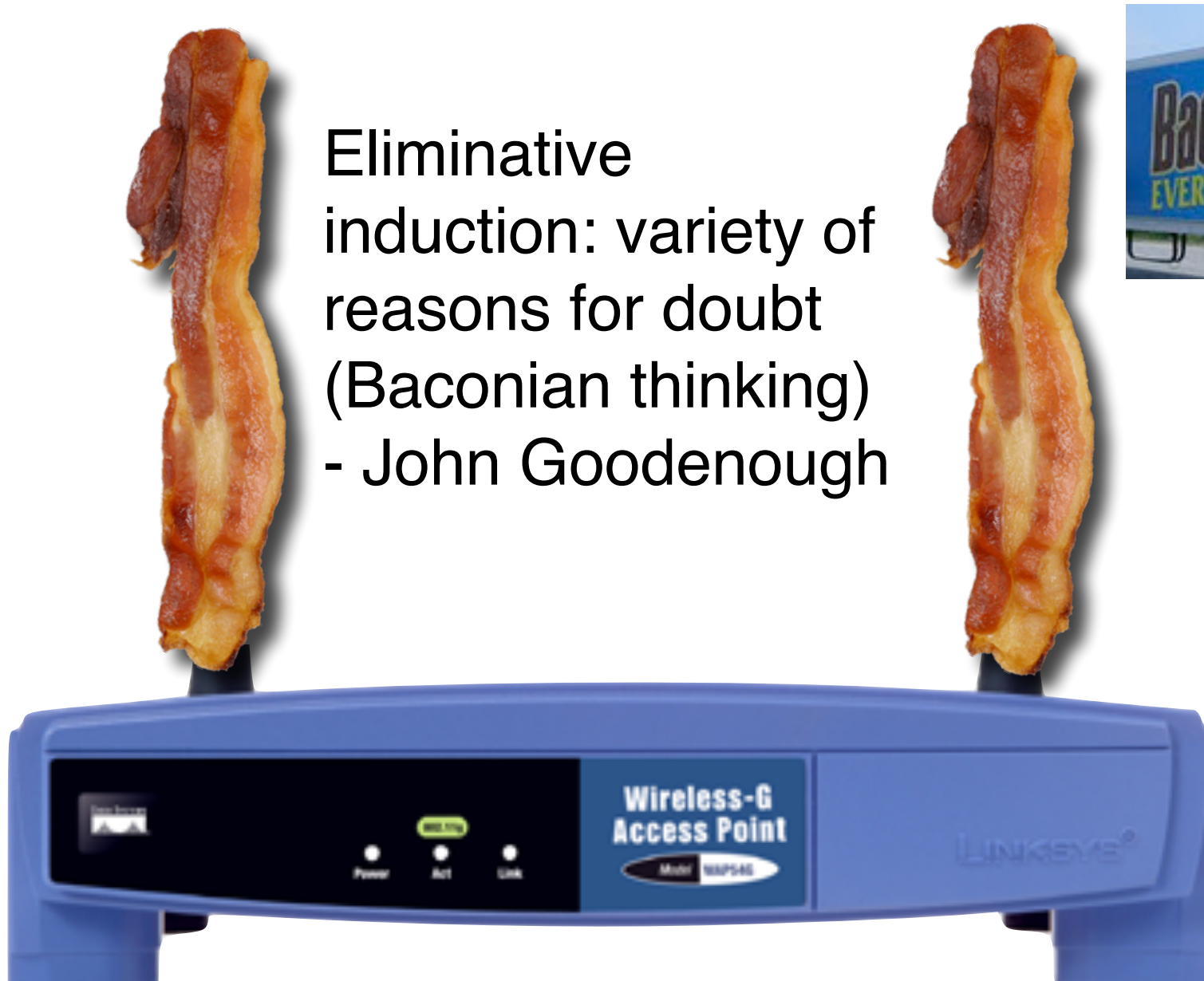


Photo by Kevin Fu @ Medtronic museum



# Wireless Makes Everything Better?



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





“Safe, secure, and reliable **wireless medical device** systems require...  
focus on wireless performance,  
**security**, and EMC.”

-Don Witters, FDA CDRH

## Wireless Security

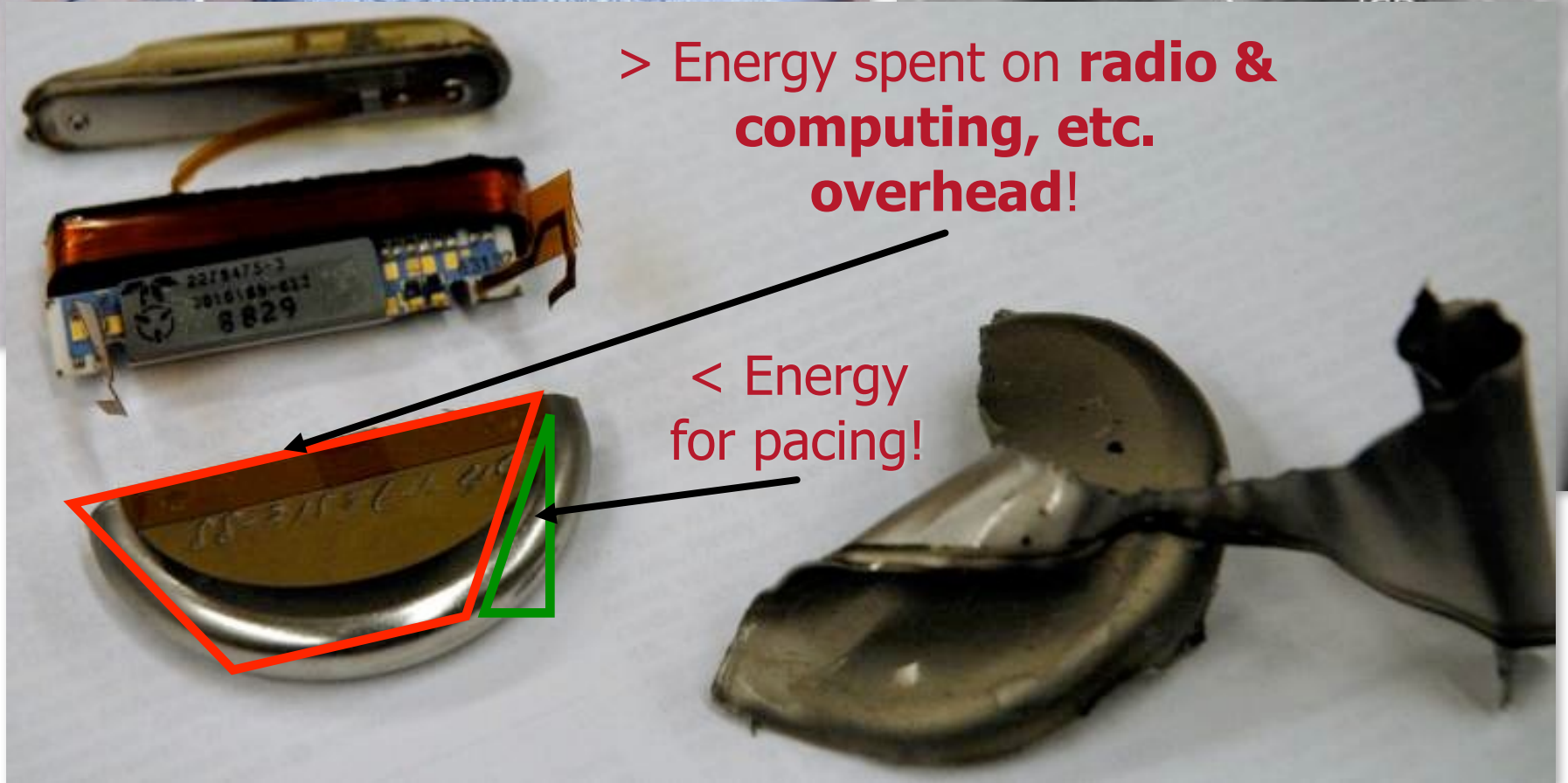
### ▶ **Wireless security issues**

- ▶ 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

# Pacemakers: Regulate heartbeat



# 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





# Overconfidence in Software

IEEE Computer 1993

## An Investigation of the Therac-25 Accidents

Nancy G. Leveson, University of Washington

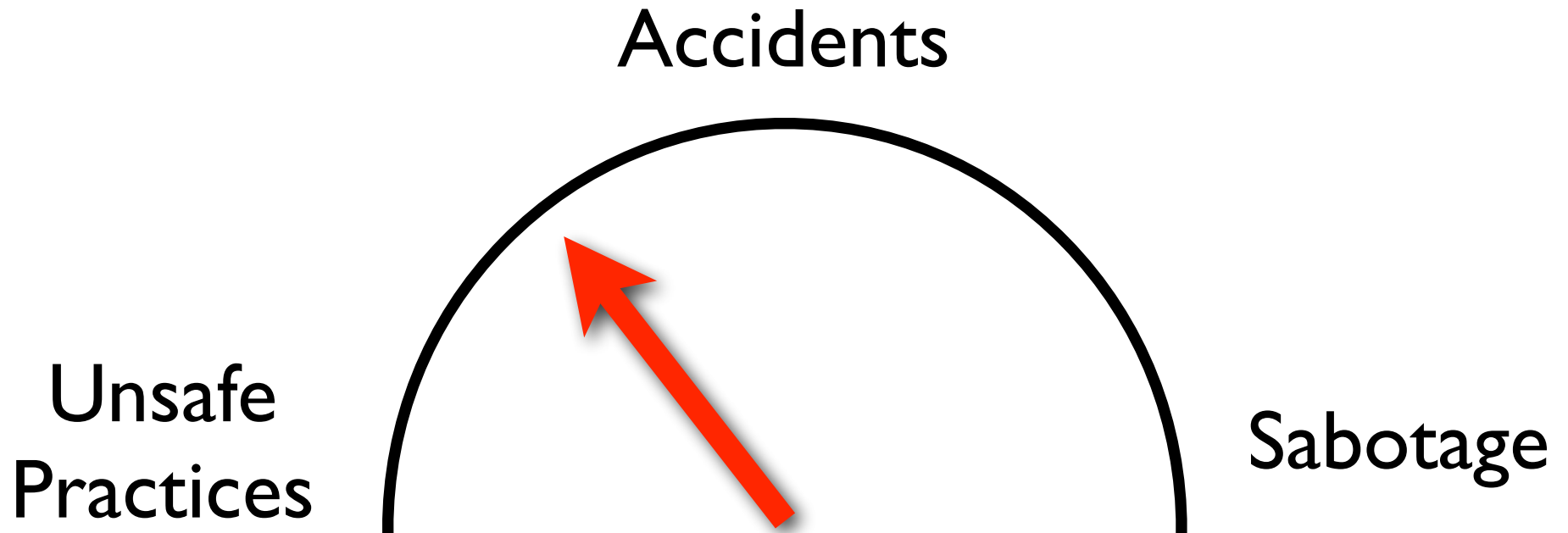
Clark S. Turner, University of California, Irvine

“...the machine could not possibly over treat a patient and ... no similar complaints were submitted...”

[Leveson & Turner, 1993]

# Accumulative Risks of...

---



**Threat-o-meter**

# Symptom: Implementation Errors

FDA U.S. Food and Drug Administration

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

FDA Home > Medical Devices > Databases

A-Z Index Search

## MAUDE Adverse Event Report

- 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

BAXTER HEALTHCARE PTE. LTD. COLLEAGUE 1 CYB VOLUMETRIC INFUSION PUMP 805RN

[Back to Search Results](#)

Catalog Number 2M9163

Event Date 07/30/2007

Event Type Death Patient Outcome Death;

Manufacturer Narrative

■ levophed (blood pressure)

■ insulin

■ Organs donated

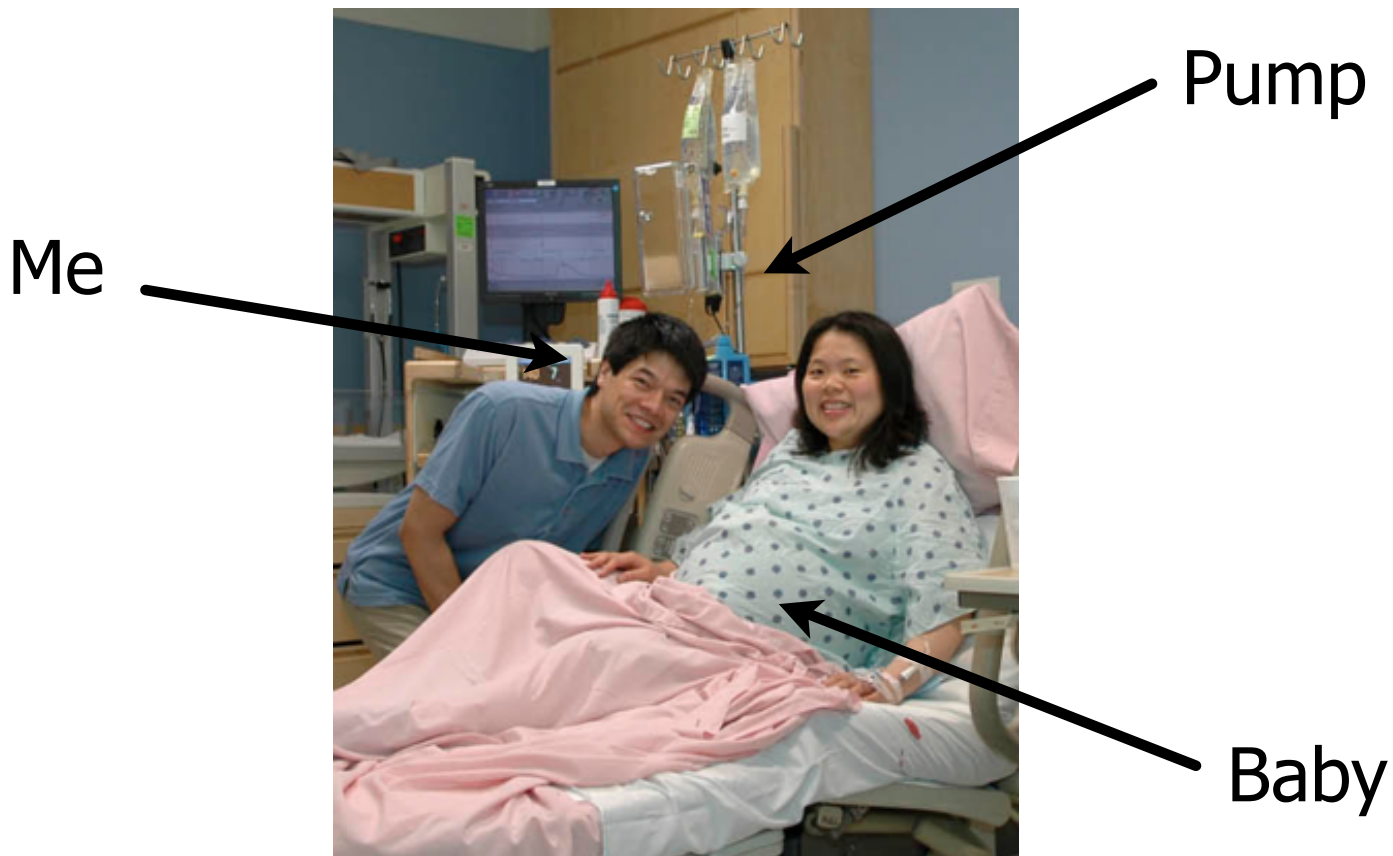
Evaluation of the device indicates the reported condition of fail code 16:310 was confirmed but could not be duplicated during service. The pump passed power on self-test on ac. The front bezel was opened & a visual inspection of all wires, harness connections, and user interface module printed circuit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

# 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]

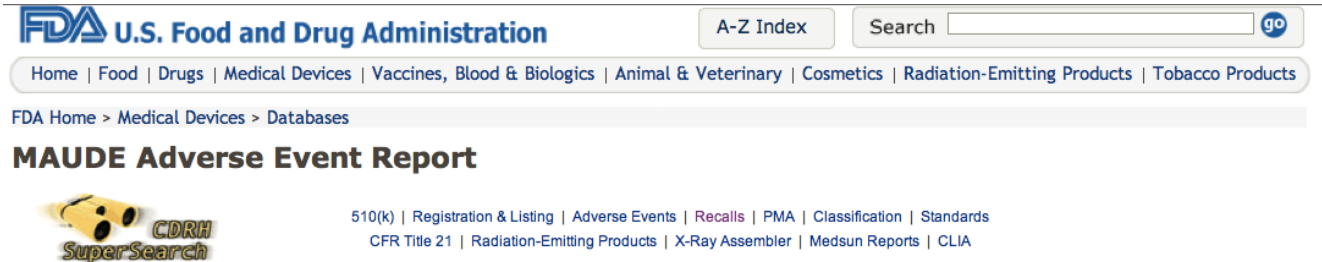
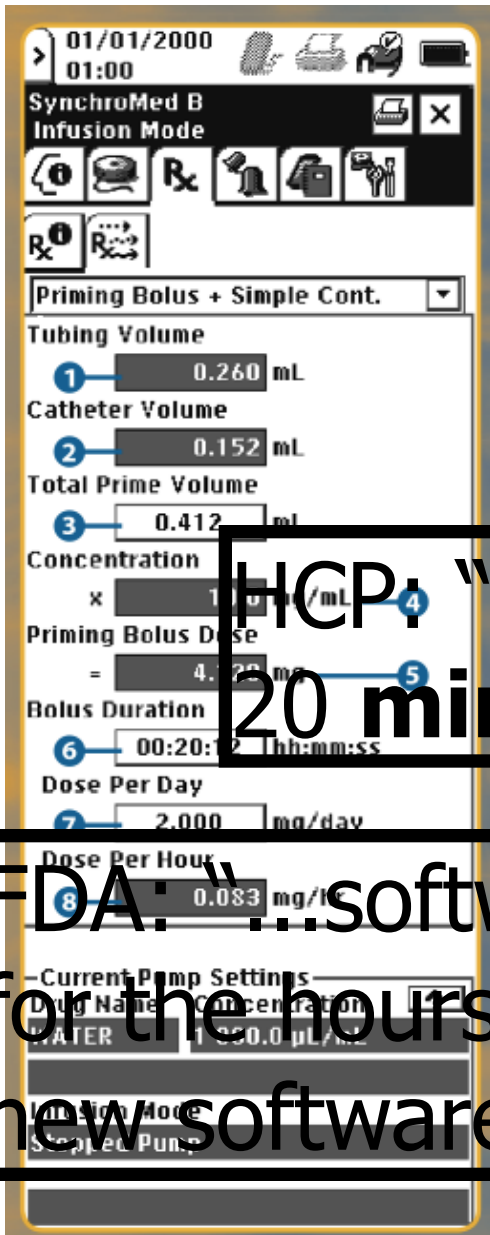
# Pump+SW Problems=Deadly Cocktail

---

- “... 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]

**"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**

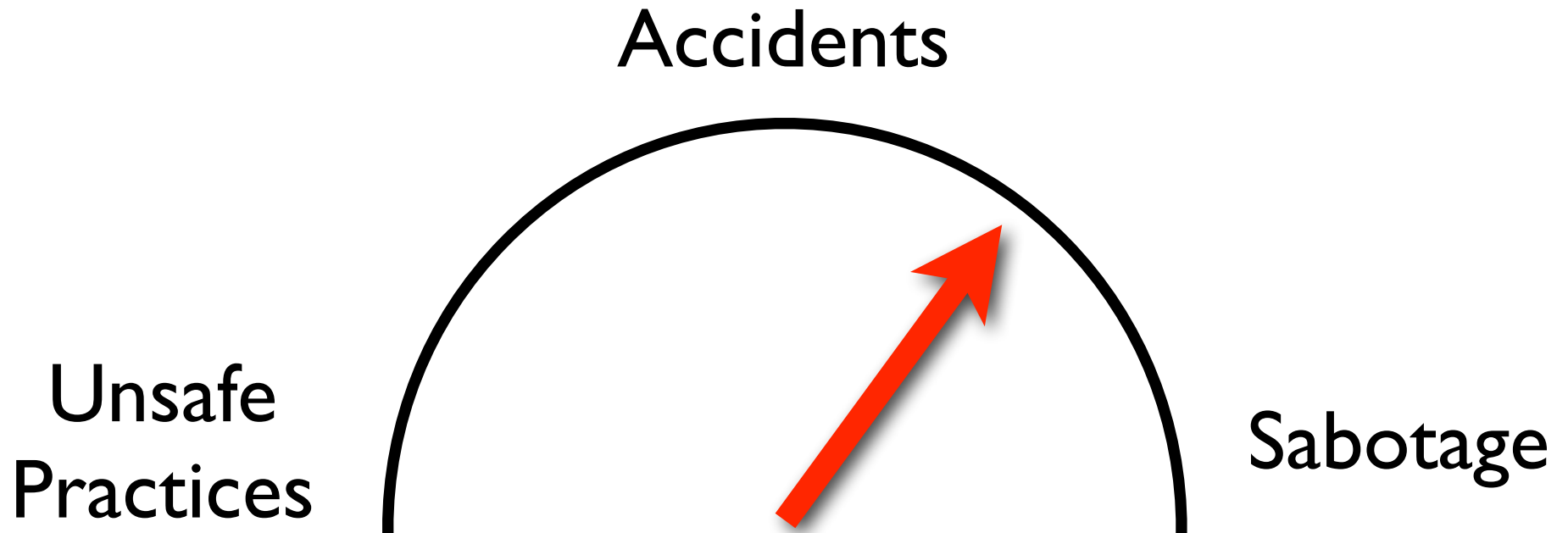


**Shipwreck  
as seen  
from  
space.**

**Credit: DigitalGlobe**

# Accumulative Risks of...

---

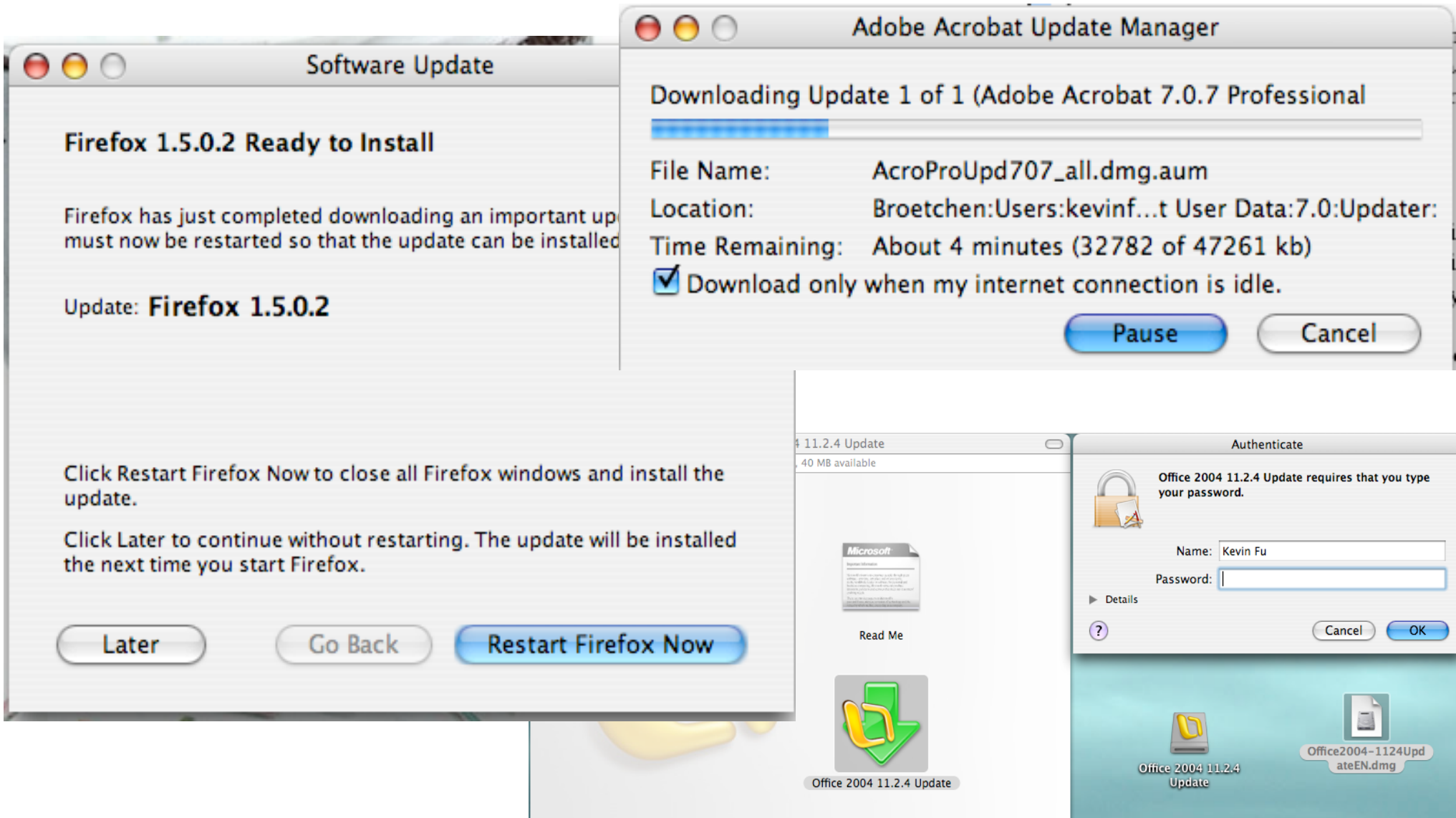


**Threat-o-meter**



# 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

# Users are Helpless

Windows

Home Windows 7 Windows Vista Windows X

Windows Client TechCenter > Windows XP IT Pro Forums > V from SP3 to SP2

Ask a question Search Forums: Search

## ? Downgrade from SP3 to SP2

0

Sign In to Vote

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

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.

Reply Quote

# Slashdot

NEWS FOR NERDS. STUFF THAT MATTERS.

Stories Recent Popular Search

## 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."





# 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

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

Get cu  
more fle  
security  
virtualiz

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



[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.

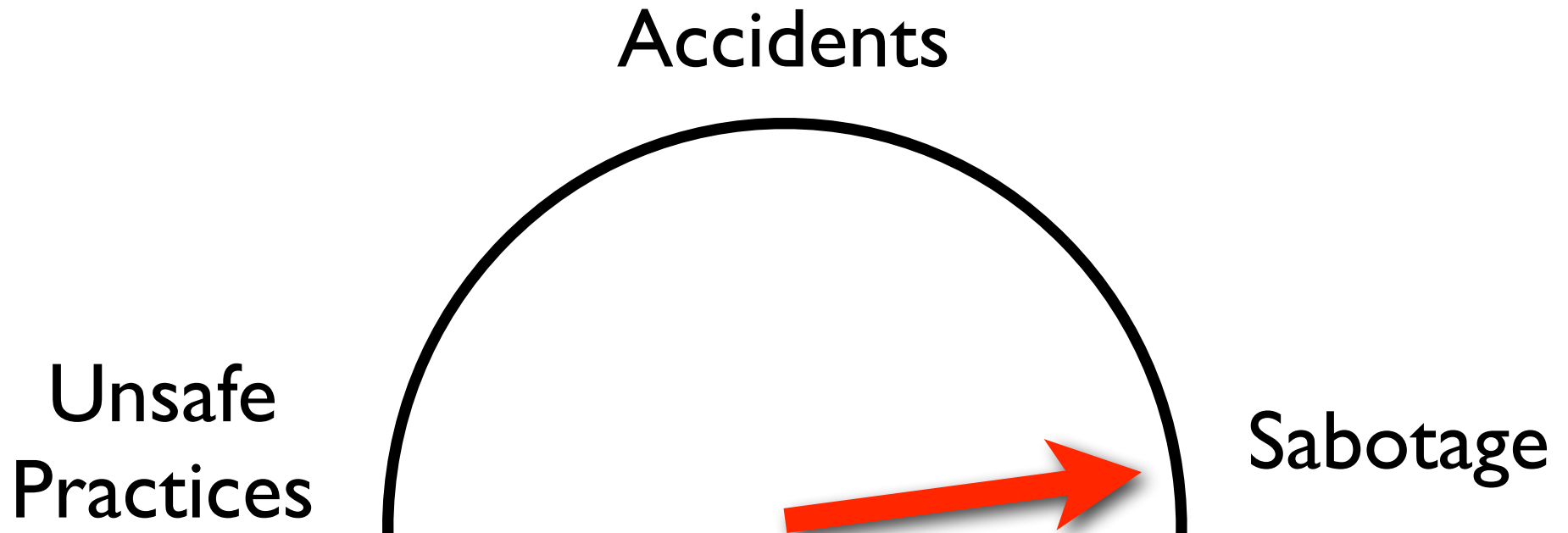
FDA is aware of misinterpretation of the regulations for the cybersecurity of medical devices that are connected to computer networks. FDA's interpretation of the regulations can be found in the 2005 [guidance](#) for industry and its accompanying [information for healthcare organizations](#).

# Managerial issues: Diffusion of responsibility

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

# Foreseeable Cybersecurity Risks...

---



**Foreseeable risk-o-meter**

# 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

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  $\sim 1$  msec to the T-wave
- Designed to induce ventricular fibrillation
- No RF amplification necessary



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

[Print](#)[Tweet](#)[Like](#)

31

## Insulin pump hack delivers fatal dosage over the air **Sugar Blues, James Bond style**

By [Dan Goodin in San Francisco](#) • [Get more from this author](#)

Posted in [Security](#), 27th October 2011 06:23 GMT

In a hack fitting of a James Bond movie, a security researcher has devised a way to hijack nearby insulin pumps, enabling him to surreptitiously deliver fatal dosages to patients who rely on them.



Barnaby Jack



**bigJAB 1.0 [beta]**

File Scan

PumpID	Firmware	Pump Model	Max Bolus	Remaining Insulin
535		722	25 Units	27 Units

- Populate List Fields
- Dump Insulin**
- Send Raw Command
- Read From Memory
- Write To Memory
- Suspend Pump
- Resume Pump

CONSOLE

```
Checking for USB device..
Device connected.
Scan Started..
Sending RF enable packets...
Sending association...
Associated!
Requesting ID...
ID Found!
Sending RF enable packets...
Sending association...
Stopping Scan..
Attempting association with PumpID 535239.. SUCCESS
Retrieving Firmware Version..
Retrieving Pump Model..
Retrieving Max Bolus..
Retrieving Remaining Insulin..
```

Status: Idle..

Start Scan Stop Scan

# AED Firmware Replacement



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

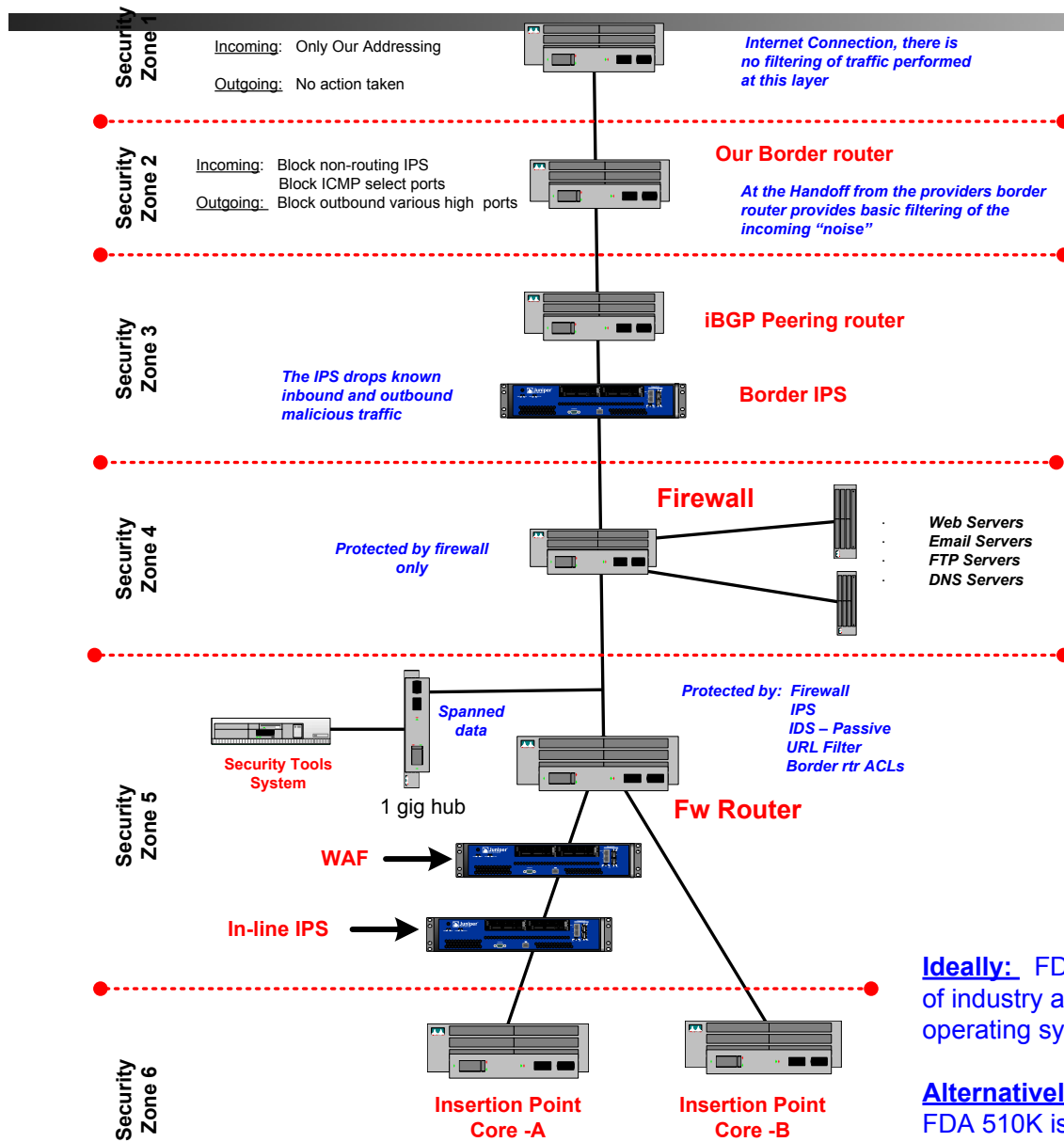
**DEVICE COMPROMISED**

# Hospitals & Malware





# Hospitals Stuck With Windows XP



## General System Counts

Systems with AV.....	6398
Printers.....	2074
Medical equipment....	<b>905</b>
Misc.....	2460
-----	
Total Devices:.....	11837

## OS Makeup - Medical

Windows 95.....	1
Windows 98.....	15
Windows 2000.....	23
Windows CE.....	9
Windows Vista.....	0
<b>Windows XP.....</b>	<b>600</b>
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](http://www.viasyshealthcare.com)

Advisory provided by 

### What is the current listing status for [www.viasyshealthcare.com](http://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 [nikju.com/](http://nikju.com/), [lilupophilupop.com/](http://lilupophilupop.com/), [koklik.com/](http://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](http://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](mailto:support.vent.us@carefusion.com)

FnVe



# Waiter, there's a virus in my SW!

## MAUDE Adverse Event Report: BAXA CORPORATION BAXA 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](#)

**5982-6691-4332-1458-0338**

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

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

[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 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.



# But According to FDA...

“Virtual Patient Safety: Worms, Viruses and Other Threats to Computer-Based Medical Technology” by Al Taylor of FDA CDRH

## The burning question

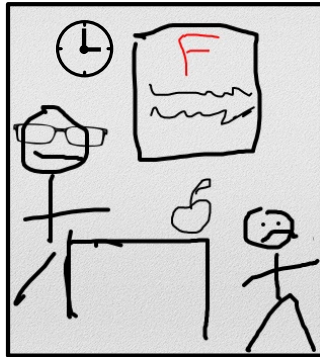
**Q.** Is FDA policy degraded performance by imp implementation of s patches in commercial off-the-shelf (COTS) software used in network connected medical devices?

**A.** No. But there seems to what is required, and *m of FDA policy (and the contributing to the pr*

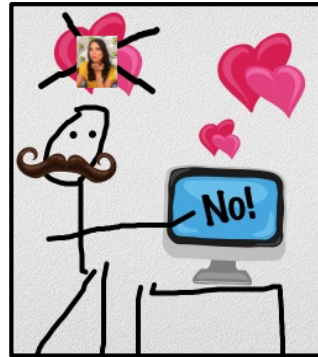
Unspecified manufacturers have reportedly told hospital IT staff that they can't install security patches "because of FDA rules."

Biomedical engineering staff need to report SW security problems to FDA for things to change!!!

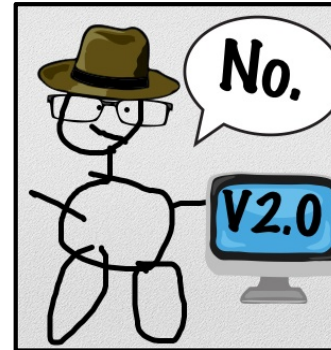
Homework prevents me from passing class.



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](http://blog.secure-medicine.org)

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 Tylenol 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)

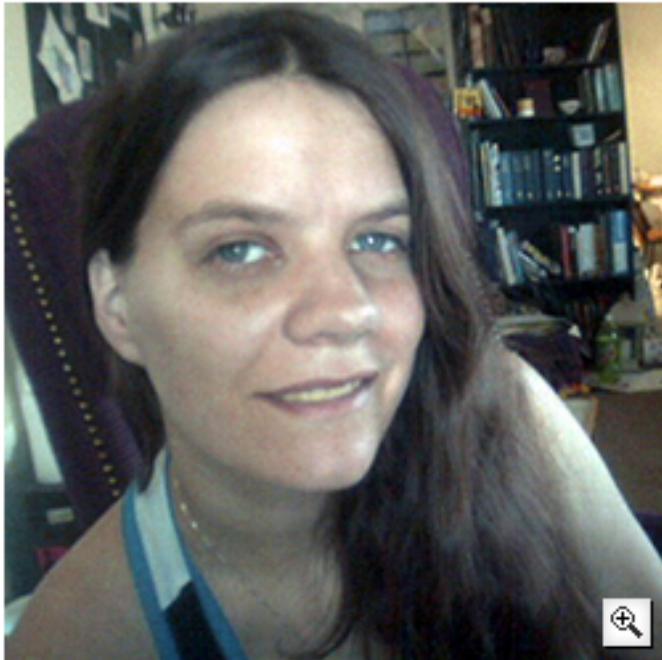
CAMBRIDGE -- FBI agents and State Police investigators searched a Cambridge condominium yesterday that is the longtime home of a leading suspect in the 1982 deaths of seven people from cyanide-laced Tylenol capsules in the Chicago area, one of the most notorious unsolved crimes in the last generation.



# 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.

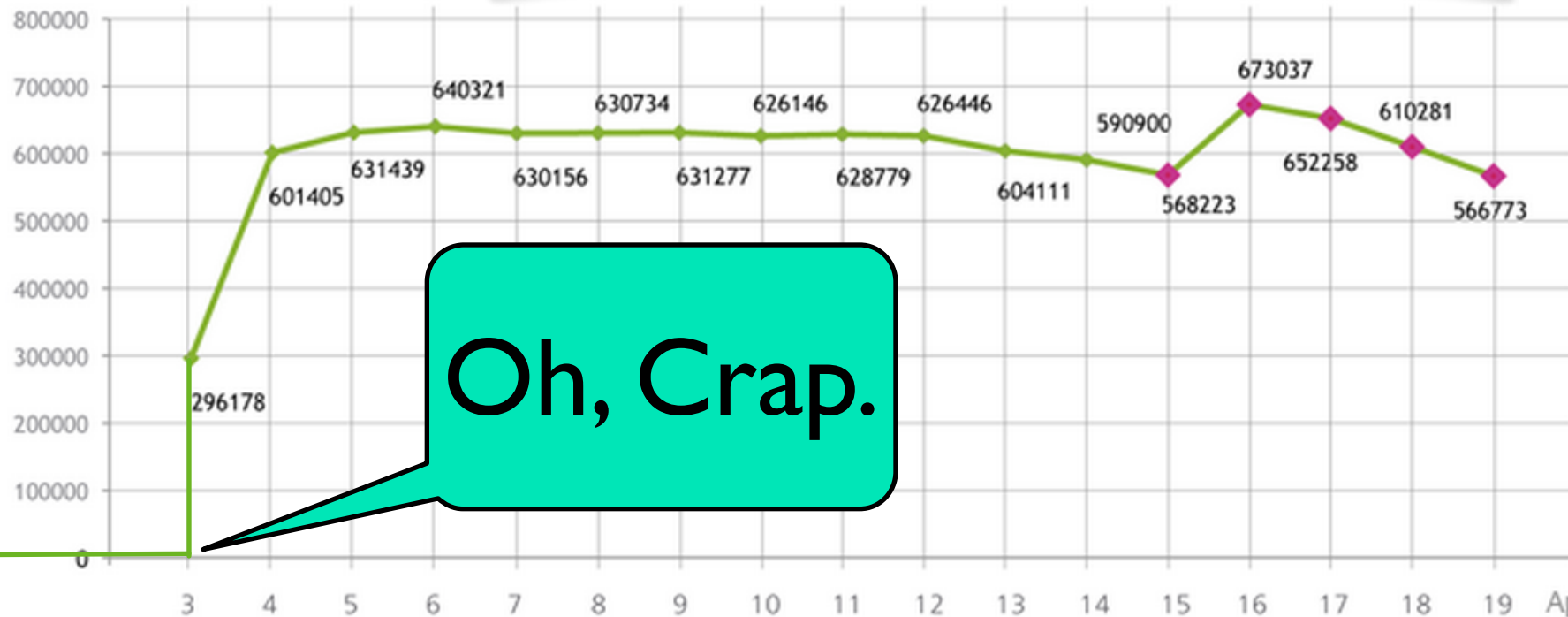
# Lack of Exploits is Not Assurance

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

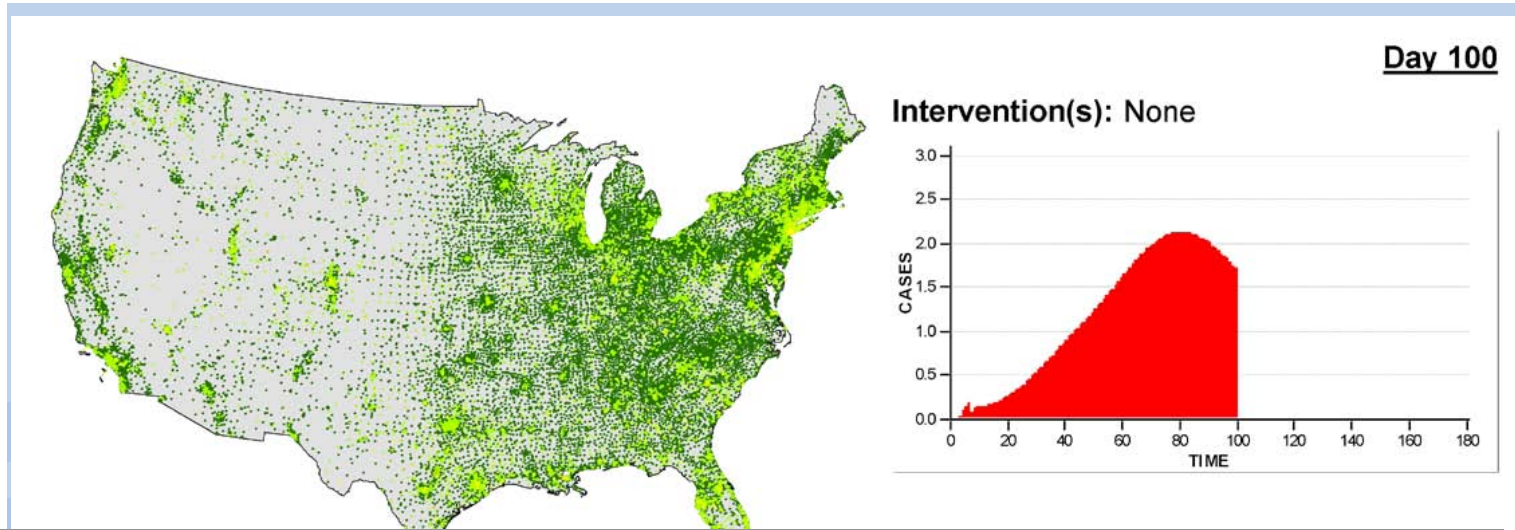


# Security of 156 VA Med. Centers

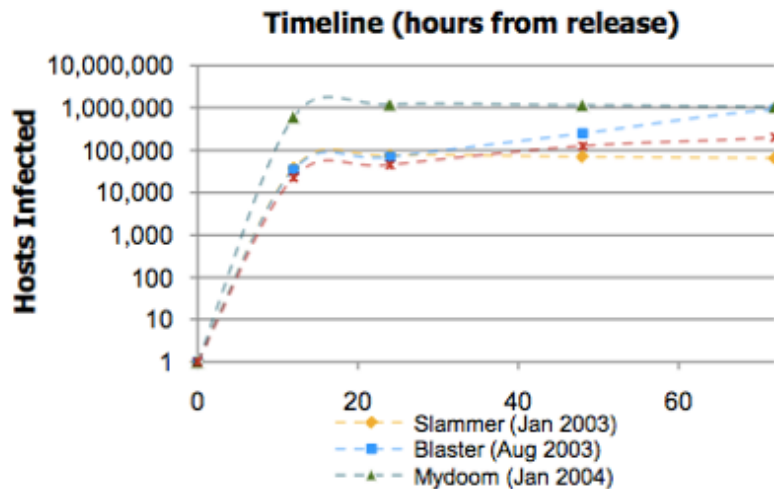
---

- 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

# Disease to Malware: Days to Hours



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

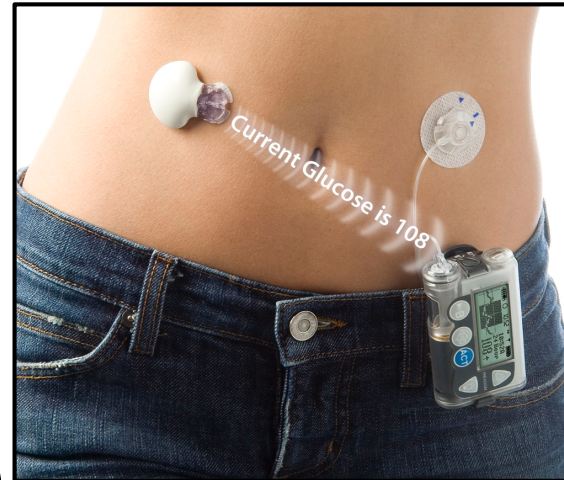




# Halo of Improved Security on Horizon!

"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

# Security Built In: A New Hope?

- Slide excerpt from **Boston Scientific**
- (not me)



## Security Risk Assessment Process

Boston Scientific

Security Risk process parallels safety risk

- Driven by IEC 14971

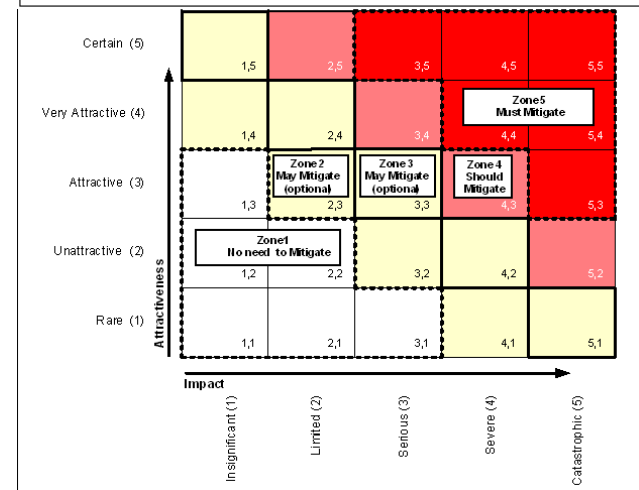
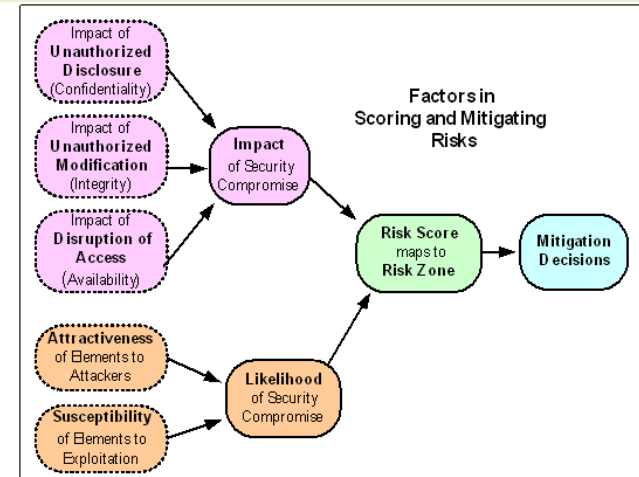
Cross-functional analysis, maintained across development lifecycle

- Starting at **concept phase**

Broad list of threat classes and protectable assets to consider

Risk axes

- Attractiveness (likelihood)
- Impact (severity)

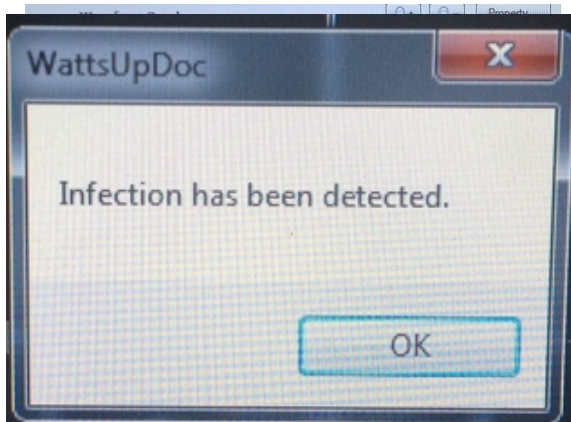
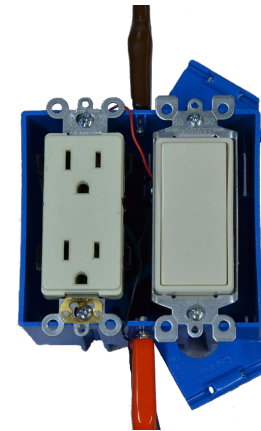
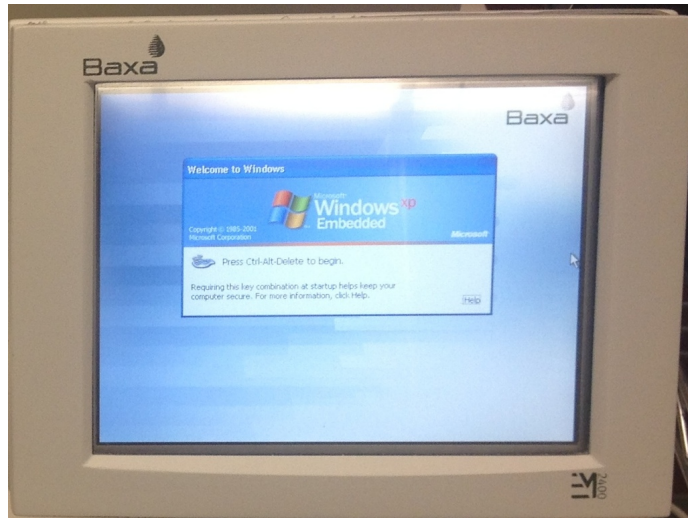


39

Copyright © 2012 by Boston Scientific Corporation or its affiliates. All rights reserved.

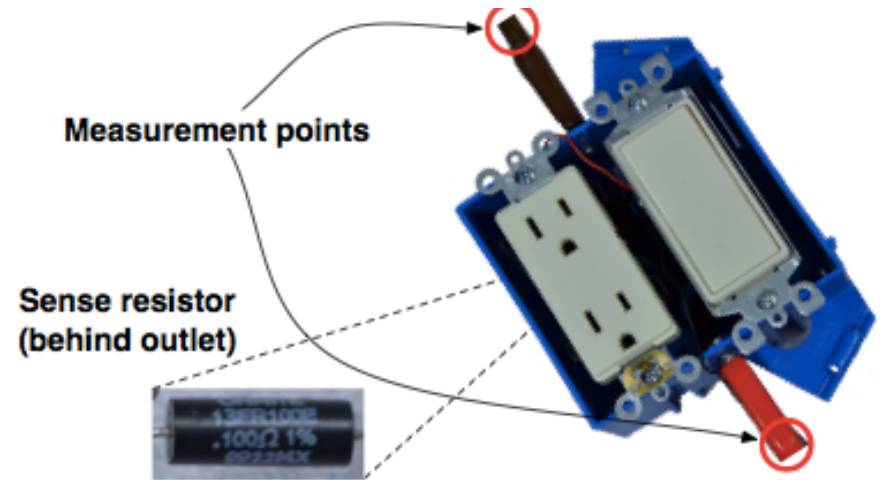
CRM-92205-AA JUN20

# Power Analysis of Medical Devices



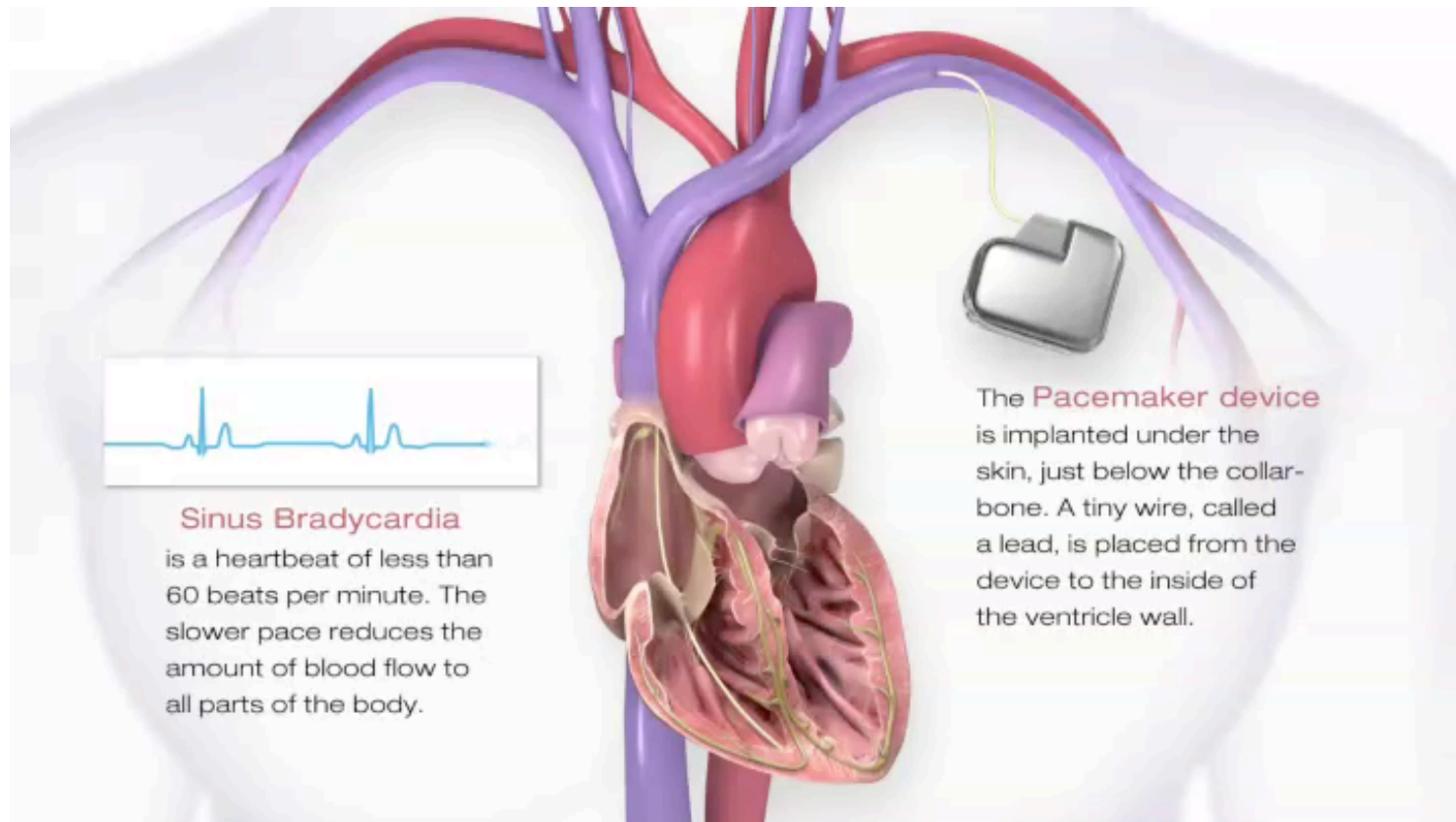
# Power Analysis of Medical Devices

- Power analysis for good!
- Detect malware on medical devices that cannot run conventional anti-virus SW
  - “WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices” by Clark et al. In USENIX HealthTech, 2013.
  - “Potentia est Scientia: Energy Proportionality Enables Whole-System Power Analysis” by Clark et al. In USENIX HotSec, 2012.



# The cardiac cycle

---



*American Heart Association, August 2012*



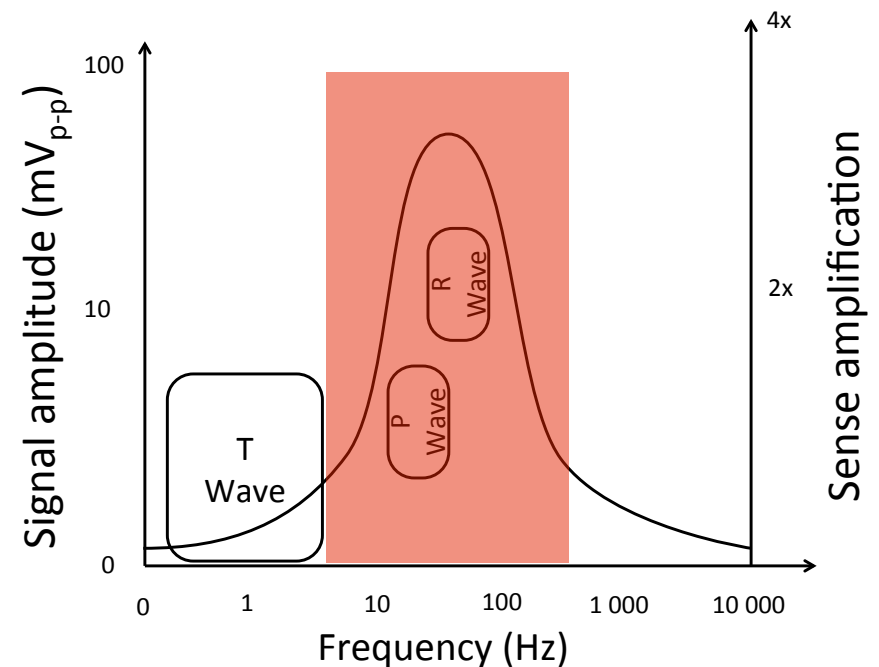
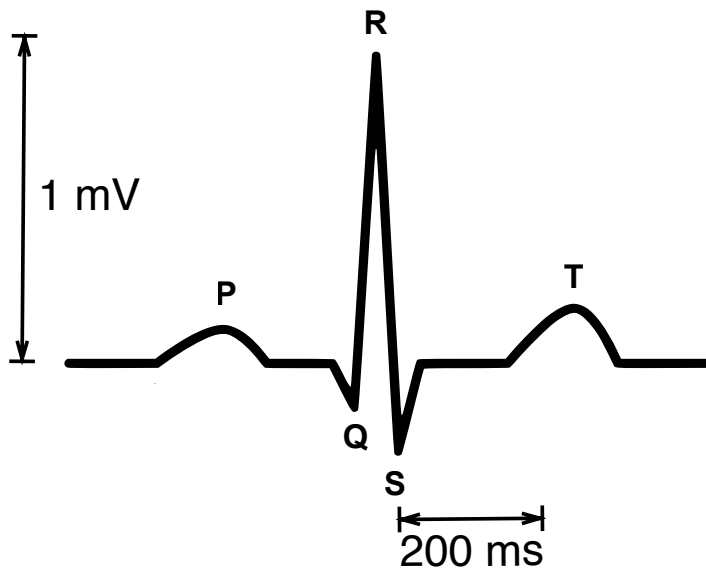
# Cardiac devices and sensor interference?

- Pacemakers, defibrillators
- Electrocardiogram machines



# Cardiac devices vulnerable to baseband EMI

- Filter high frequency
  - 800MHz and GHz range: attenuation of 40dB to 60dB
- Can't filter baseband

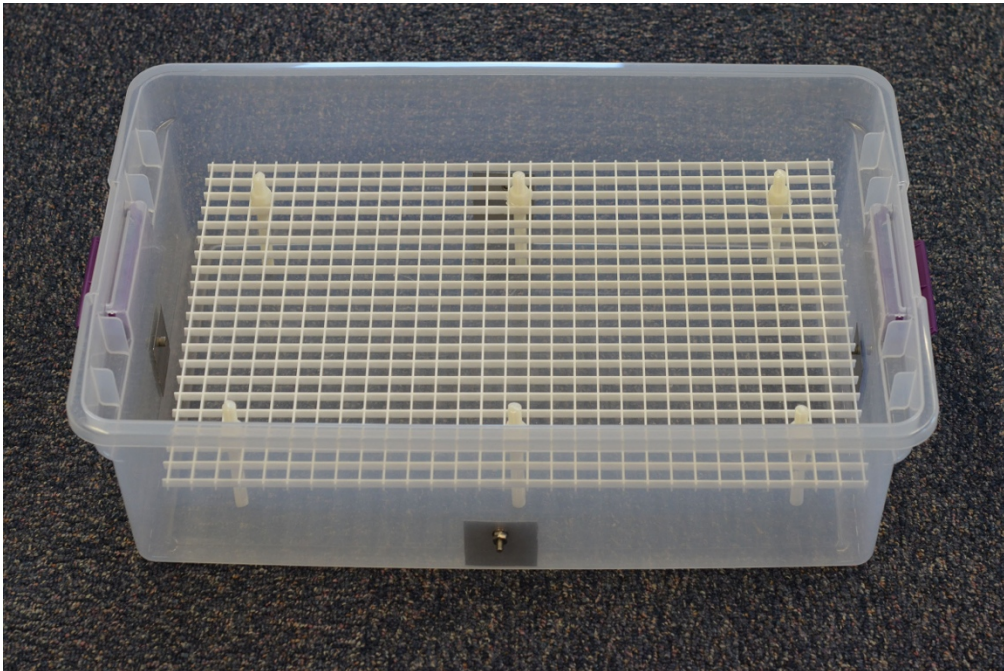


*Cohan et al, 2008*

# Experimental setup: Simulators

---

Saline bath

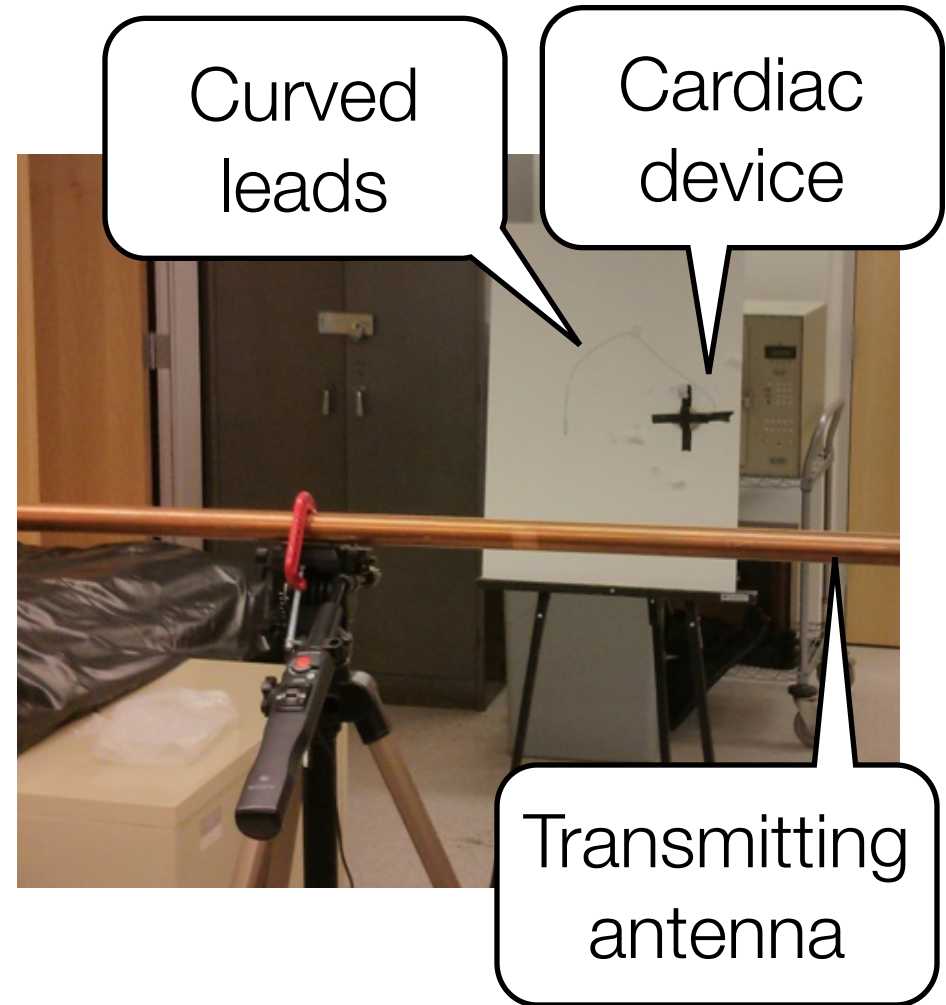
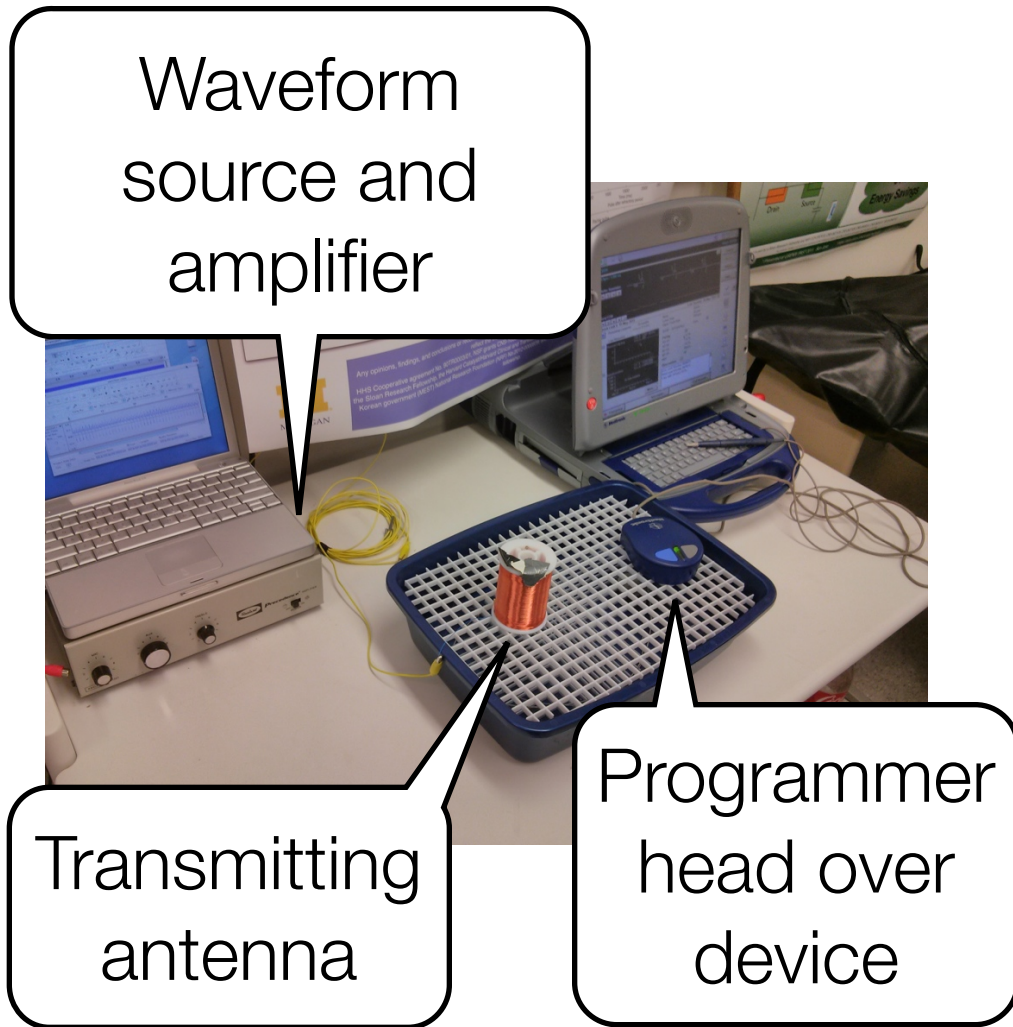


Synthetic human



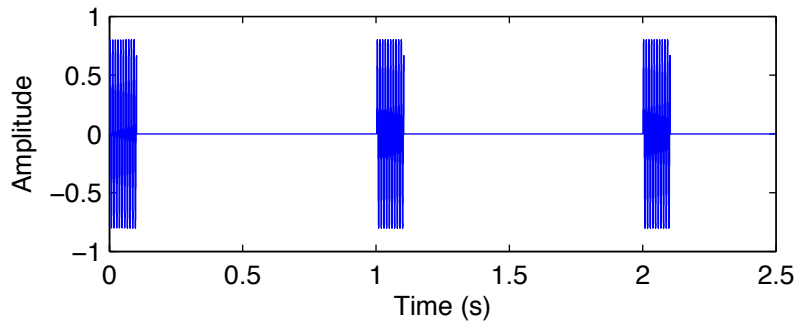


# Experimental setup: Devices and emitters

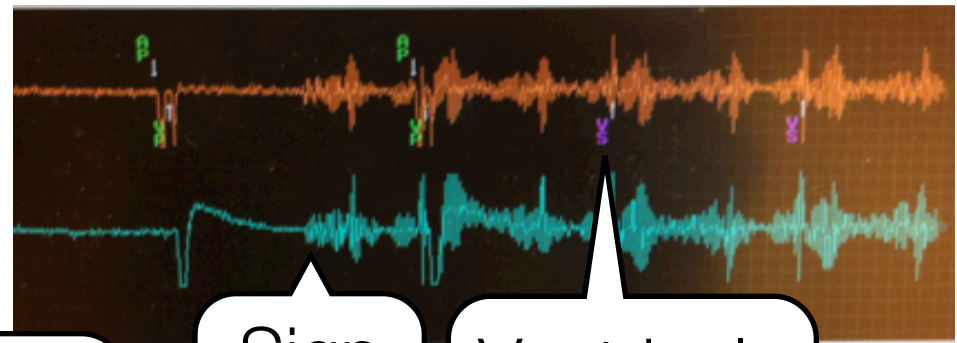
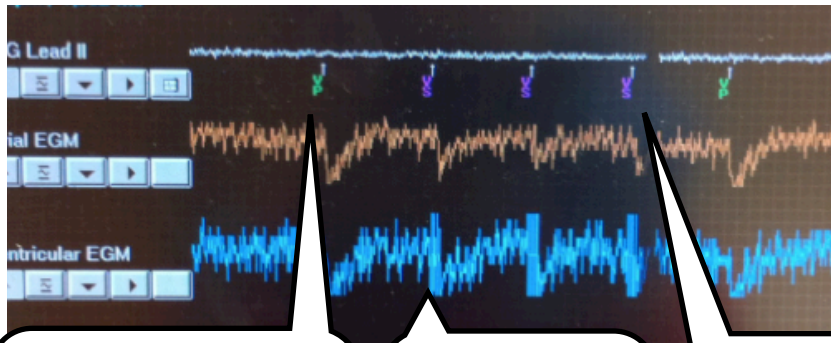
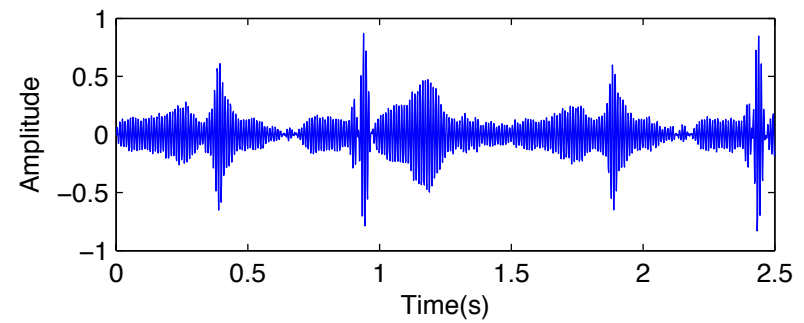


# Results: Waveforms and responses

## Pulsed sinusoid



## Modulated heart beat



Ventricle  
pace

Signal  
onset

Ventricle  
sense

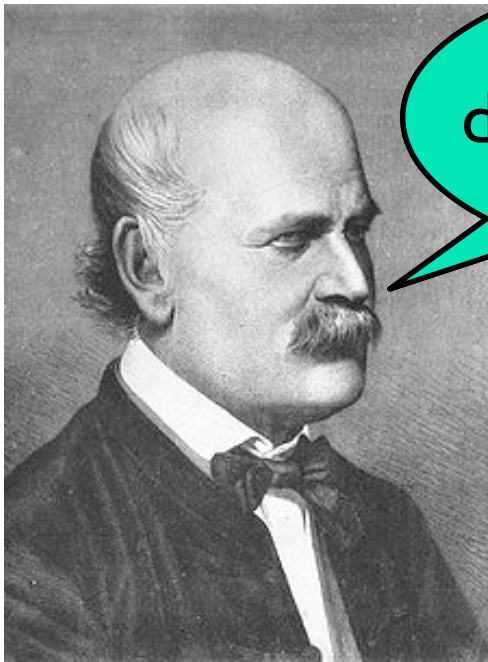
Signal

Ventricle  
sense



# 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>

# Economics of Security

---

- Hacked medical devices = collateral damage
- Spammers just want your bandwidth
  - It takes **1 response out of 12,000,000 spam** emails to turn a profit
  - Botnets are sold on the **black market**
- Idea: Find technical approaches that make your devices worthless for spammers and botnets.



# Cybersecurity: A Foreseeable Risk

- Biggest risk at the moment:
  - ~~Hackers breaking into medical devices~~
  - Wide-scale **unavailability** of patient care
  - **Integrity** of medical sensors
- Security can't be bolted on.
  - Build it in during manufacturing
  - Don't interrupt clinical workflow
  - Plan ahead: V&V for patches of foreseeable risks
- Hospitals should
  - **Procurement processes:** Require meaningful cybersecurity (ask how quickly vendor will patch new Windows XP vulnerabilities)
  - **Report near misses** via voluntary MedWatch Form 3500
  - Read [blog.secure-medicine.org](http://blog.secure-medicine.org)

