Medical Device System Security

Kevin Fu

Associate Professor

Security & Privacy Research Lab

UMass Amherst Computer Science

☞ University of Michigan EECS

http://SPQR.cs.umass.edu/

Supported in part by a Sloan Research Fellowship, NSF CNS-0831244, HHS 90TR0003/01. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

ACCE
July 2012

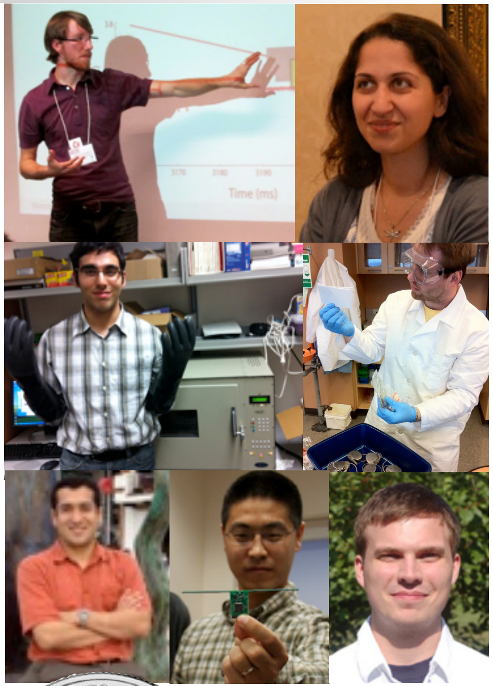
Acknowledgments

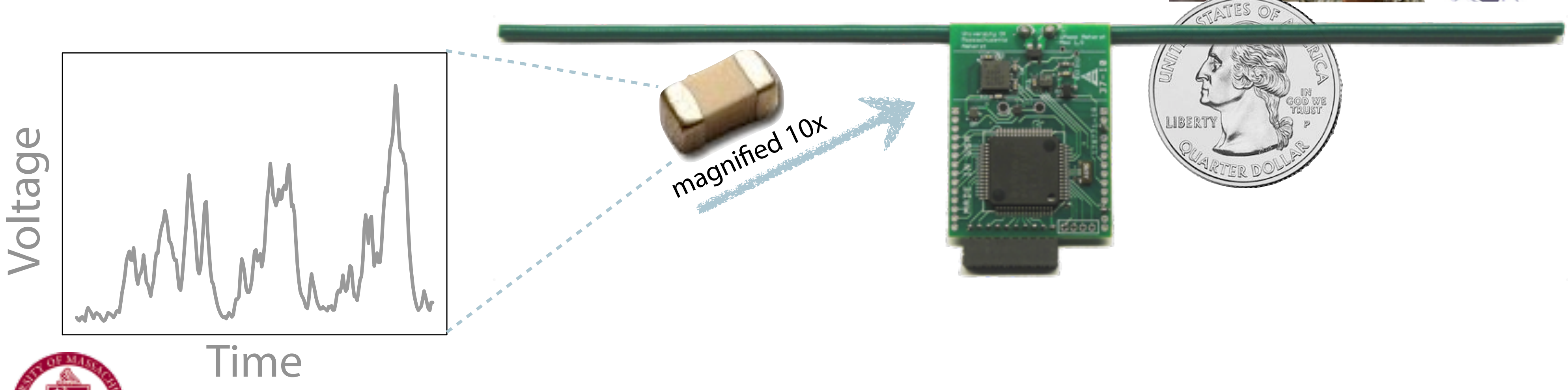
- CS faculty and physicians
  - Prof. Dina Katabi, MIT Computer Science and AI Lab
  - Prof. Tadayoshi Kohno, University of Washington CSE
  - Dr. Daniel Kramer, BIDMC, Harvard Med School
  - Dr. William Maisel, BIDMC, Harvard Med School (fmr)
  - Dr. Matthew Reynolds, BIDMC, Harvard Med School
  - Prof.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

SPQR Lab [Security & Privacy Research Lab]

- Cybersecurity
  - Medical devices, RFID
- Stochastic computing
  - Rethinking HW-SW interfaces to reduce energy
  - Probabilistic storage in low-voltage NOR flash
  - Zero-power clocks for smartcards

Today's talk





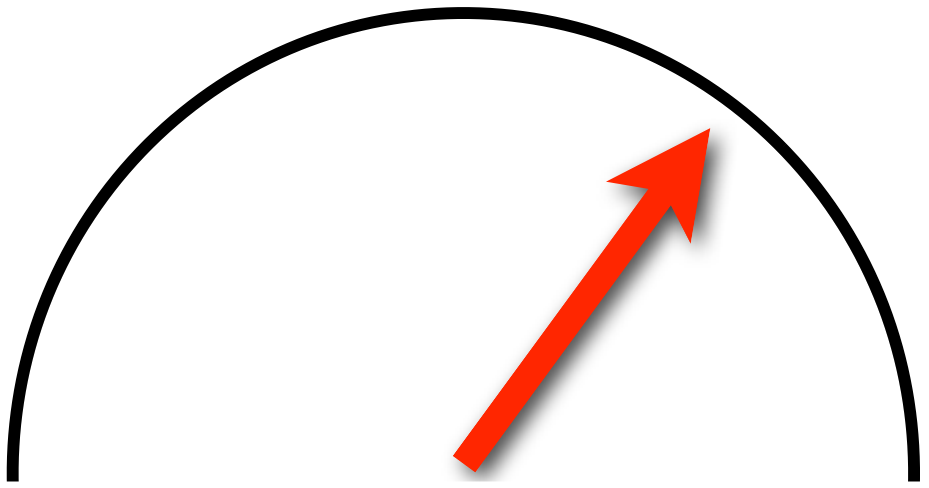
Disclosures

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

Hat: zazzle.com

- This presentation is based on both my own research and the research of others. None of the opinions, findings, or conclusions necessarily reflect the views of my past or present employers.

Accumulative Risks of...



Accidents

Unsafe Practices

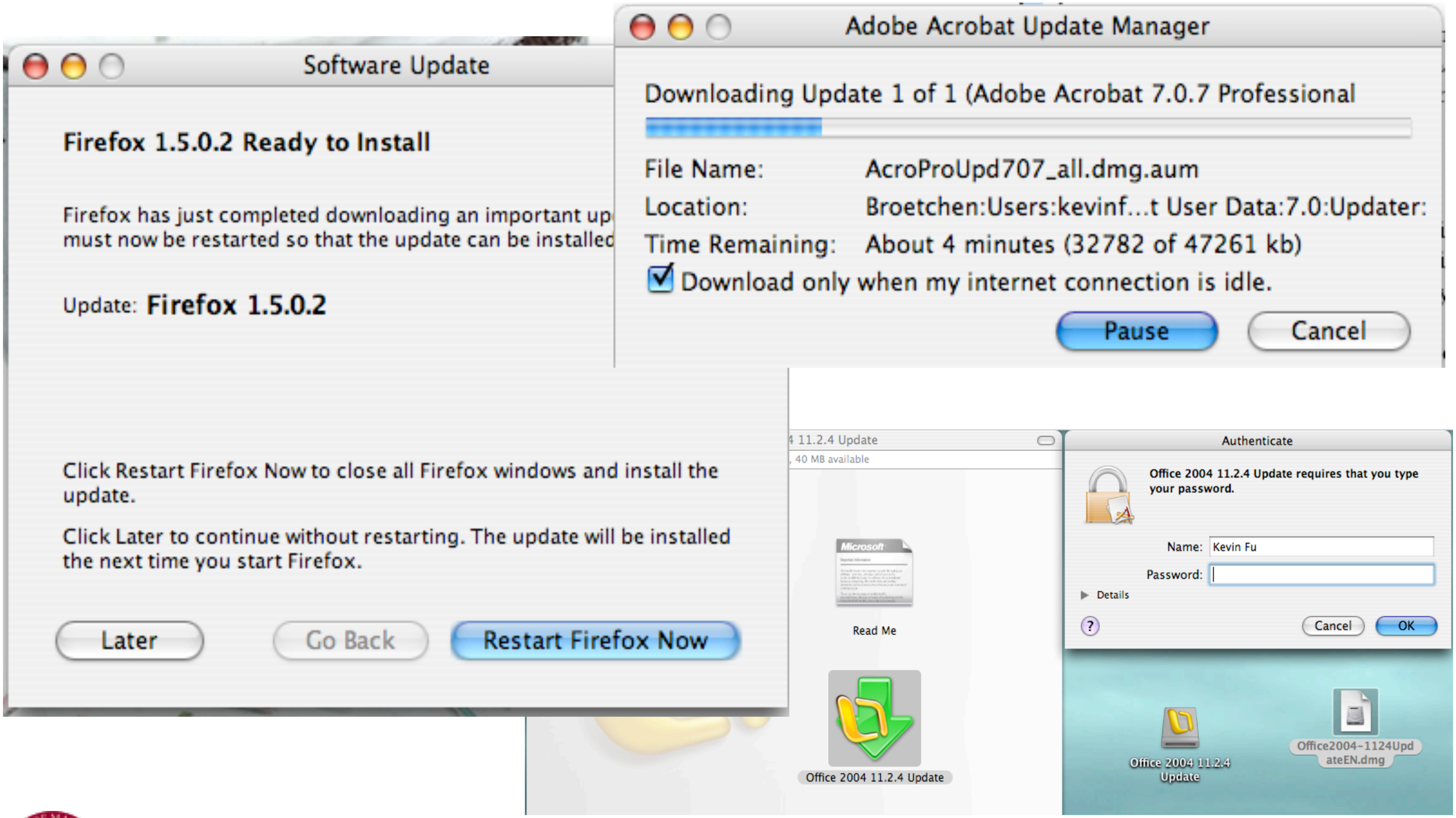
Sabotage

Threat-o-meter

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)

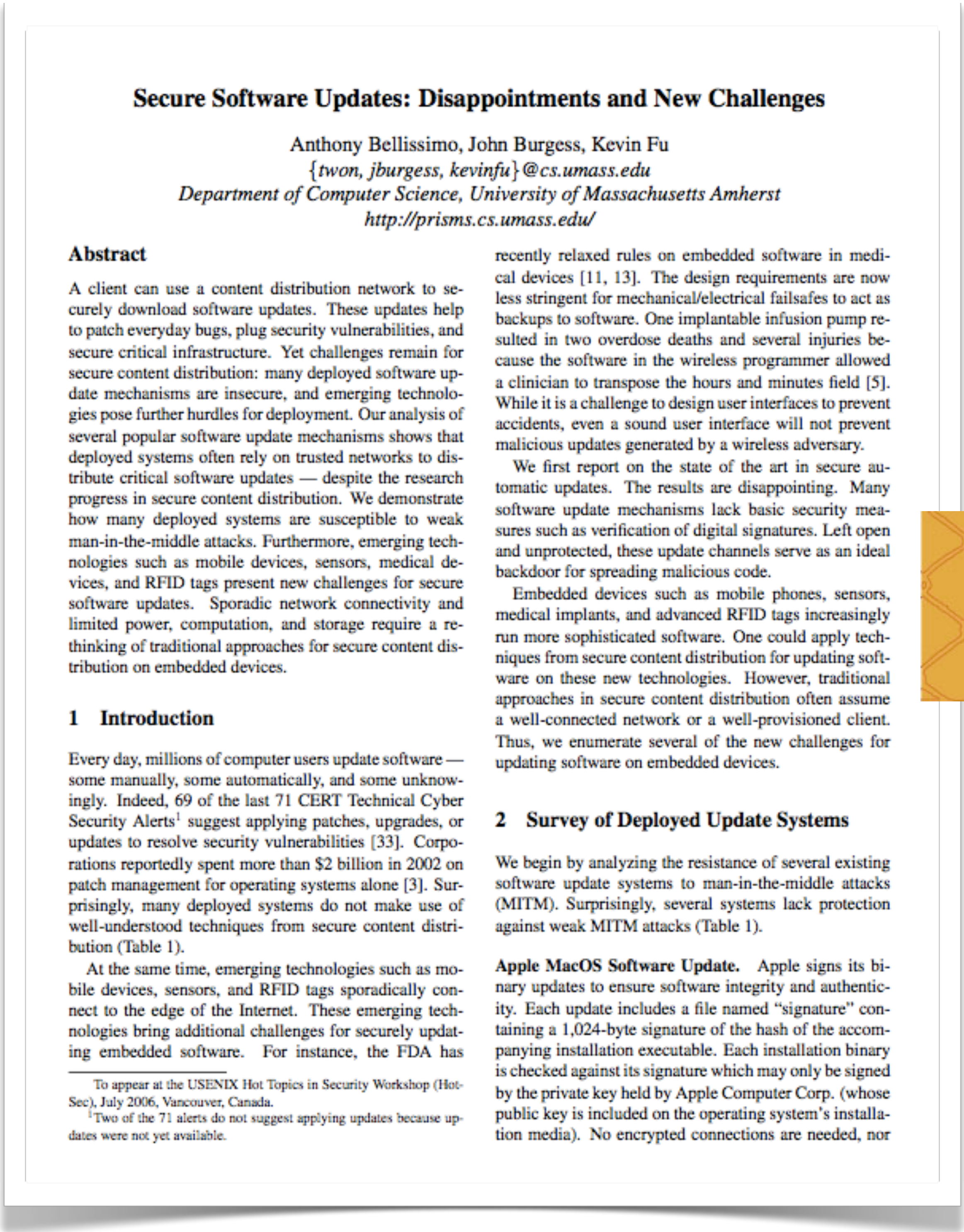
☑ Download only when my internet connection is idle.

Authenticate

Office 2004 11.2.4 Update requires that you type your password.

Name: Kevin Fu

Password:



Secure Software Updates: Disappointments and New Challenges

Anthony Bellissimo, John Burgess, Kevin Fu
{twon, jburgess, kevinfu}@cs.umass.edu
Department of Computer Science, University of Massachusetts Amherst
http://prisms.cs.umass.edu/

Abstract

A client can use a content distribution network to securely download software updates. These updates help to patch everyday bugs, plug security vulnerabilities, and secure critical infrastructure. Yet challenges remain for secure content distribution: many deployed software update mechanisms are insecure, and emerging technologies pose further hurdles for deployment. Our analysis of several popular software update mechanisms shows that deployed systems often rely on trusted networks to distribute critical software updates — despite the research progress in secure content distribution. We demonstrate how many deployed systems are susceptible to weak man-in-the-middle attacks. Furthermore, emerging technologies such as mobile devices, sensors, medical devices, and RFID tags present new challenges for secure software updates. Sporadic network connectivity and limited power, computation, and storage require a rethinking of traditional approaches for secure content distribution on embedded devices.

1 Introduction

Every day, millions of computer users update software — some manually, some automatically, and some unknowingly. Indeed, 69 of the last 71 CERT Technical Cyber Security Alerts[1] suggest applying patches, upgrades, or updates to resolve security vulnerabilities [33]. Corporations reportedly spent more than $2 billion in 2002 on patch management for operating systems alone [3]. Surprisingly, many deployed systems do not make use of well-understood techniques from secure content distribution (Table 1).

At the same time, emerging technologies such as mobile devices, sensors, and RFID tags sporadically connect to the edge of the Internet. These emerging technologies bring additional challenges for securely updating embedded software. For instance, the FDA has recently relaxed rules on embedded software in medical devices [11, 13]. The design requirements are now less stringent for mechanical/electrical failsafes to act as backups to software. One implantable infusion pump resulted in two overdose deaths and several injuries because the software in the wireless programmer allowed a clinician to transpose the hours and minutes field [5]. While it is a challenge to design user interfaces to prevent accidents, even a sound user interface will not prevent malicious updates generated by a wireless adversary.

We first report on the state of the art in secure automatic updates. The results are disappointing. Many software update mechanisms lack basic security measures such as verification of digital signatures. Left open and unprotected, these update channels serve as an ideal backdoor for spreading malicious code.

Embedded devices such as mobile phones, sensors, medical implants, and advanced RFID tags increasingly run more sophisticated software. One could apply techniques from secure content distribution for updating software on these new technologies. However, traditional approaches in secure content distribution often assume a well-connected network or a well-provisioned client. Thus, we enumerate several of the new challenges for updating software on embedded devices.

2 Survey of Deployed Update Systems

We begin by analyzing the resistance of several existing software update systems to man-in-the-middle attacks (MITM). Surprisingly, several systems lack protection against weak MITM attacks (Table 1).

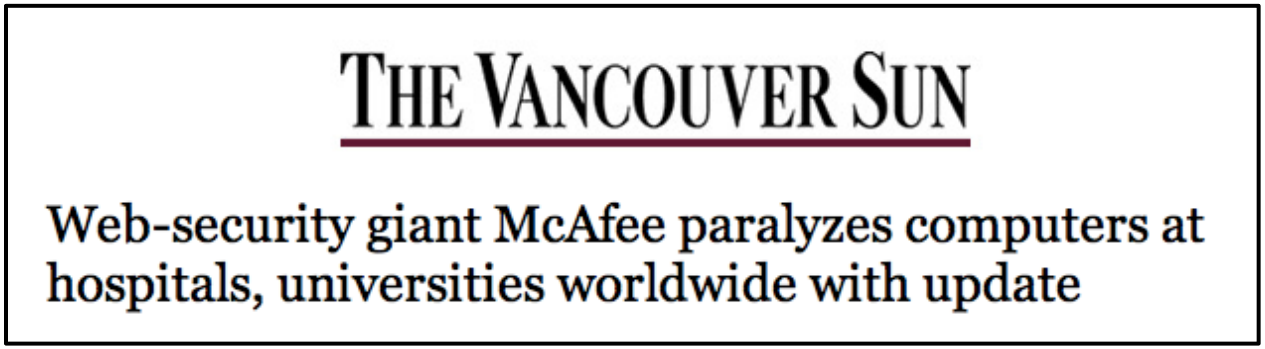
Apple MacOS Software Update. Apple signs its binary updates to ensure software integrity and authenticity. Each update includes a file named "signature" containing a 1,024-byte signature of the hash of the accompanying installation executable. Each installation binary is checked against its signature which may only be signed by the private key held by Apple Computer Corp. (whose public key is included on the operating system's installation media). No encrypted connections are needed, nor

To appear at the USENIX Hot Topics in Security Workshop (HotSec), July 2006, Vancouver, Canada.

[1] Two of the 71 alerts do not suggest applying updates because updates were not yet available.

Software Update Woes

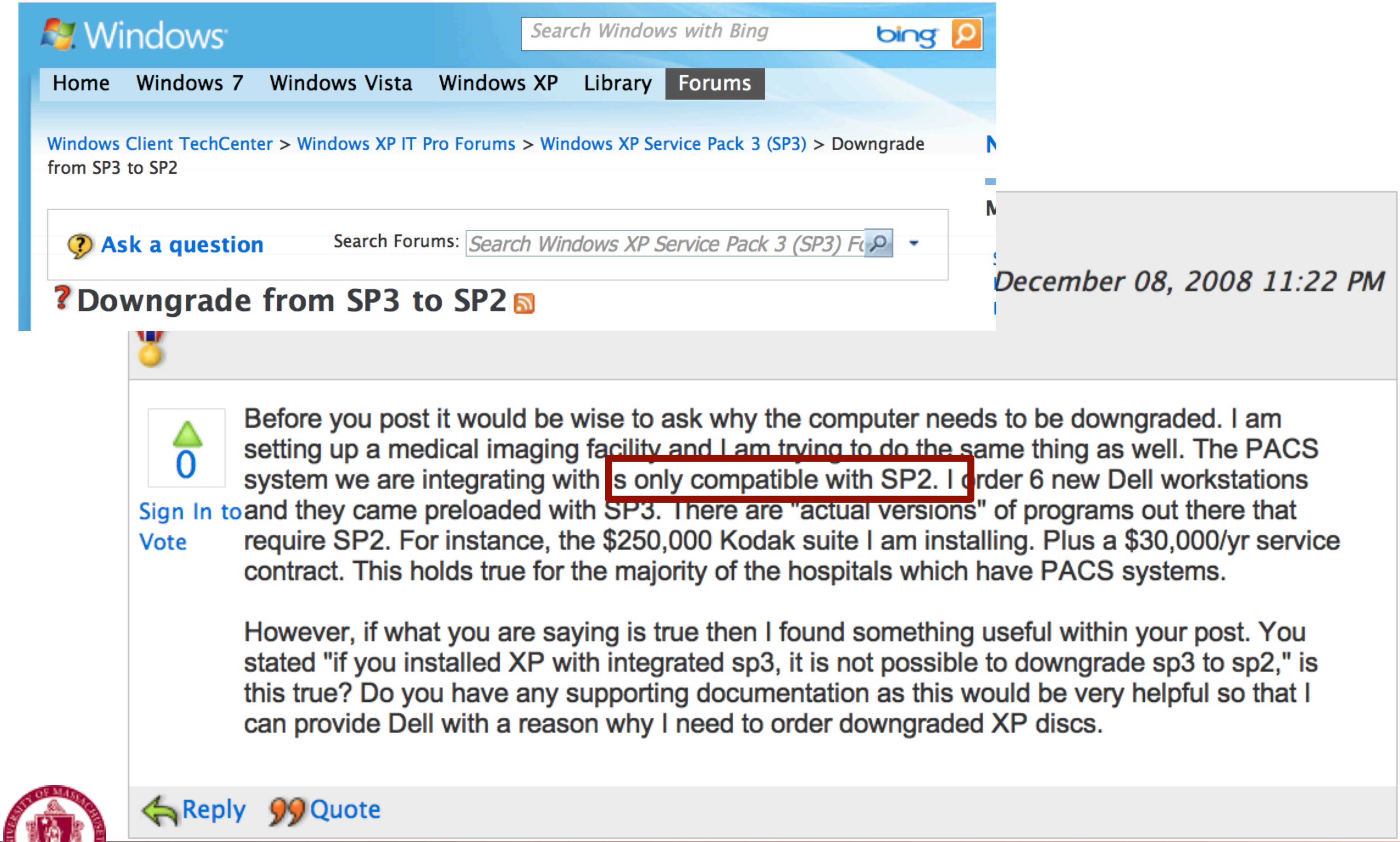
- Health Information Technology (HIT) devices globally rendered unavailable
- Cause: Automated software update went haywire
- Numerous hospitals were affected April 21, 2010
  - Rhode Island: a third of the hospitals were forced ``to postpone elective surgeries and stop treating patients without traumas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

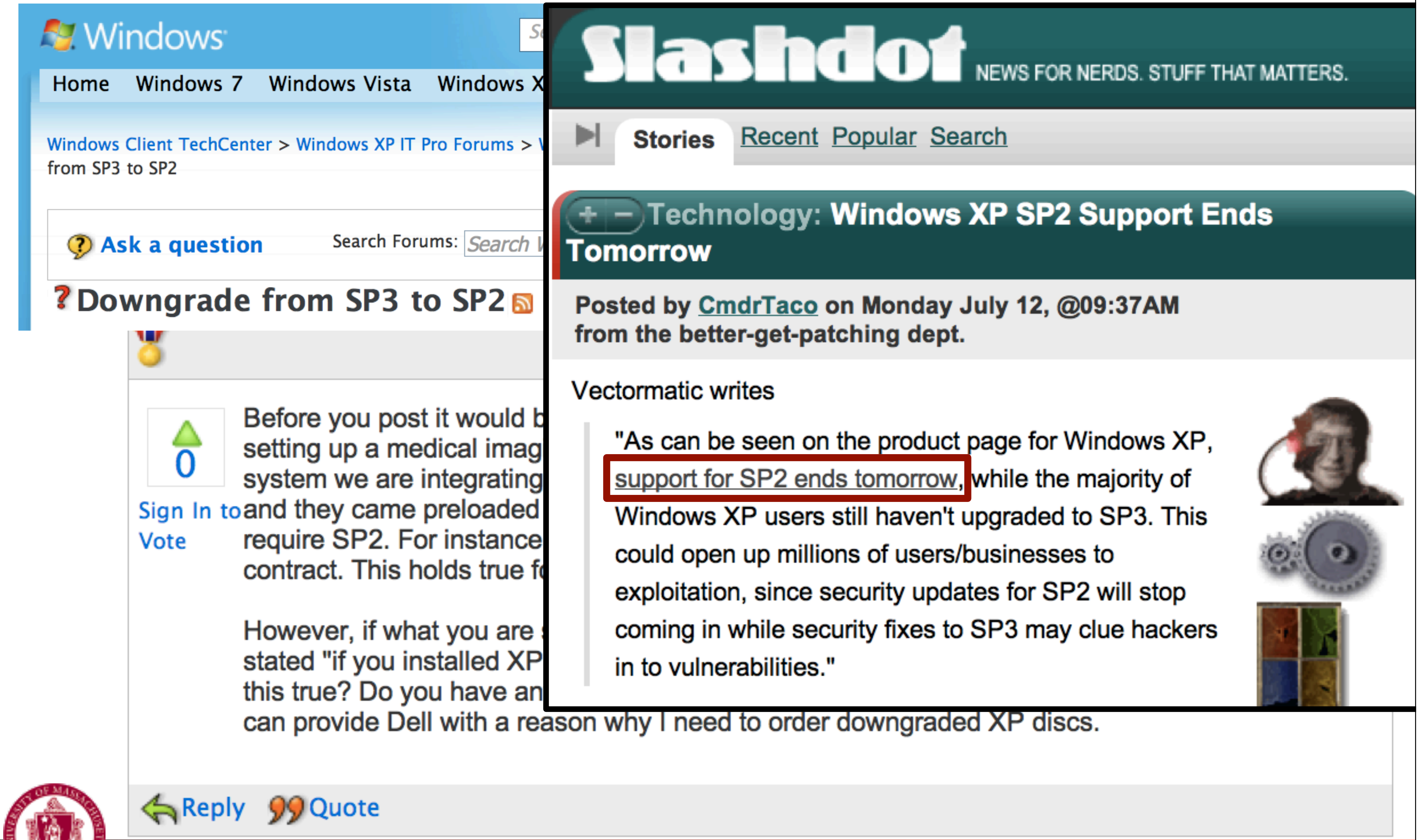
Downgrade from SP3 to SP2

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



Windows
Home Windows 7 Windows Vista Windows X
Windows Client TechCenter > Windows XP IT Pro Forums > W
from SP3 to SP2
Ask a question
Search Forums: Search W

? 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 s
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.

Slashdot NEWS FOR NERDS. STUFF THAT MATTERS.
Stories Recent Popular Search

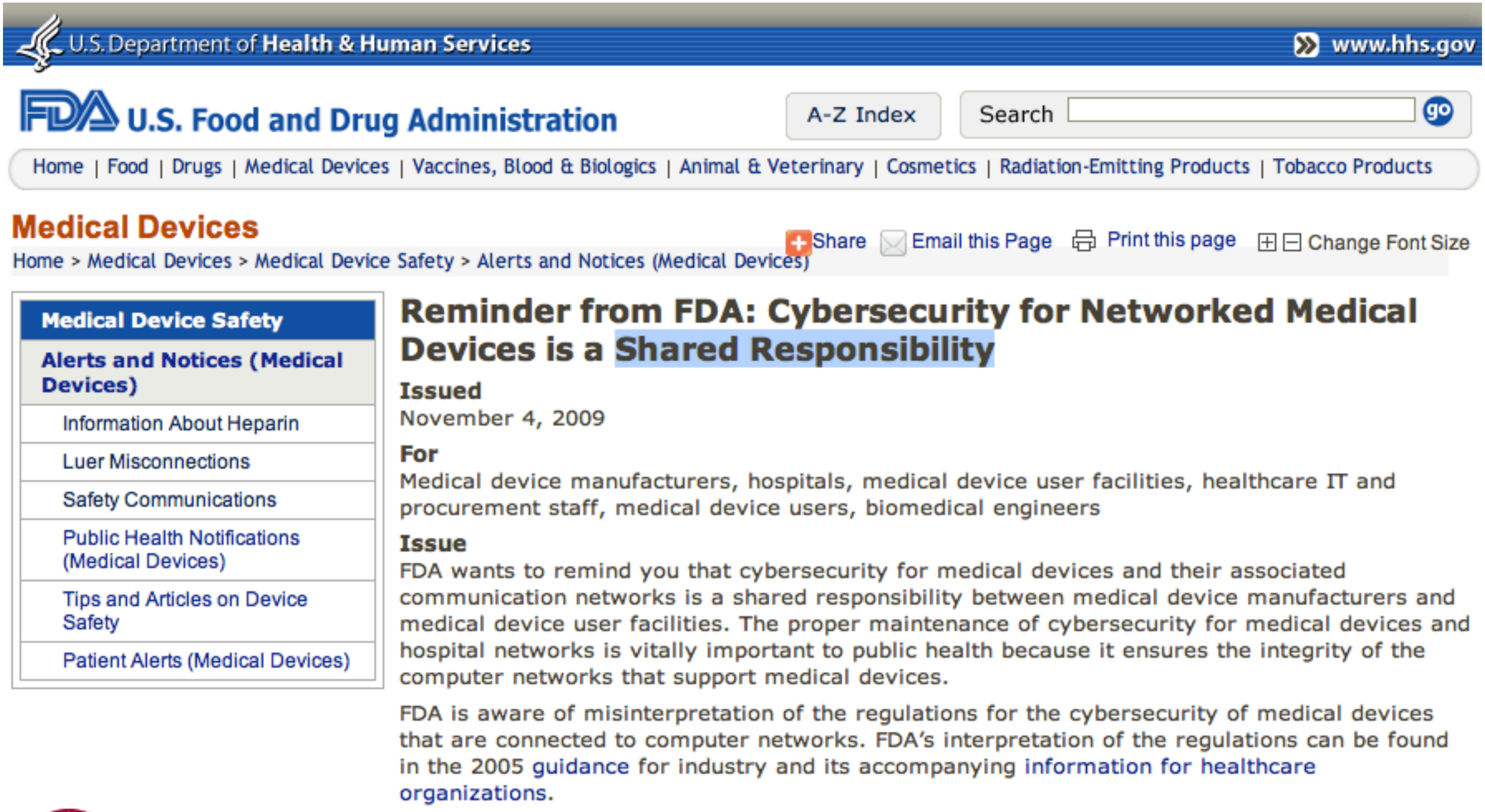
Technology: Windows XP SP2 Support Ends Tomorrow

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."

Still Not It: Hospitals, Manufacturers


U.S. Department of Health & Human Services
www.hhs.gov
FDA U.S. Food and Drug Administration
A-Z Index
Search
go
Home | Food | Drugs | Medical Devices | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Radiation-Emitting Products | Tobacco Products
Medical Devices
Share
Email this Page
Print this page
Change Font Size
Home > Medical Devices > Medical Device Safety > Alerts and Notices (Medical Devices)
Medical Device Safety
Alerts and Notices (Medical Devices)
Information About Heparin
Luer Misconnections
Safety Communications
Public Health Notifications (Medical Devices)
Tips and Articles on Device Safety
Patient Alerts (Medical Devices)

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

Issued

November 4, 2009

For

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

Issue

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

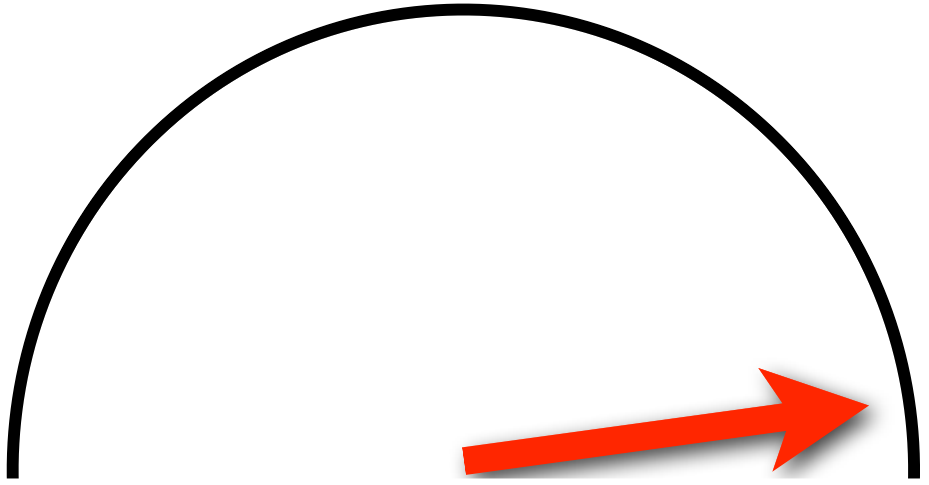
FDA is aware of misinterpretation of the regulations for the cybersecurity of medical devices that are connected to computer networks. FDA's interpretation of the regulations can be found in the 2005 guidance for industry and its accompanying information for healthcare organizations.

Managerial issues:

Diffusion of responsibility

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

Accumulative Risks of...



Accidents

Unsafe Practices

Sabotage

Threat-o-meter

Benefits of Wireless

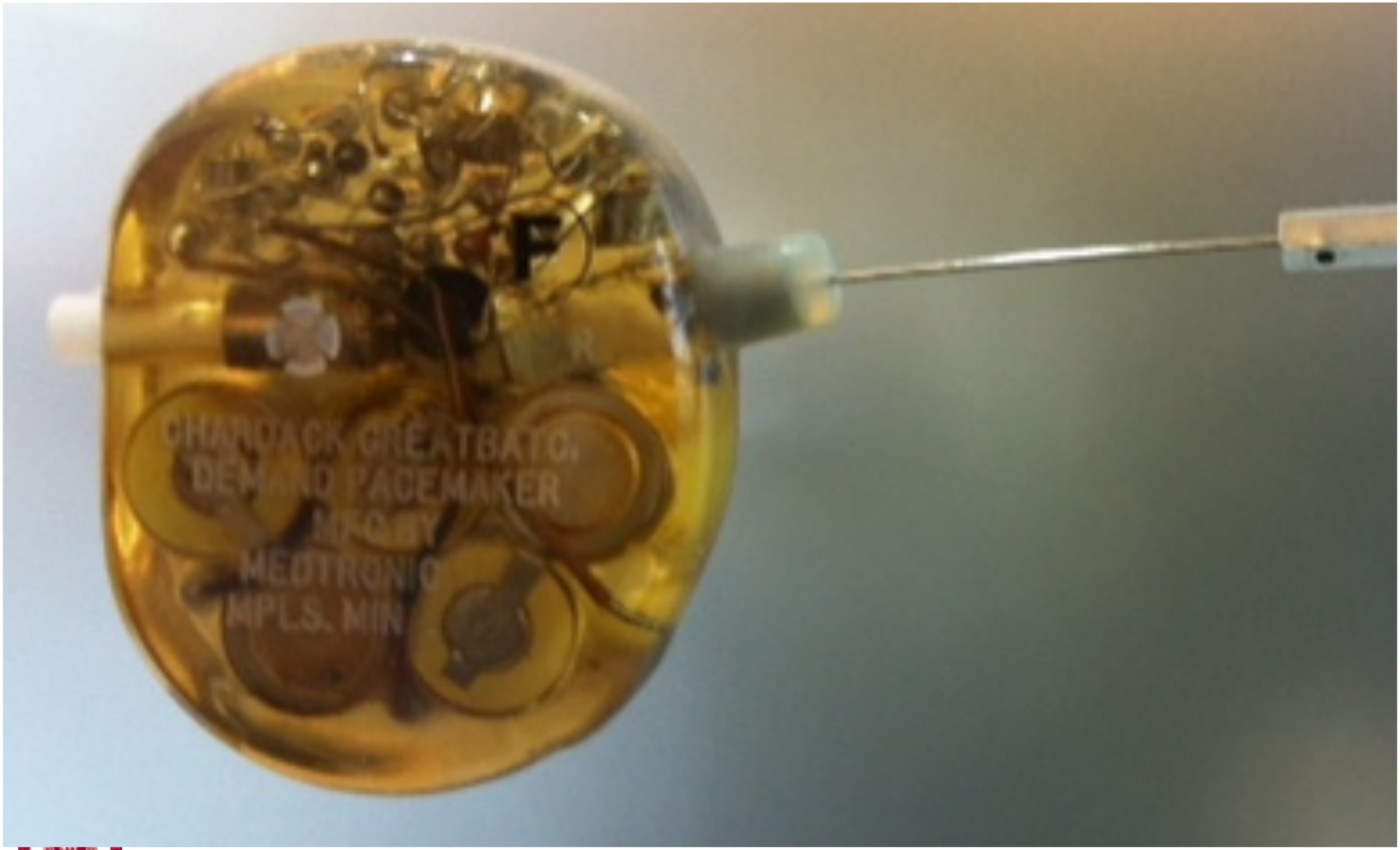
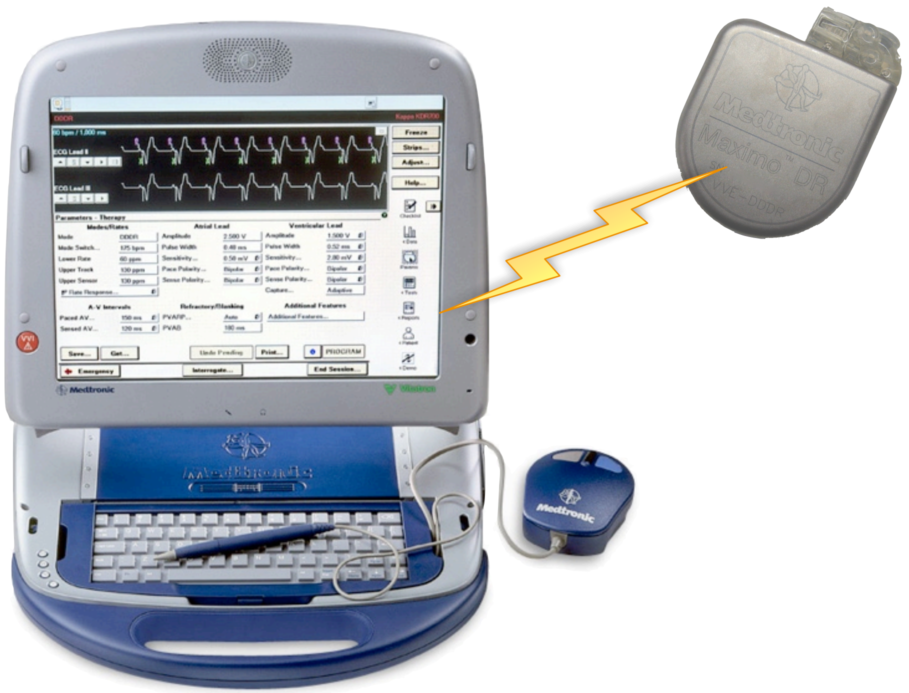


Photo by Kevin Fu @ Medtronic museum

Implantation of Defibrillator

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

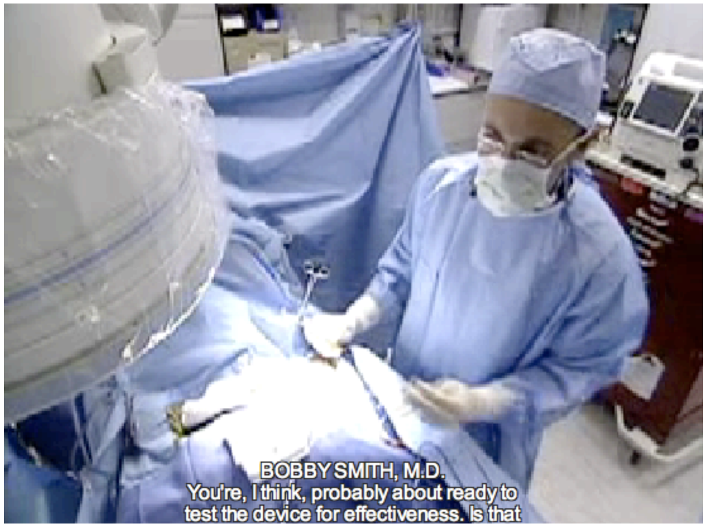


Device Programmer

Photos: Medtronic; Video: or-live.com

Implantation of Defibrillator

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

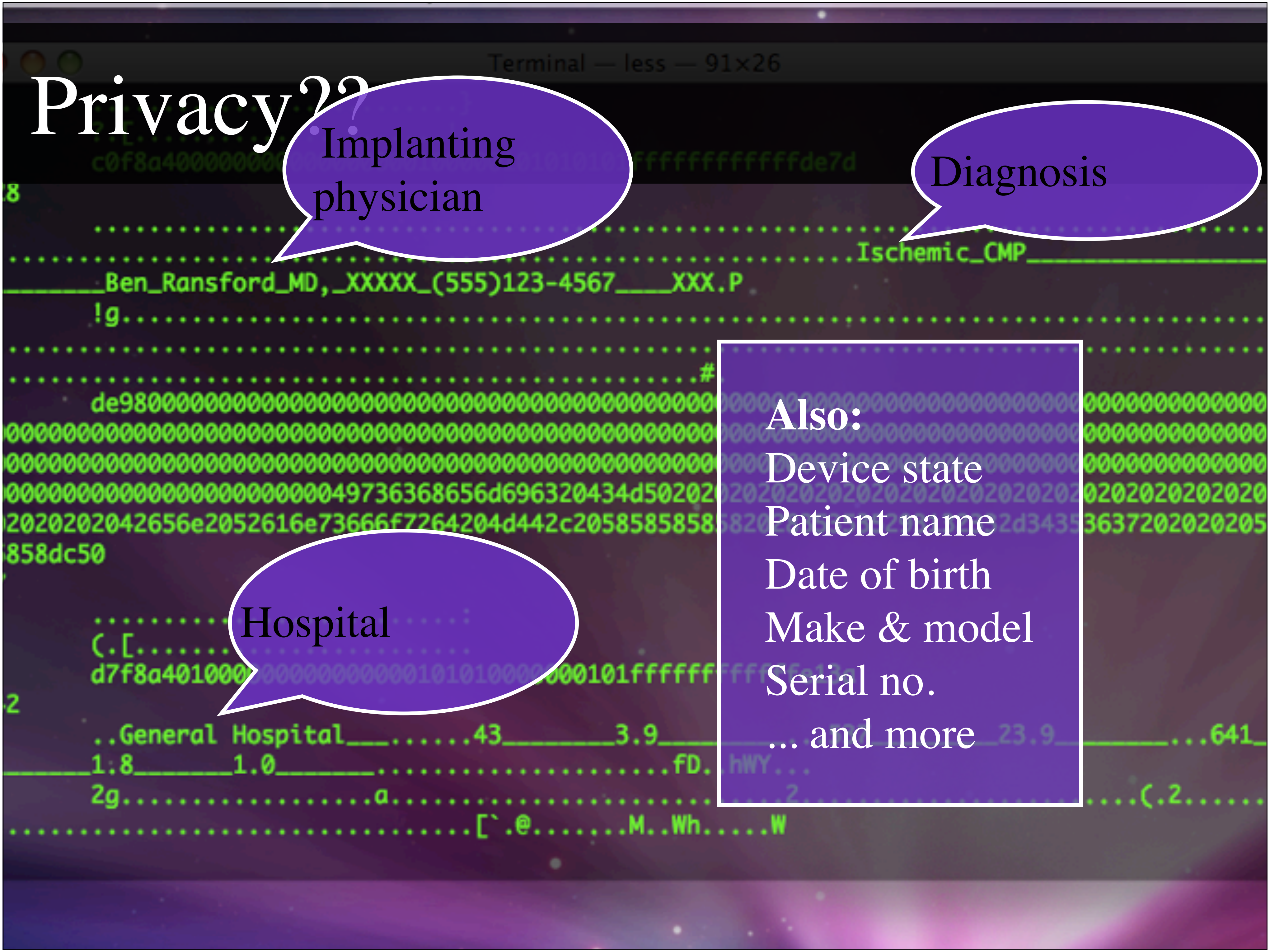
Implantation of Defibrillator

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

Home monitor

Photos: Medtronic; Video: or-live.com

Privacy??



```
    c0f8a4000000000                                  ffffffffffffde7d
8
    ..................................................................................
.......................................................................Ischemic_CMP__________________
________Ben_Ransford_MD,_XXXXX_(555)123-4567____XXX.P
    !g....................................................................................
.......................................................................................
.........................................................#
    de9800000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000004973636865 6d696320434d50202020202020202020202020202020202020202020202020
2020202042656e2052616e73666f7264204d442c20585858585858202d3435363720202020205
858dc50

    ..........
    (.[.......
    d7f8a4010000000000000000010101000000000101ffffffffff
2
    ..General Hospital___......43_________3.9_______________23.9__________...641_
________1.8________1.0__________......................fD..hWY...
    2g..................a..............................2...................(.2......
..................................[`.@........M..Wh.....W
```

Implanting physician

Diagnosis

Hospital

Also:

Device state

Patient name

Date of birth

Make & model

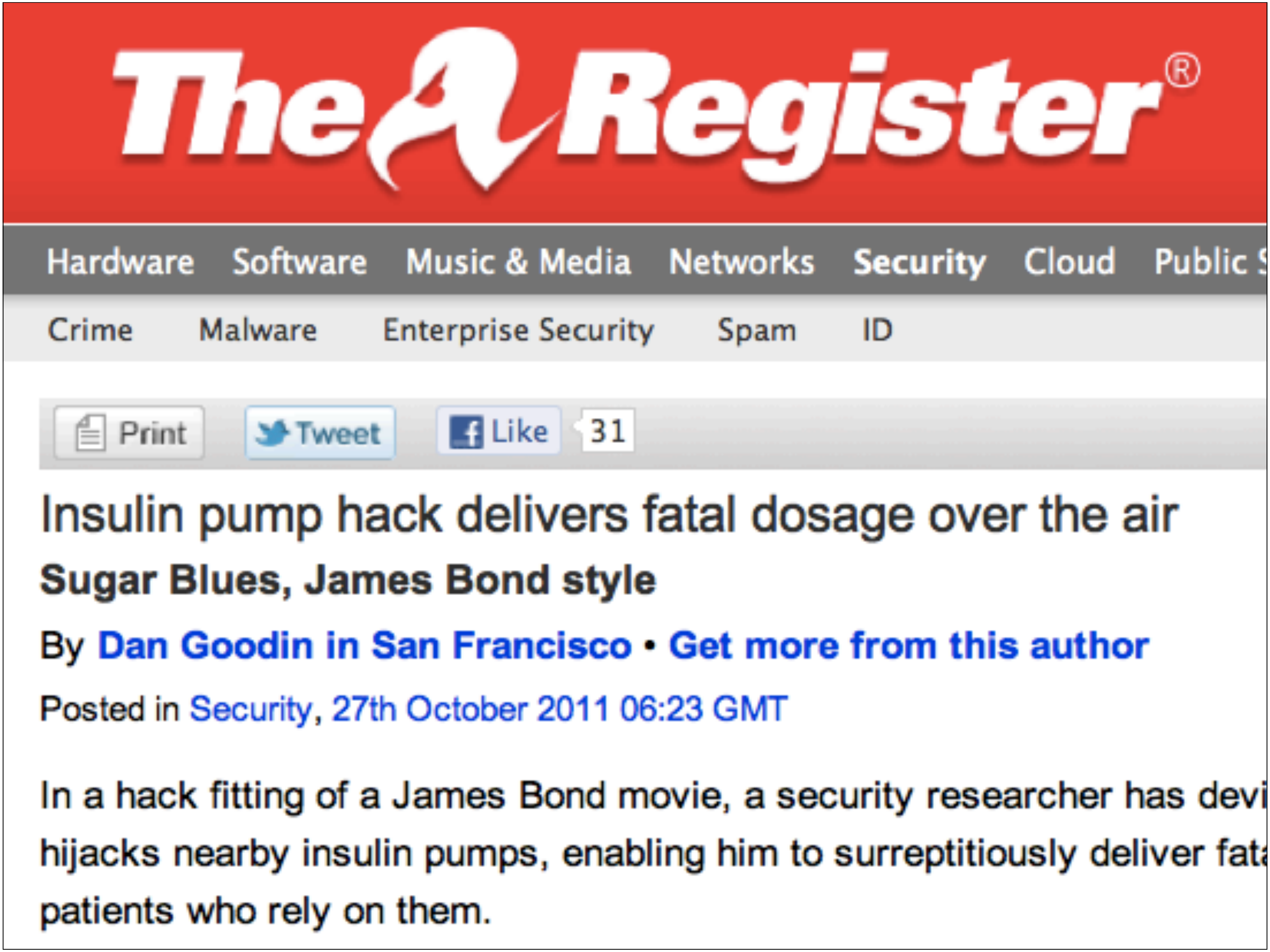
Serial no.

... and more

Wirelessly Induce Fatal Heart Rhythm

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

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



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

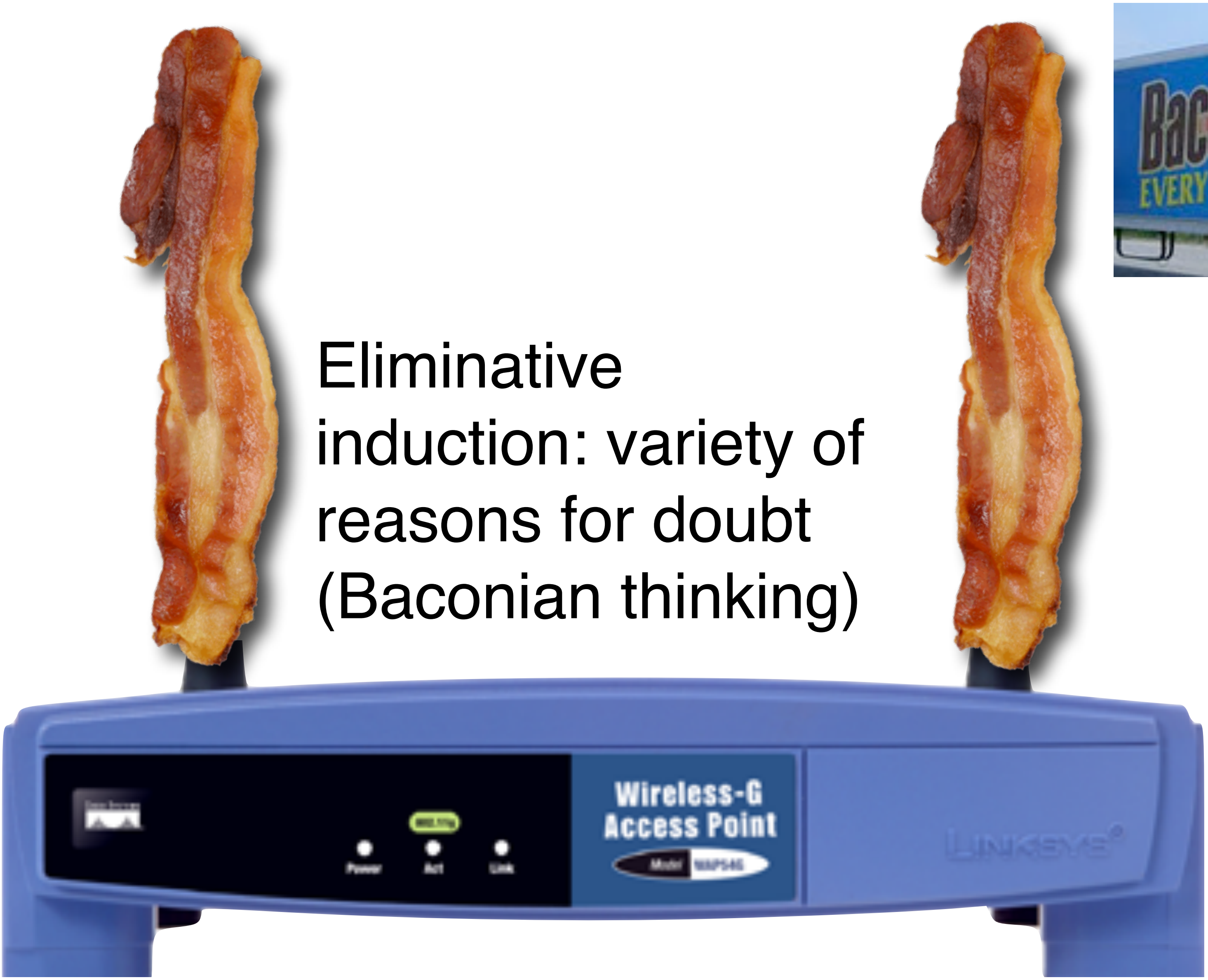
In a hack fitting of a James Bond movie, a security researcher has devi
hijacks nearby insulin pumps, enabling him to surreptitiously deliver fata
patients who rely on them.

Wireless medical devices:

great benefits.

subtle inconvenient risks.

Wireless Makes Everything Better?

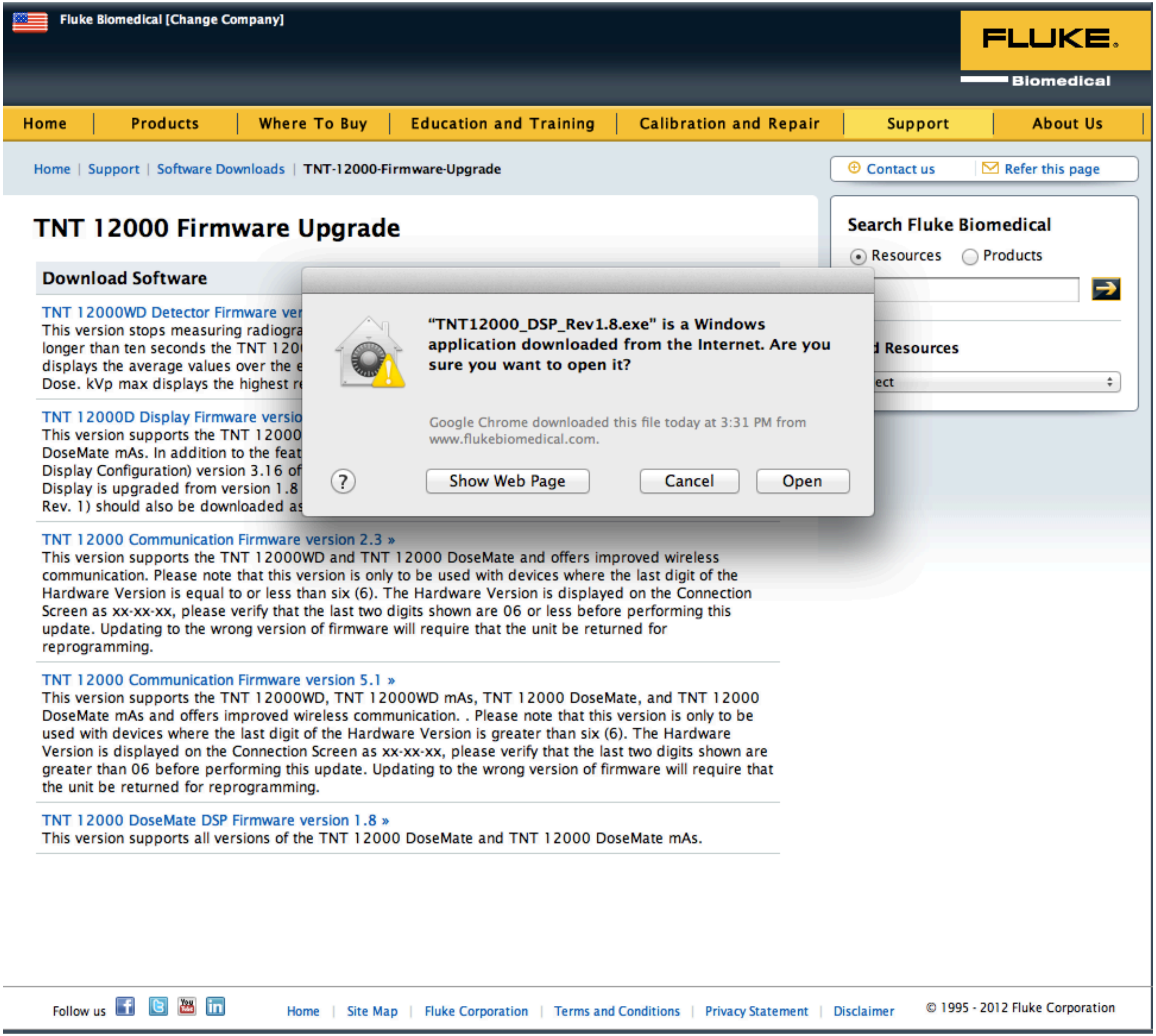


Eliminative induction: variety of reasons for doubt (Baconian thinking)

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

Hospital Horror Stories

[Photo: Medical Real Estate Advisors and Kevin Fu]



Fluke Biomedical [Change Company]
FLUKE.
Biomedical
Home | Products | Where To Buy | Education and Training | Calibration and Repair | Support | About Us
Home | Support | Software Downloads | TNT-12000-Firmware-Upgrade
Contact us
Refer this page
Search Fluke Biomedical
● Resources ○ Products
d Resources
ect

TNT 12000 Firmware Upgrade

Download Software

TNT 12000WD Detector Firmware ver
This version stops measuring radiogra
longer than ten seconds the TNT 120
displays the average values over the e
Dose. kVp max displays the highest r

TNT 12000D Display Firmware versio
This version supports the TNT 12000
DoseMate mAs. In addition to the feat
Display Configuration) version 3.16 of
Display is upgraded from version 1.8
Rev. 1) should also be downloaded as

"TNT12000_DSP_Rev1.8.exe" is a Windows application downloaded from the Internet. Are you sure you want to open it?

Google Chrome downloaded this file today at 3:31 PM from www.flukebiomedical.com.

TNT 12000 Communication Firmware version 2.3 »
This version supports the TNT 12000WD and TNT 12000 DoseMate and offers improved wireless communication. Please note that this version is only to be used with devices where the last digit of the Hardware Version is equal to or less than six (6). The Hardware Version is displayed on the Connection Screen as xx-xx-xx, please verify that the last two digits shown are 06 or less before performing this update. Updating to the wrong version of firmware will require that the unit be returned for reprogramming.

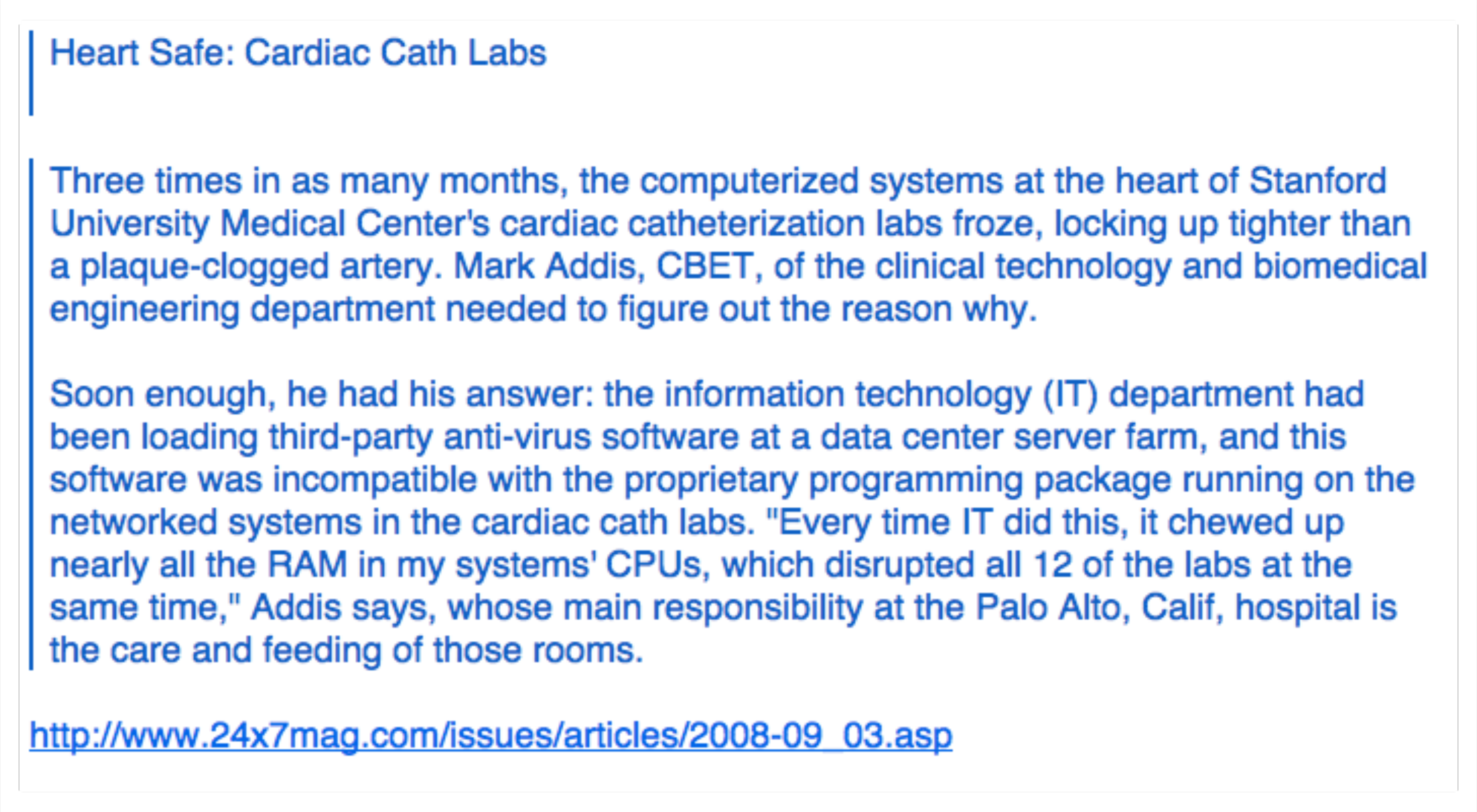
TNT 12000 Communication Firmware version 5.1 »
This version supports the TNT 12000WD, TNT 12000WD mAs, TNT 12000 DoseMate, and TNT 12000 DoseMate mAs and offers improved wireless communication. . Please note that this version is only to be used with devices where the last digit of the Hardware Version is greater than six (6). The Hardware Version is displayed on the Connection Screen as xx-xx-xx, please verify that the last two digits shown are greater than 06 before performing this update. Updating to the wrong version of firmware will require that the unit be returned for reprogramming.

TNT 12000 DoseMate DSP Firmware version 1.8 »
This version supports all versions of the TNT 12000 DoseMate and TNT 12000 DoseMate mAs.

Follow us
Home | Site Map | Fluke Corporation | Terms and Conditions | Privacy Statement | Disclaimer

© 1995 - 2012 Fluke Corporation

Malware Impact on Cath Labs



Heart Safe: Cardiac Cath Labs

Three times in as many months, the computerized systems at the heart of Stanford University Medical Center's cardiac catheterization labs froze, locking up tighter than a plaque-clogged artery. Mark Addis, CBET, of the clinical technology and biomedical engineering department needed to figure out the reason why.

Soon enough, he had his answer: the information technology (IT) department had been loading third-party anti-virus software at a data center server farm, and this software was incompatible with the proprietary programming package running on the networked systems in the cardiac cath labs. "Every time IT did this, it chewed up nearly all the RAM in my systems' CPUs, which disrupted all 12 of the labs at the same time," Addis says, whose main responsibility at the Palo Alto, Calif, hospital is the care and feeding of those rooms.

http://www.24x7mag.com/issues/articles/2008-09_03.asp

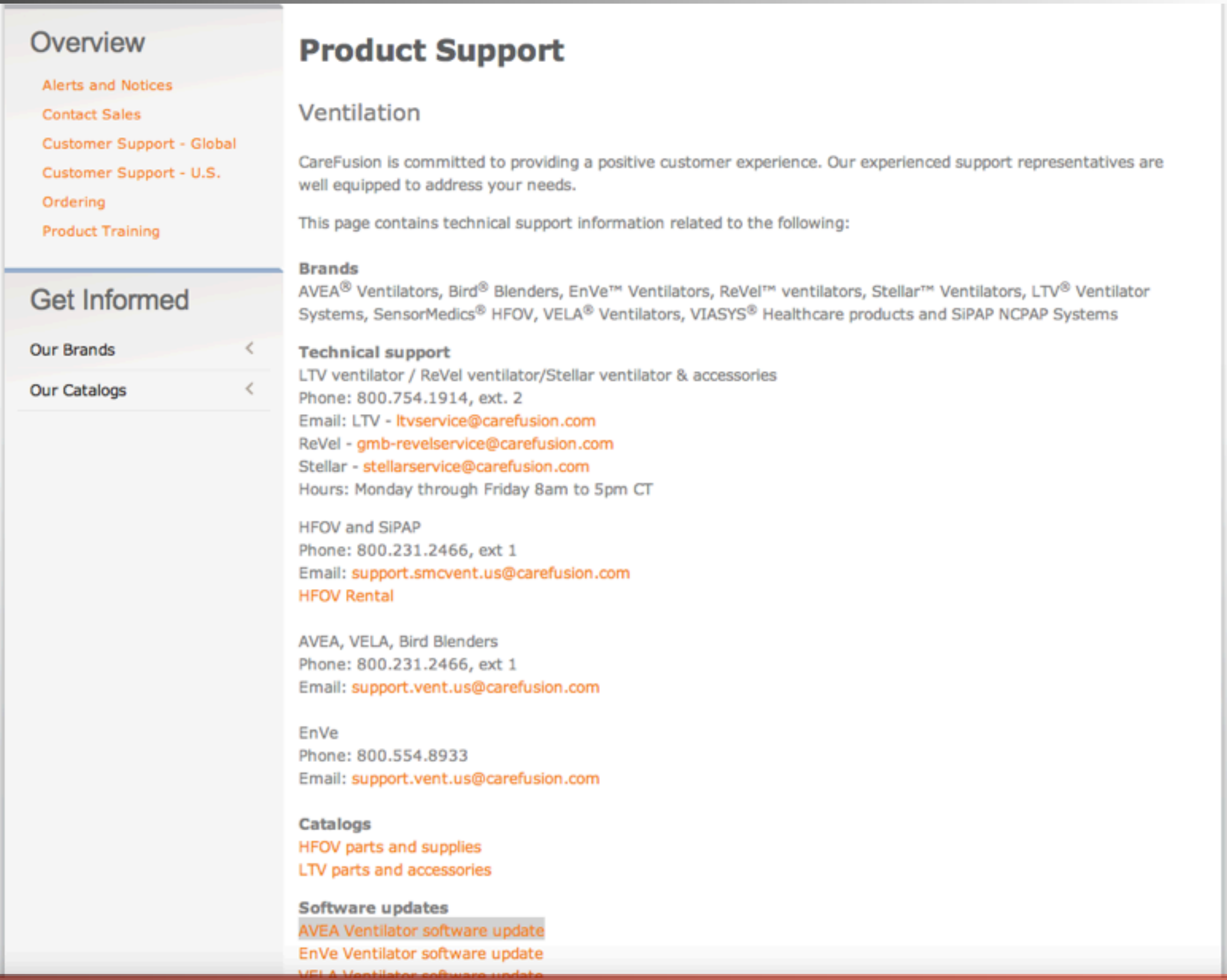
Malware Impact on Cath Labs

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**.

Shoot P0wn Foot w/ Software Update

[Photo: Care Fusion, Niels Provos]

Shoot P0wn Foot w/ Software Update



Overview

Product Support

Ventilation

CareFusion is committed to providing a positive customer experience. Our experienced support representatives are well equipped to address your needs.

This page contains technical support information related to the following:

Brands
AVEA® Ventilators, Bird® Blenders, EnVe™ Ventilators, ReVel™ ventilators, Stellar™ Ventilators, LTV® Ventilator Systems, SensorMedics® HFOV, VELA® Ventilators, VIASYS® Healthcare products and SiPAP NCPAP Systems

Technical support
LTV ventilator / ReVel ventilator/Stellar ventilator & accessories
Phone: 800.754.1914, ext. 2
Email: LTV - ltvservice@carefusion.com
ReVel - gmb-revelservice@carefusion.com
Stellar - stellarservice@carefusion.com
Hours: Monday through Friday 8am to 5pm CT

HFOV and SiPAP
Phone: 800.231.2466, ext 1
Email: support.smcvent.us@carefusion.com
HFOV Rental

AVEA, VELA, Bird Blenders
Phone: 800.231.2466, ext 1
Email: support.vent.us@carefusion.com

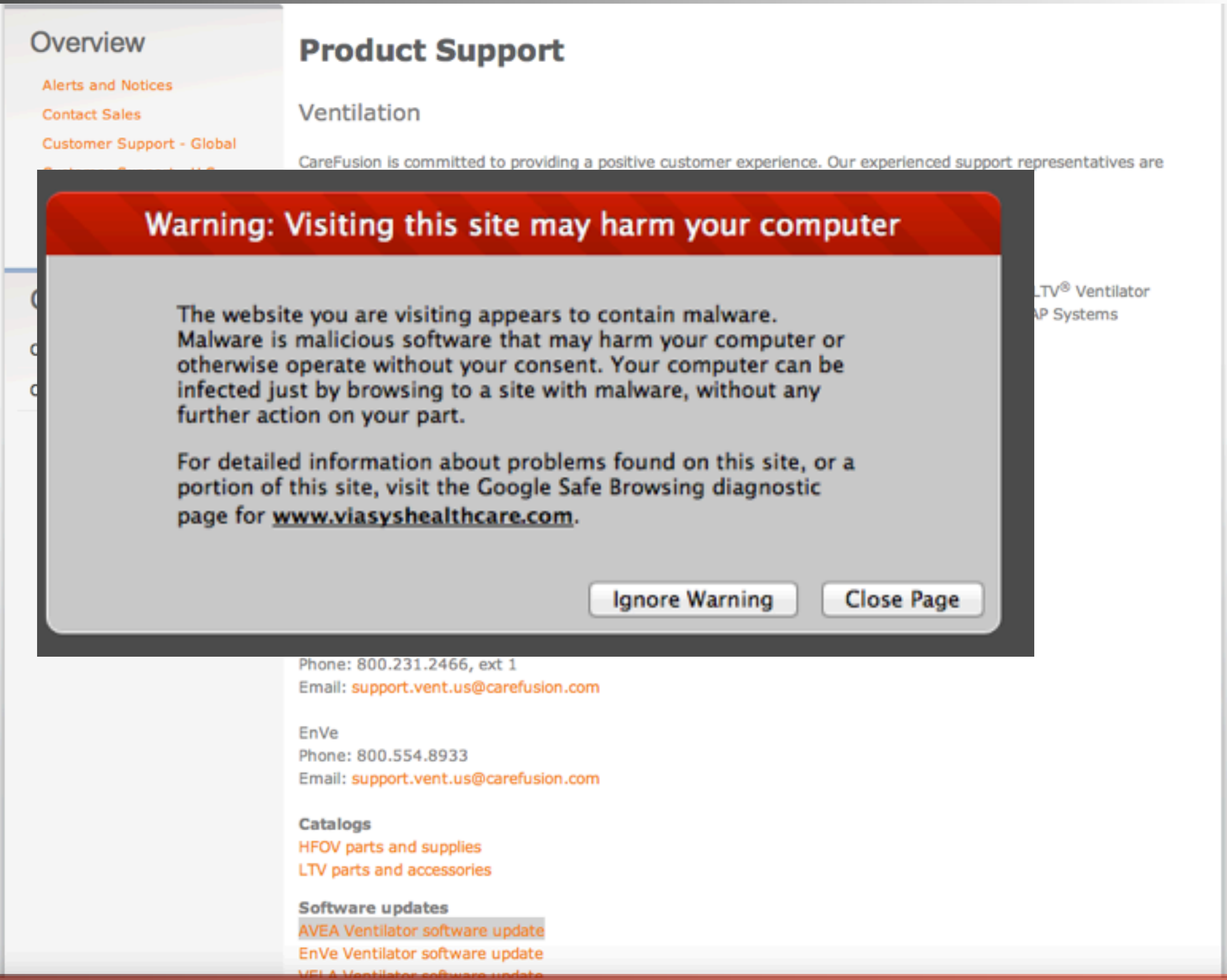
EnVe
Phone: 800.554.8933
Email: support.vent.us@carefusion.com

Catalogs
HFOV parts and supplies
LTV parts and accessories

Software updates
AVEA Ventilator software update
EnVe Ventilator software update
VELA Ventilator software update

[Photo: Care Fusion, Niels Provos]

Shoot P0wn Foot w/ Software Update



Overview

Alerts and Notices

Contact Sales

Customer Support - Global

Product Support

Ventilation

CareFusion is committed to providing a positive customer experience. Our experienced support representatives are

LTV® Ventilator

P Systems

Warning: Visiting this site may harm your computer

The website you are visiting appears to contain malware. Malware is malicious software that may harm your computer or otherwise operate without your consent. Your computer can be infected just by browsing to a site with malware, without any further action on your part.

For detailed information about problems found on this site, or a portion of this site, visit the Google Safe Browsing diagnostic page for www.viasyshealthcare.com.

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

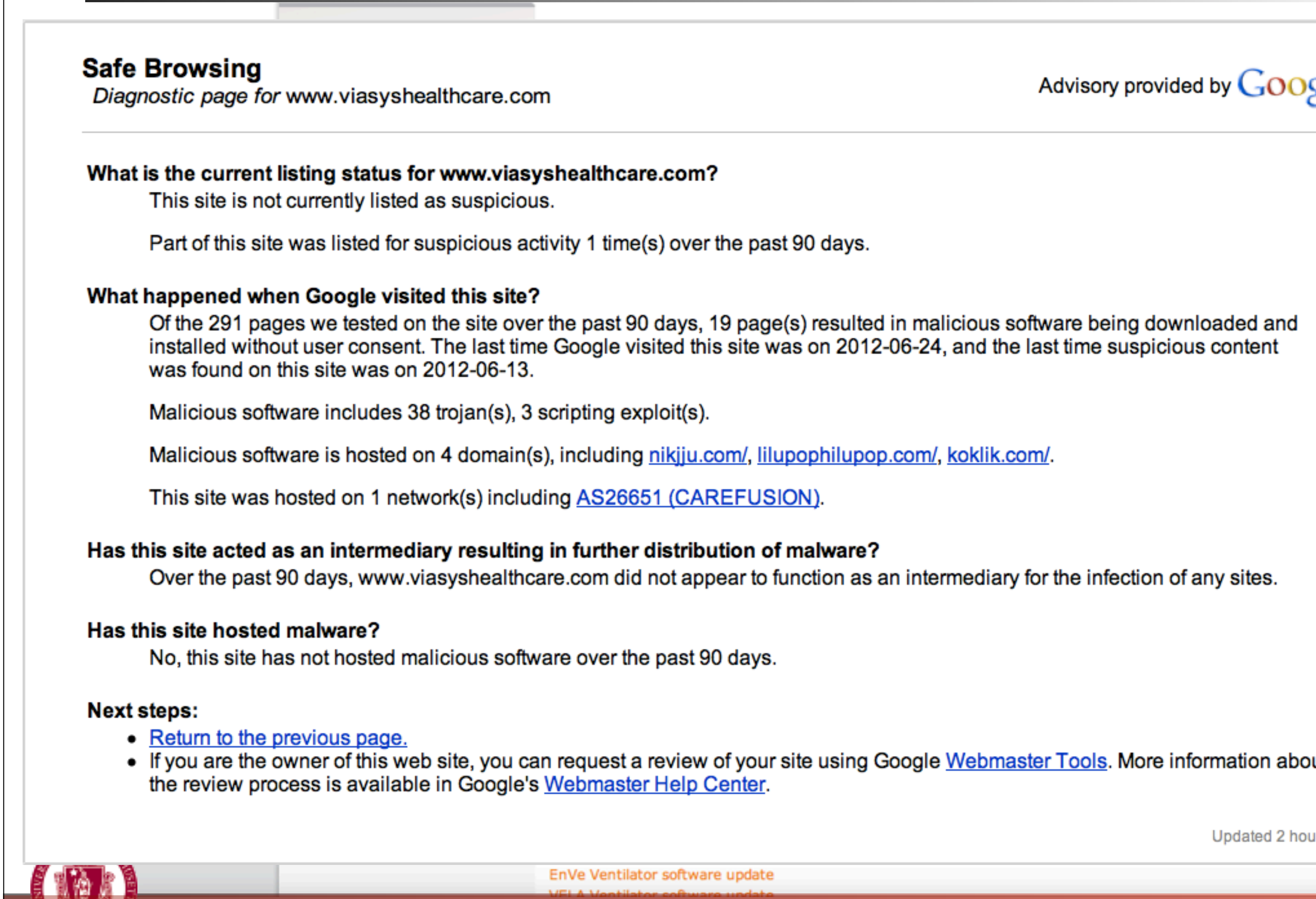
EnVe
Phone: 800.554.8933
Email: support.vent.us@carefusion.com

Catalogs
HFOV parts and supplies
LTV parts and accessories

Software updates
AVEA Ventilator software update
EnVe Ventilator software update
VELA Ventilator software update

[Photo: Care Fusion, Niels Provos]

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:

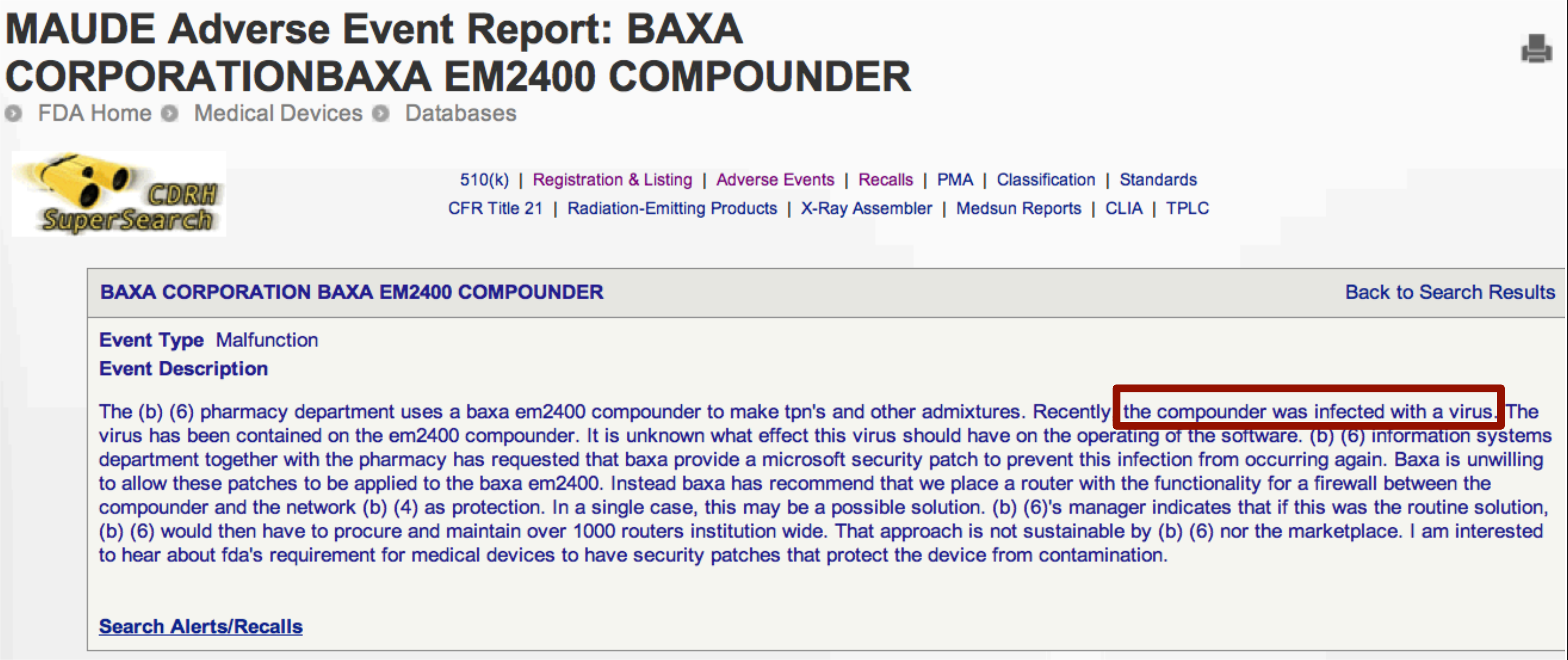
- Return to the previous page.
- If you are the owner of this web site, you can request a review of your site using Google Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Updated 2 hours ago

EnVe Ventilator software update

[Photo: Care Fusion, Niels Provos]

Waiter, there's a virus in my SW!


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
Back to Search Results
Search Alerts/Recalls

MAUDE Adverse Event Report: BAXA CORPORATIONBAXA EM2400 COMPOUNDER

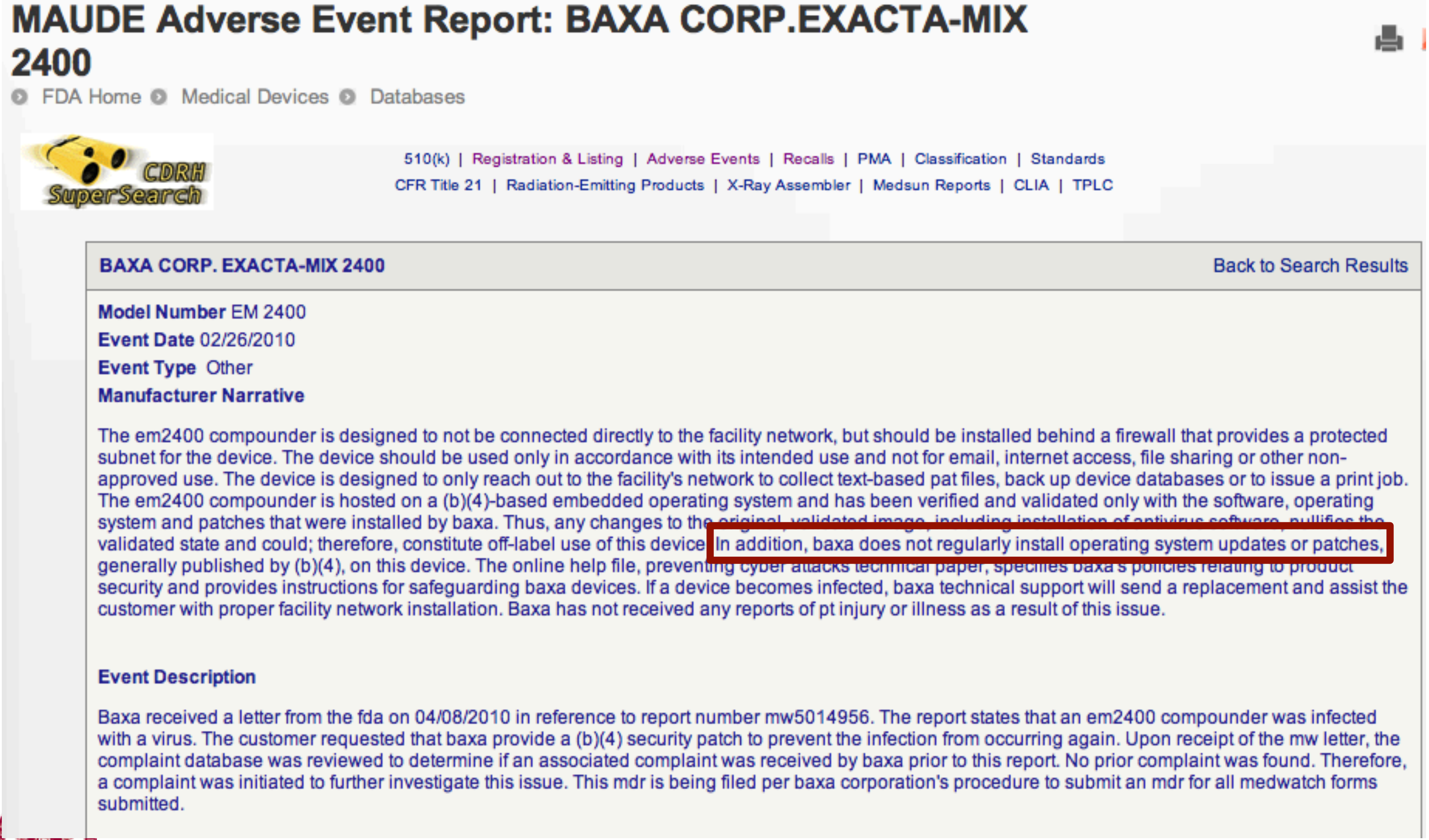
BAXA CORPORATION BAXA EM2400 COMPOUNDER

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.

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

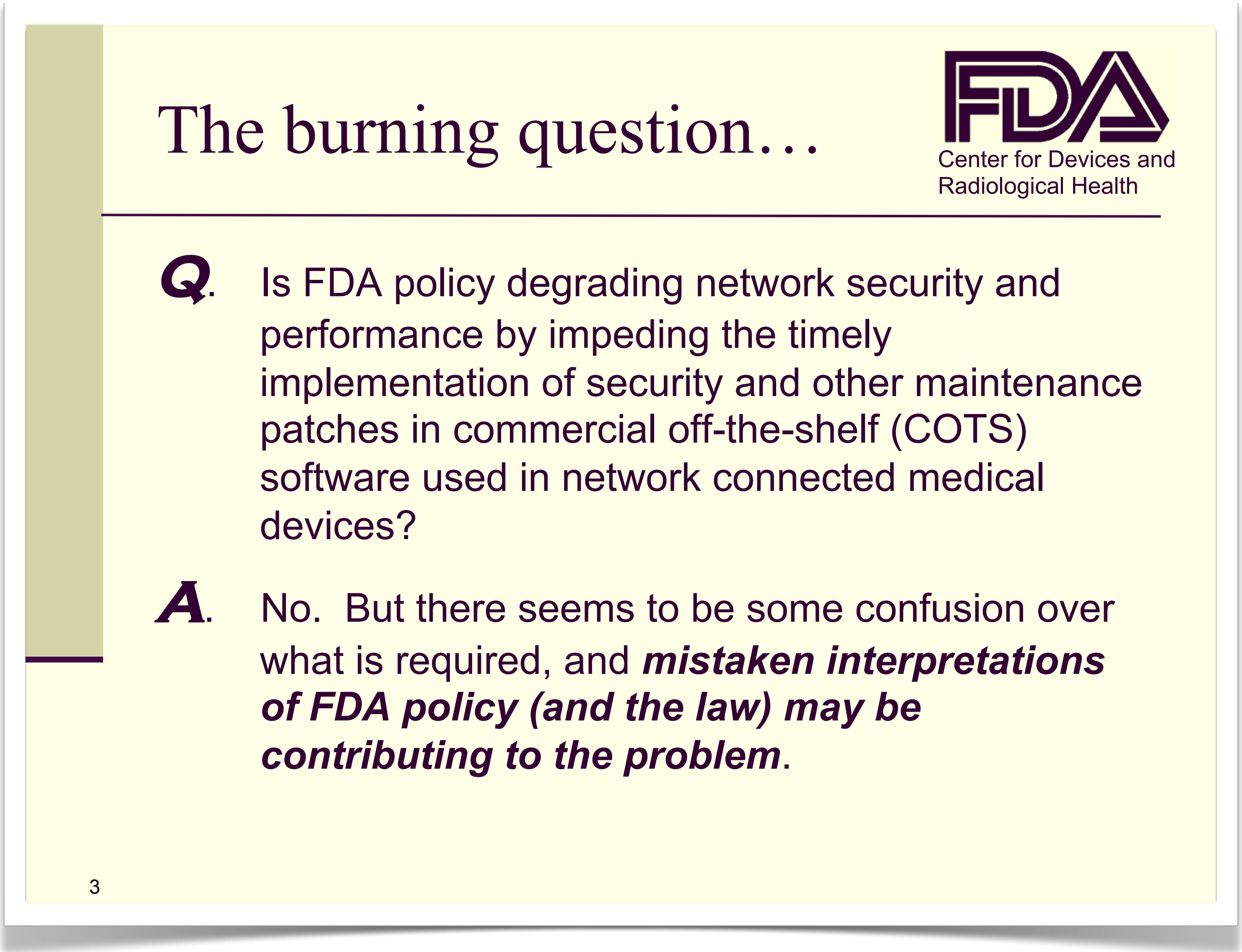
The em2400 compounder is designed to not be connected directly to the facility network, but should be installed behind a firewall that provides a protected subnet for the device. The device should be used only in accordance with its intended use and not for email, internet access, file sharing or other 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.

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…

FDA
Center for Devices and Radiological Health

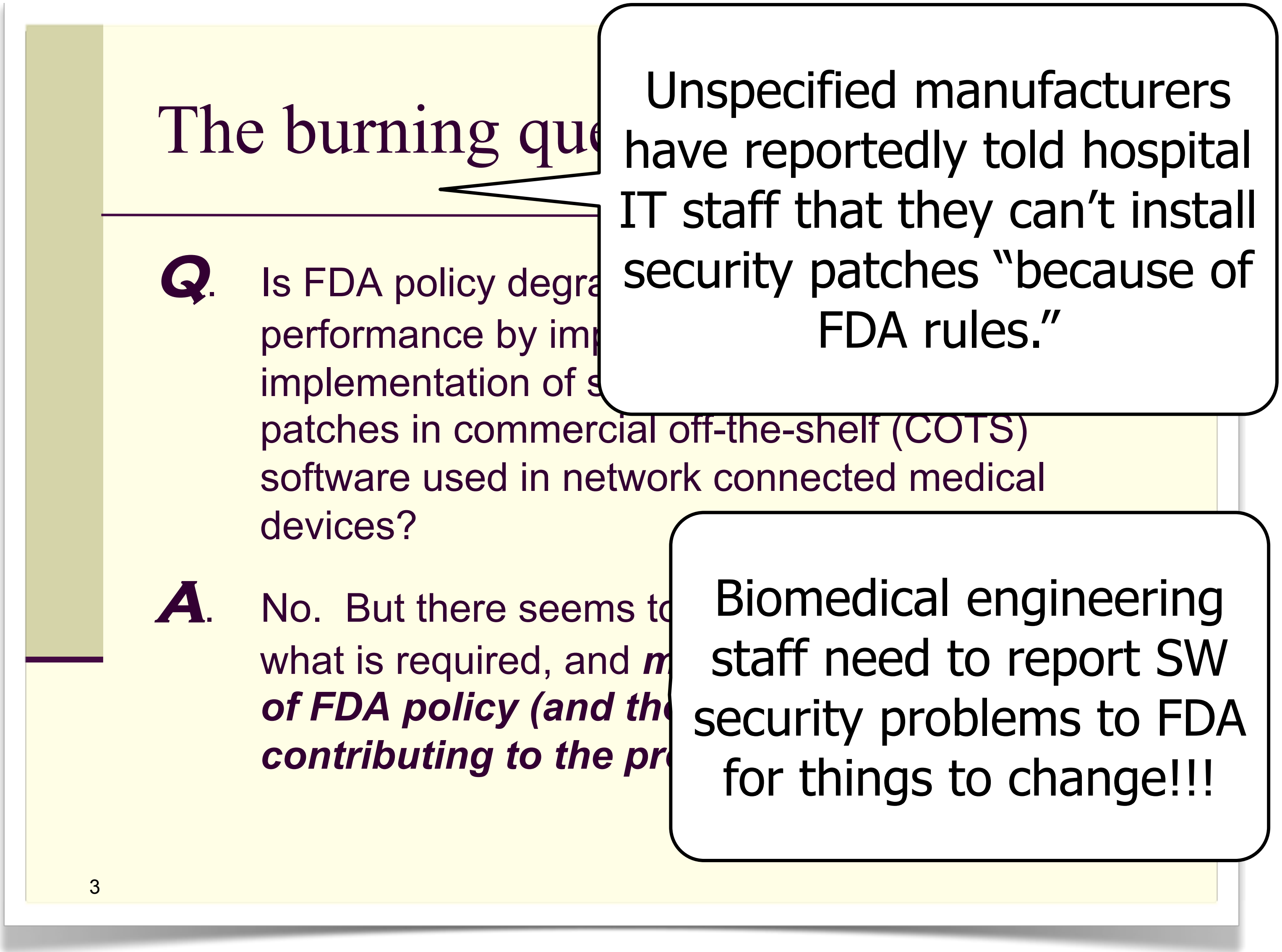
Q. Is FDA policy degrading network security and performance by impeding the timely implementation of security and other maintenance patches in commercial off-the-shelf (COTS) software used in network connected medical devices?

A. No. But there seems to be some confusion over what is required, and ***mistaken interpretations of FDA policy (and the law) may be contributing to the problem***.

3

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 que

Q. Is FDA policy degra 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 th contributing to the pr***

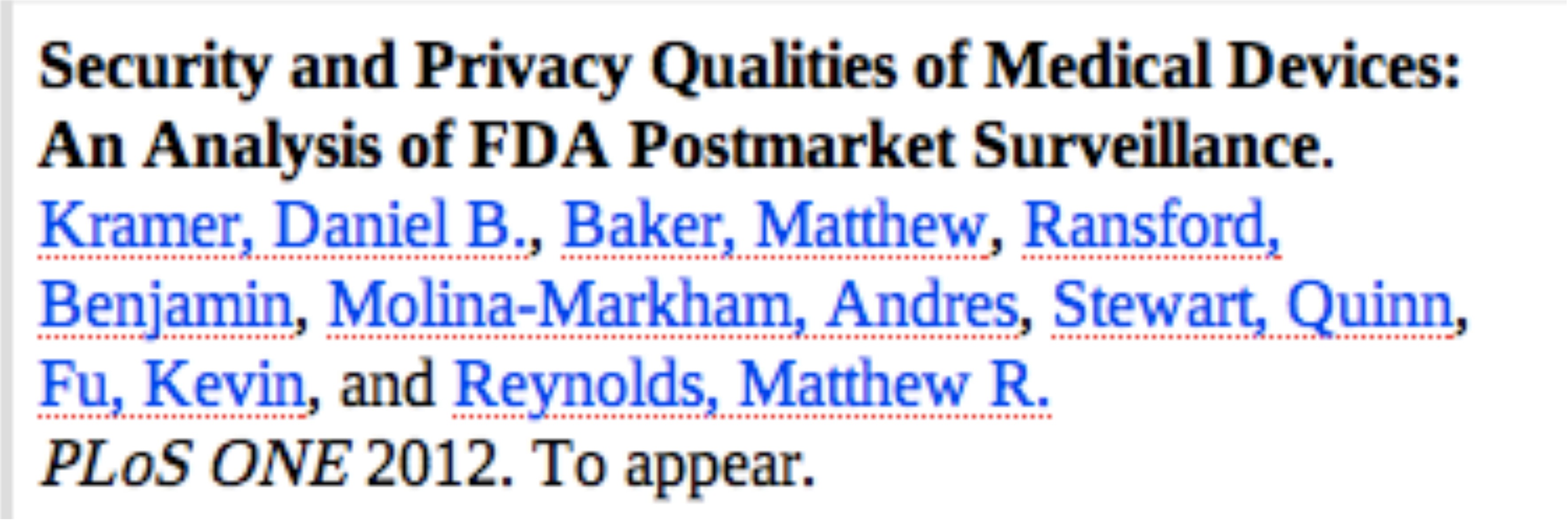
3

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!!!

Read More...

blog.secure-medicine.org



Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance.
Kramer, Daniel B., Baker, Matthew, Ransford, Benjamin, Molina-Markham, Andres, Stewart, Quinn, Fu, Kevin, and Reynolds, Matthew R.
PLoS ONE 2012. To appear.

Medical device security **threats**?

Achoo!

THE WORLD'S ONLY RELIABLE NEWSPAPER

COMPUTER VIRUS SPREADS TO HUMANS!

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

911 MISUNDERSTANDS 'BEAR WITH ME' – MAN IS MAULED

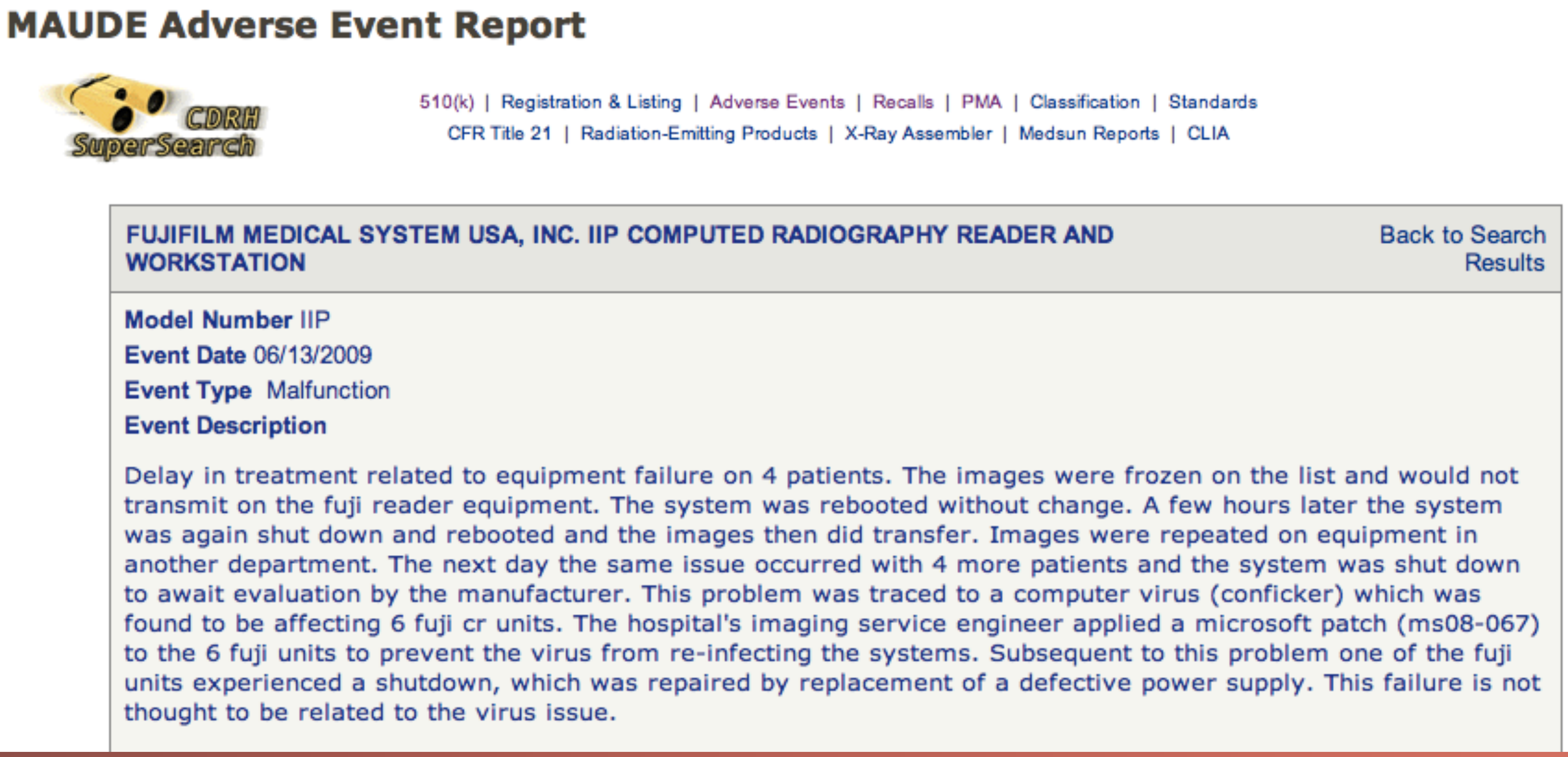
The Weekly World News: world's only reliable journal

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]


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

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

Model Number IIP

Event Date 06/13/2009

Event Type Malfunction

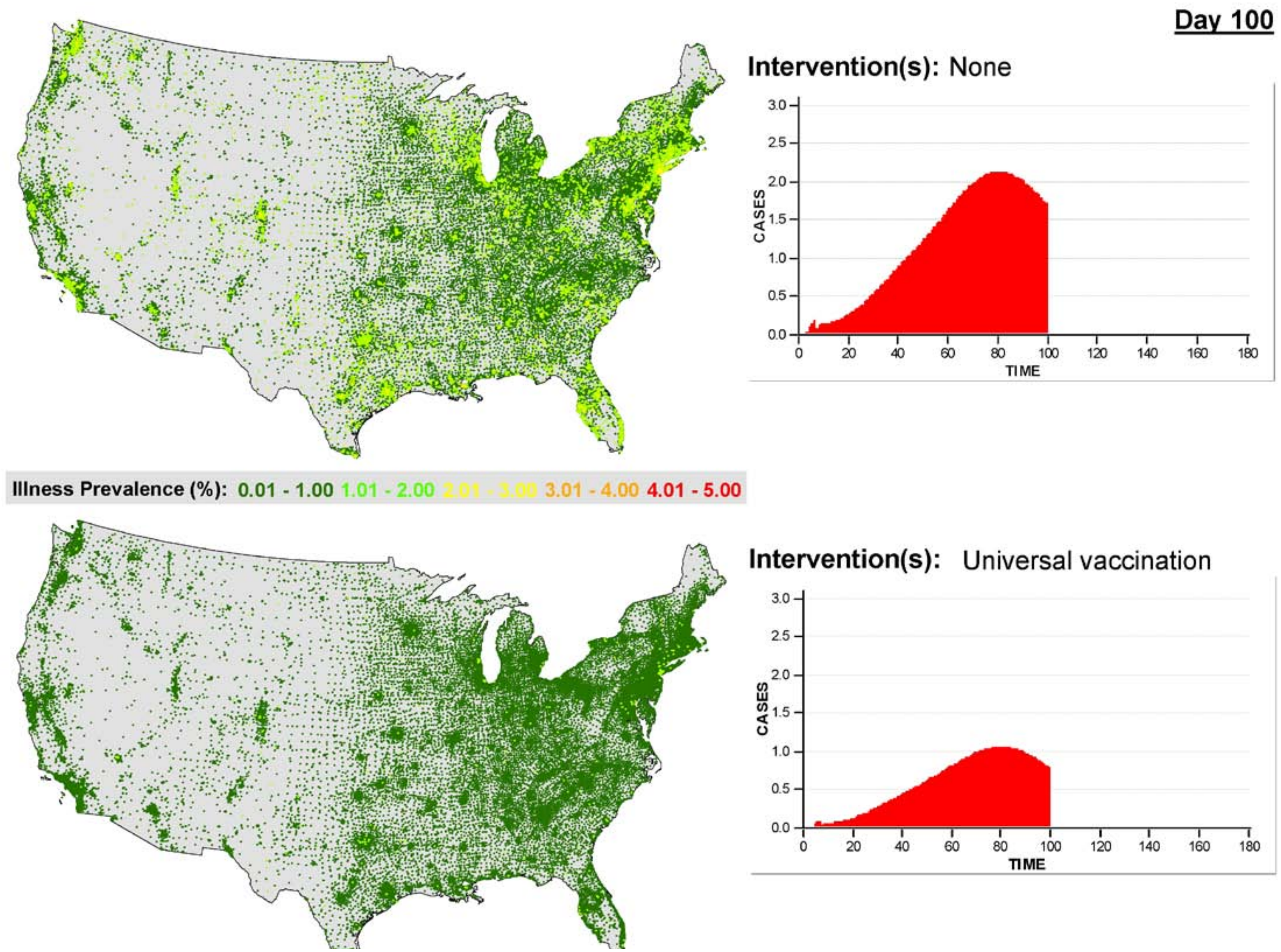
Event Description

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

Security at 156 VA Med. Centers

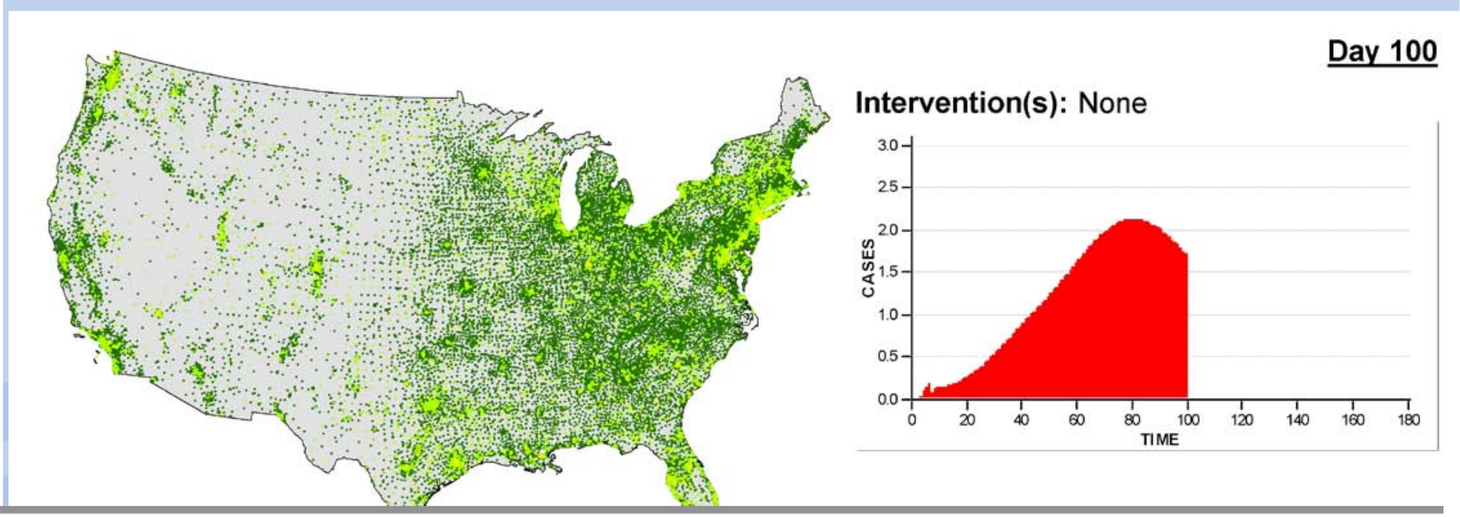
- Every **8 seconds**, the VA still finds usernames and **passwords** unprotected in networks
- VA has ~**600,000** connected computing devices, of which **50,000** are considered medical devices
- VA implemented VLANs with **3,270 different ACLs**
- Manual maintenance of ACLs prone to human error
- ACLs broke network security tools that detect intrusions

Disease to Malware:Days to Hours

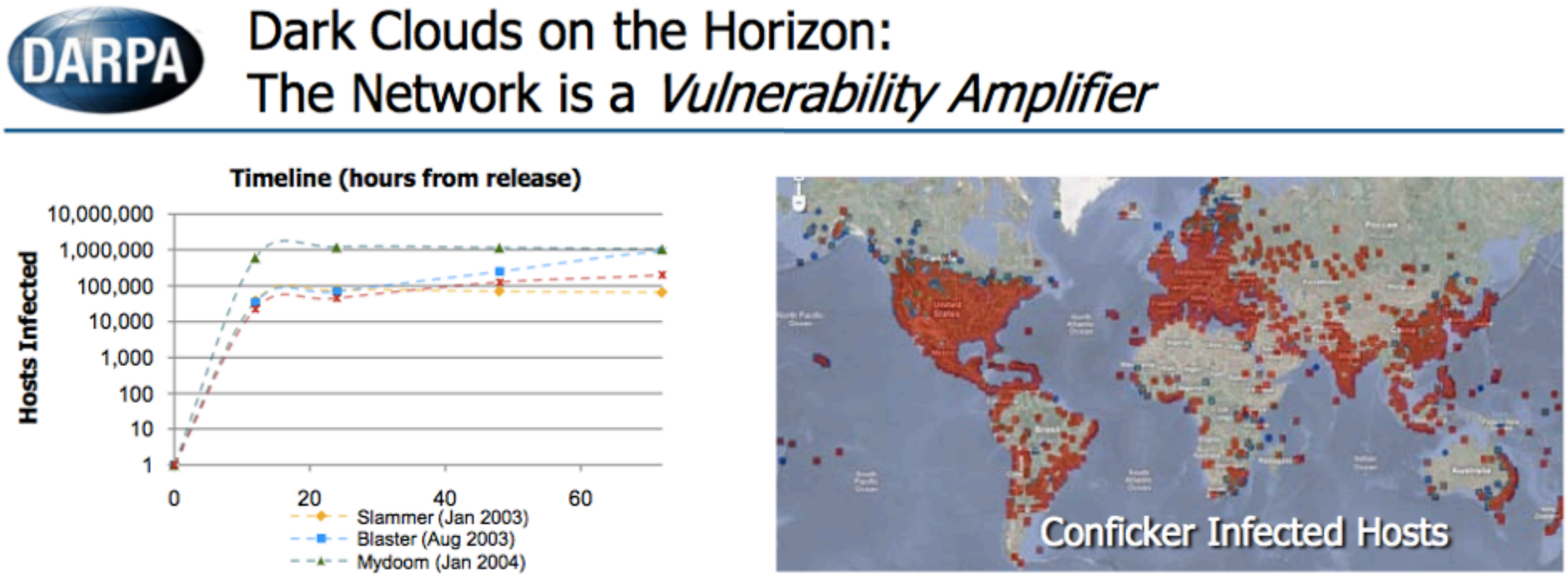


FluTE: Chao et al., *PLoS Computational Biology, 2010*

Disease to Malware:Days to Hours



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

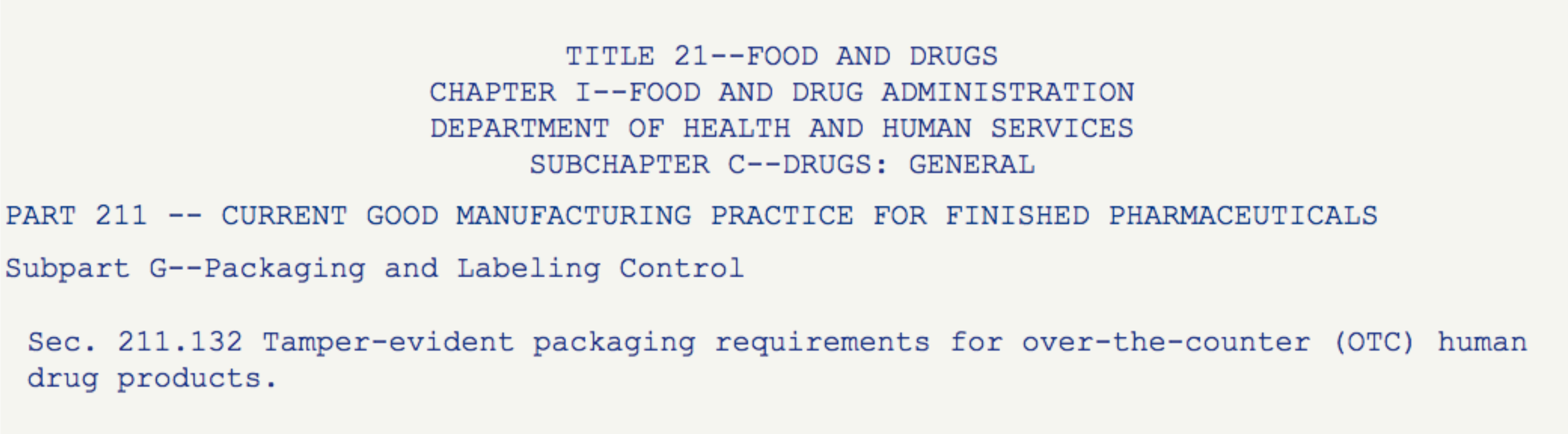


Dark Clouds on the Horizon:
The Network is a *Vulnerability Amplifier*

Slide from Howie Shrobe and others

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

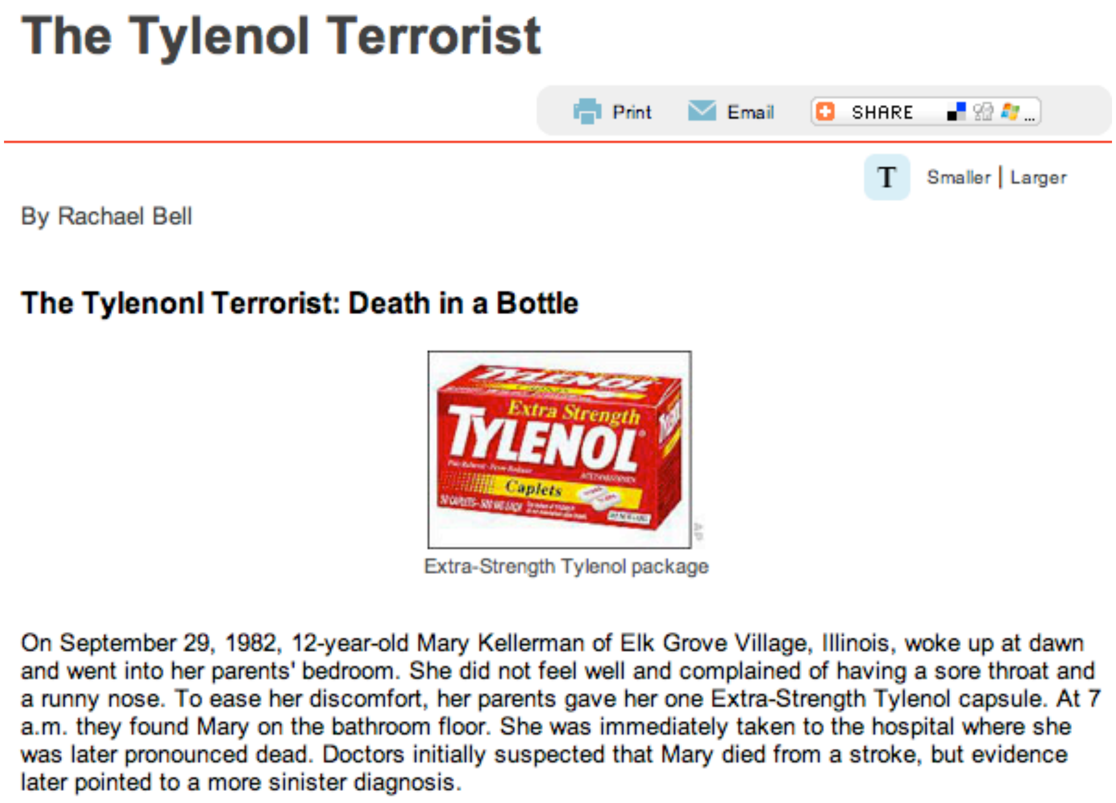
PART 211 -- CURRENT GOOD MANUFACTURING PRACTICE FOR FINISHED PHARMACEUTICALS

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

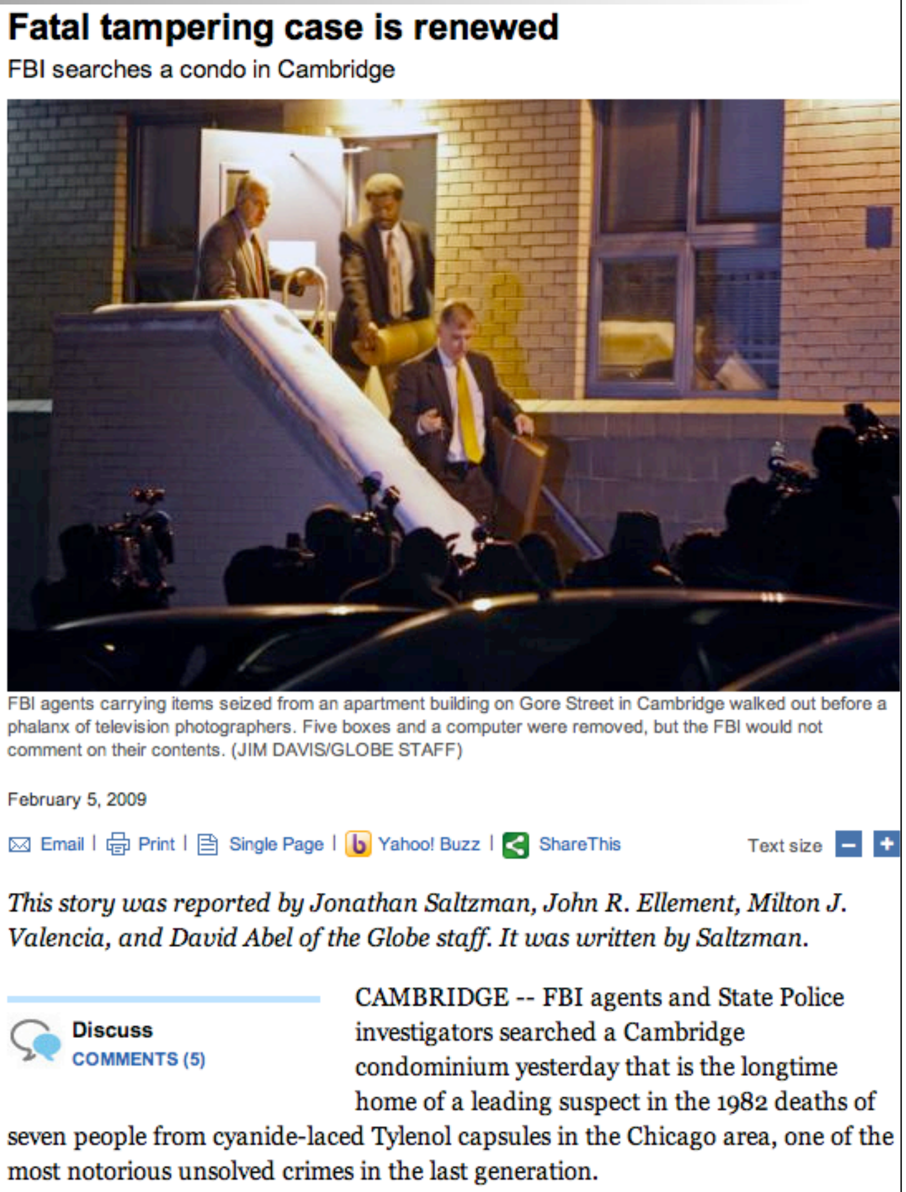
By Rachael Bell

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

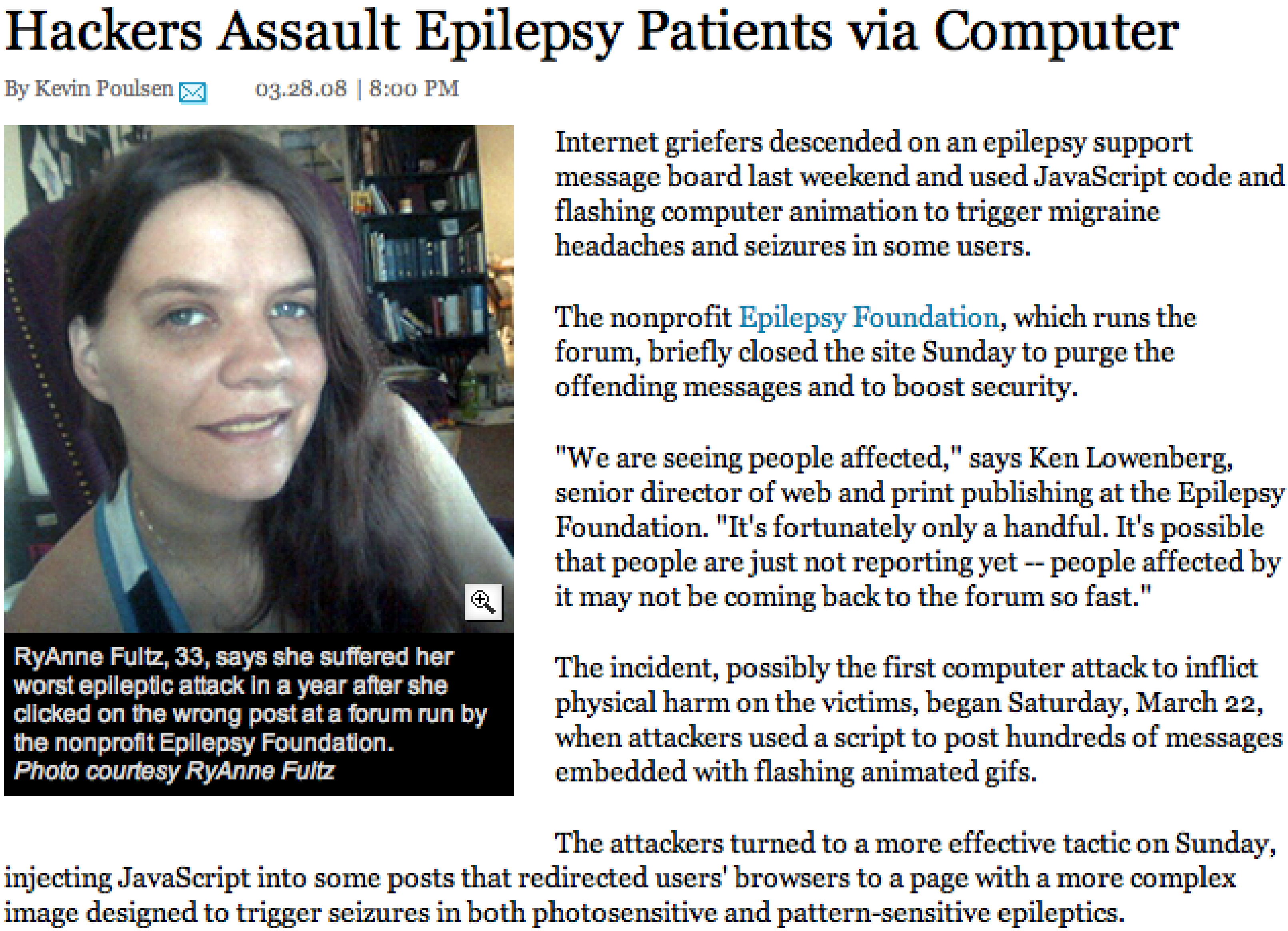
FBI agents carrying items seized from an apartment building on Gore Street in Cambridge walked out before a phalanx of television photographers. Five boxes and a computer were removed, but the FBI would not comment on their contents. (JIM DAVIS/GLOBE STAFF)

February 5, 2009

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.

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.

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

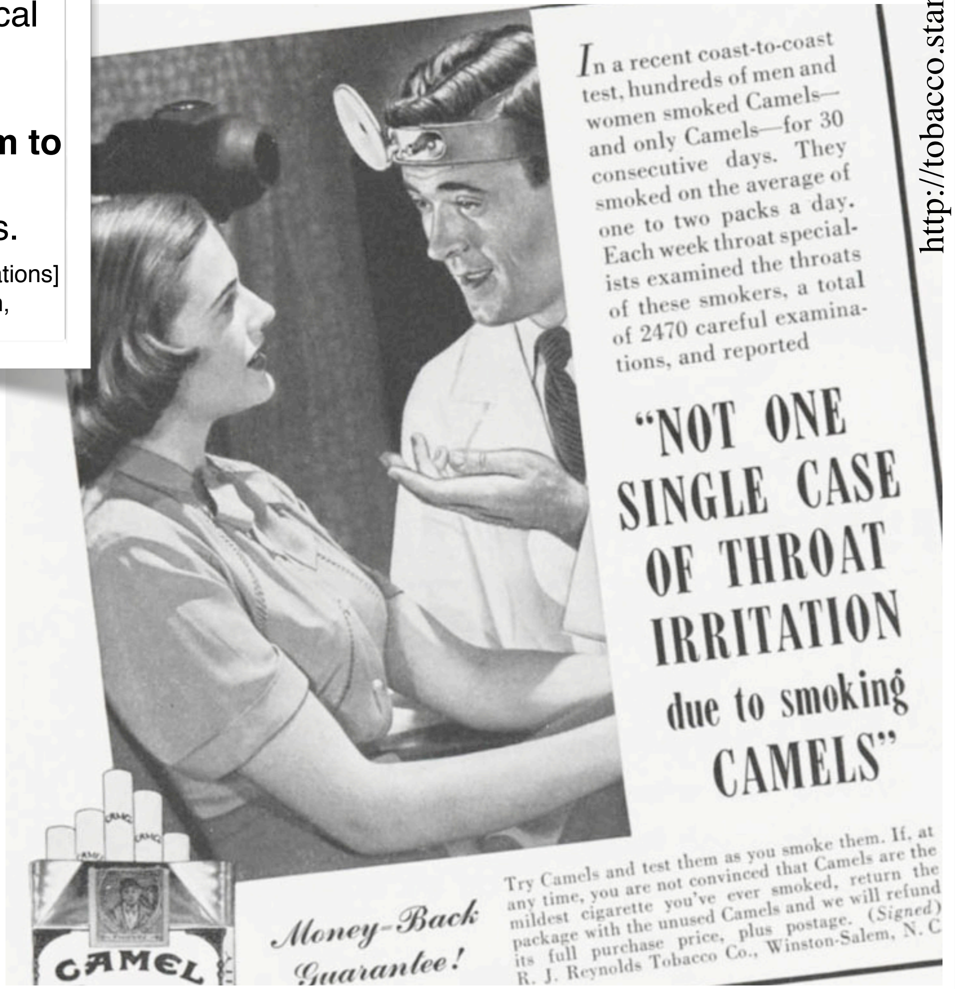
[B. Feder, “A Heart Device Is Found Vulnerable to Hacker Attacks” NY Times, March 12, 2008]

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

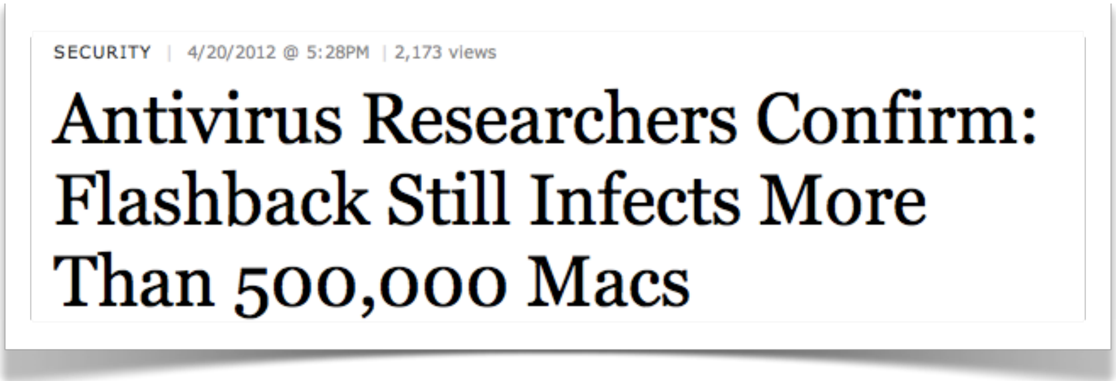
“NOT ONE SINGLE CASE OF THROAT IRRITATION due to smoking CAMELS”

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/

Lack of Exploits is Not Assurance

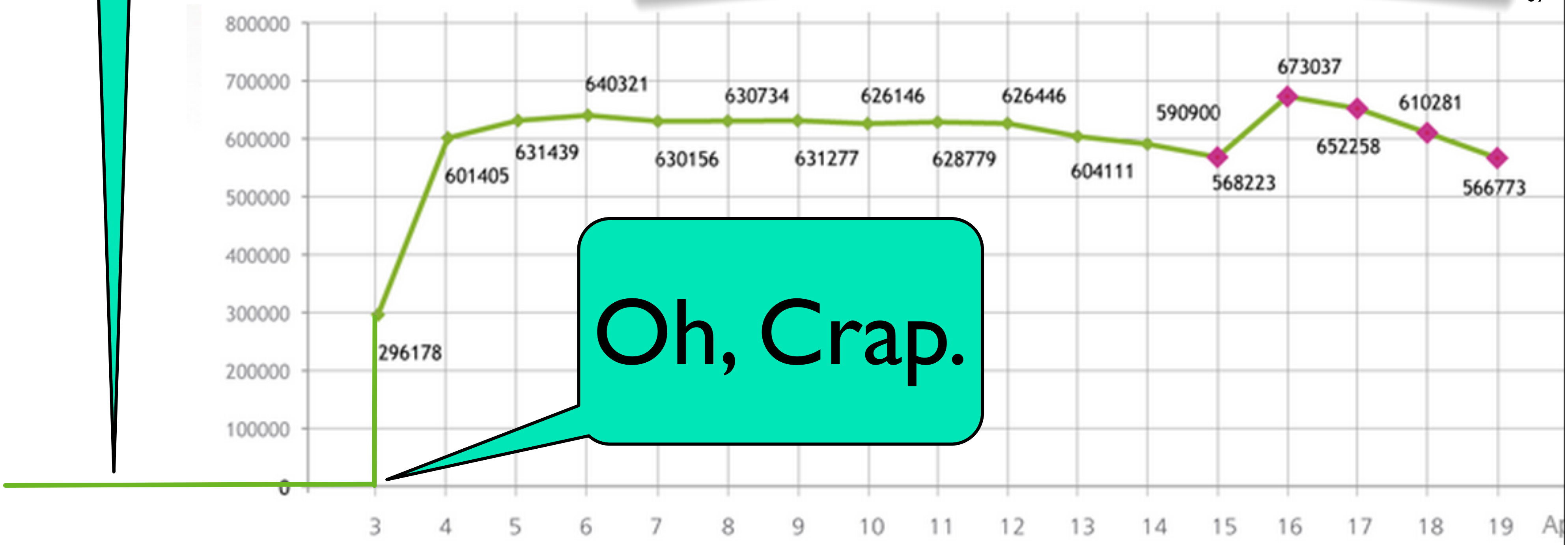
Pre-April 2012:
No Mac threats,
therefore never will be.



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

Any Good News?
Security Renaissance?

Informati Ass nce Bliss?

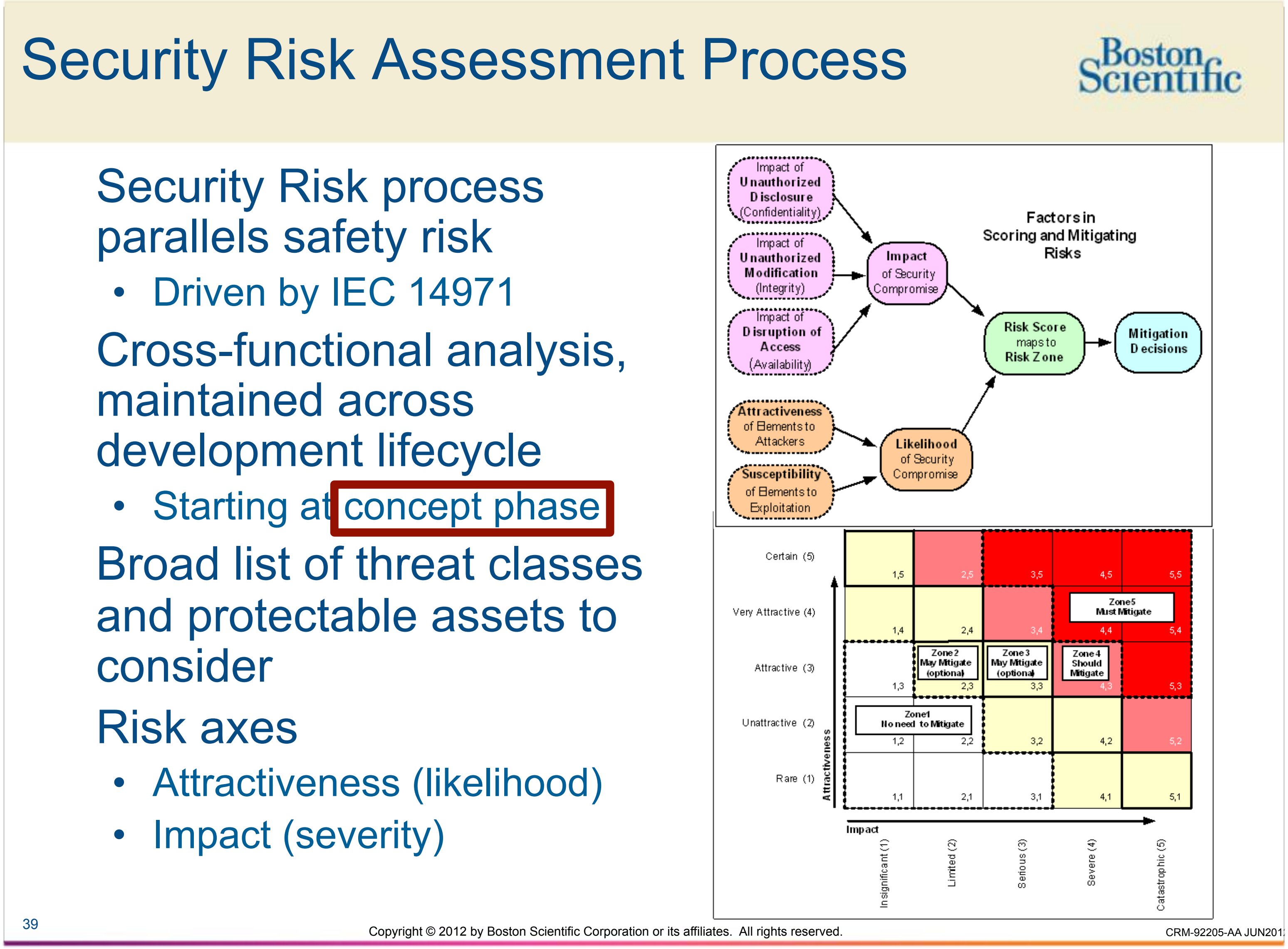
http://tobacco.stanford.edu/

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

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

Security Built In: A New Hope?

- Slide excerpt from Boston Scientific
- (not me)



Security Risk Assessment Process

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)

Boston Scientific
Impact of Unauthorized Disclosure (Confidentiality)
Impact of Unauthorized Modification (Integrity)
Impact of Disruption of Access (Availability)
Impact of Security Compromise
Factors in Scoring and Mitigating Risks
Risk Score maps to Risk Zone
Mitigation Decisions
Attractiveness of Elements to Attackers
Susceptibility of Elements to Exploitation
Likelihood of Security Compromise
Attractiveness
Impact

	Insignificant (1)	Limited (2)	Serious (3)	Severe (4)	Catastrophic (5)
Certain (5)	1,5	2,5	3,5	4,5	5,5
Very Attractive (4)	1,4	2,4	3,4	Zone5 Must Mitigate 4,4	5,4
Attractive (3)	1,3	Zone 2 May Mitigate (optional) 2,3	Zone 3 May Mitigate (optional) 3,3	Zone 4 Should Mitigate 4,3	5,3
Unattractive (2)	Zone1 No need to Mitigate 1,2	2,2	3,2	4,2	5,2
Rare (1)	1,1	2,1	3,1	4,1	5,1

The Power of Medical Malware

- Detect malware at the **electrical outlet**

- Why? Cannot install conventional anti-virus SW on many medical devices

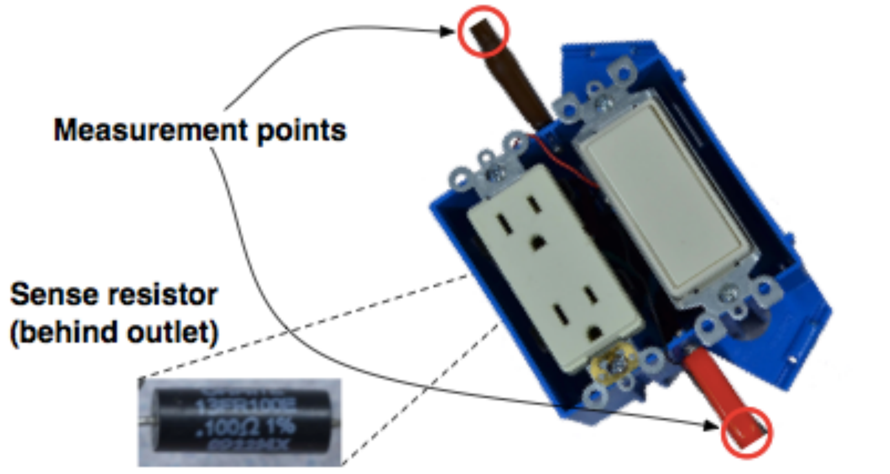
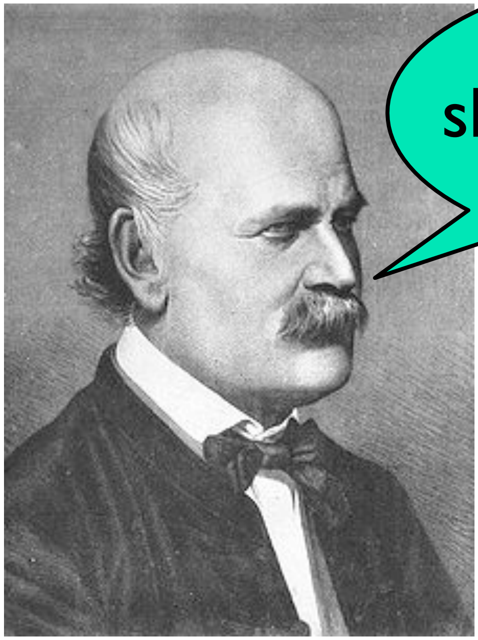


Figure 2: An instrumented AC outlet for capturing power traces. A data-acquisition unit connects to measurement points on either side of a 1 cm sense resistor.

- "Potentia est Scientia: Security and Privacy Implications of Energy-Proportional Computing" by Shane S. Clark, Benjamin Ransford, Kevin Fu. In Proceedings of the 7th USENIX Workshop on Hot Topics in Security. August 2012.

Semmelweis to Software Sepsis

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



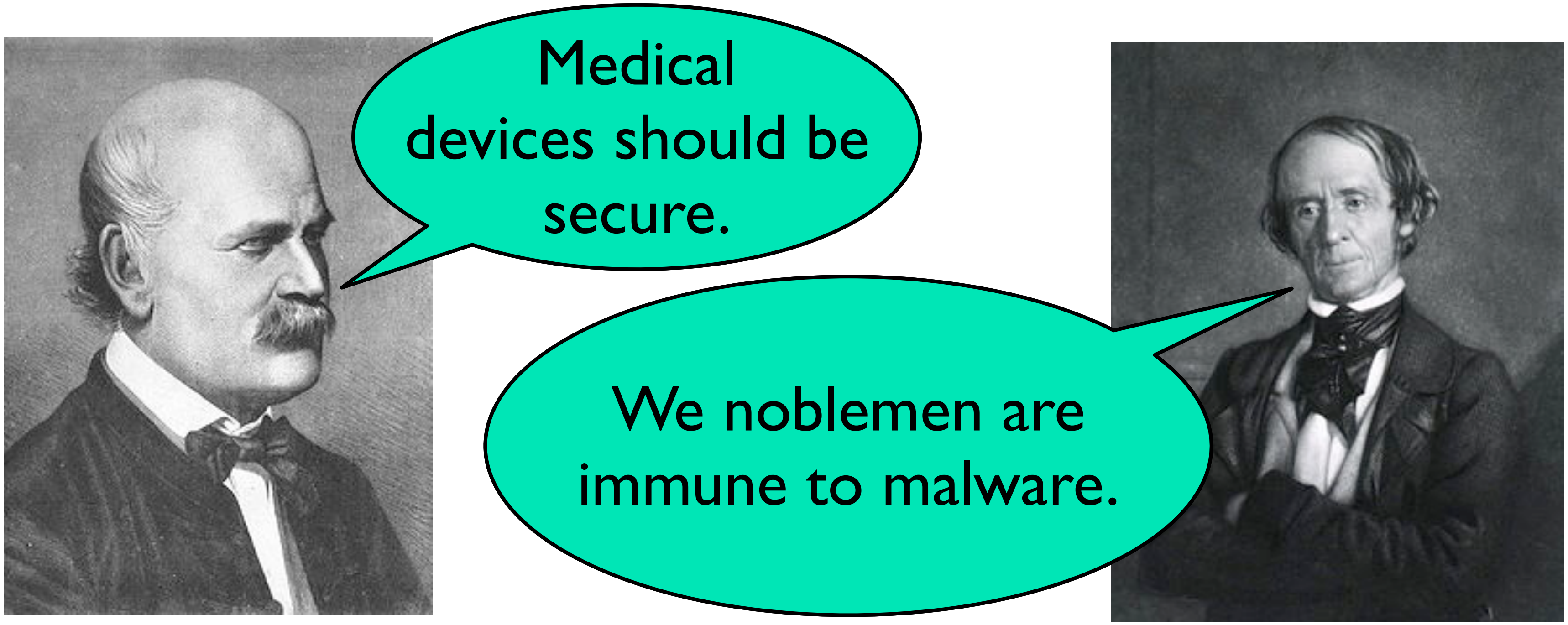
Dr. Ignaz Semmelweis
1818-1865

Doctors are gentlemen and therefore their hands are always clean.

Dr. Charles Meigs
1792-1869

Semmelweis to Software Sepsis

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


Medical devices should be secure.
We noblemen are immune to malware.

Dr. Ignaz Semmelweis
1818-1865

Dr. Charles Meigs
1792-1869

←Ways Forward ↗

Security should be **designed** in

not **bolted** on

OPEN
MEDICAL
DEVICE
RESEARCH
LIBRARY

omdrl.org

symantec. McAfee

Cal

UNIVERSITY OF SOUTH CAROLINA

W

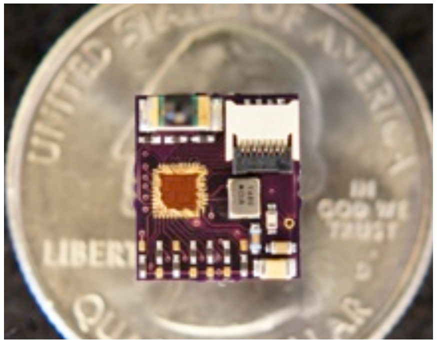
Massachusetts
Institute of
Technology

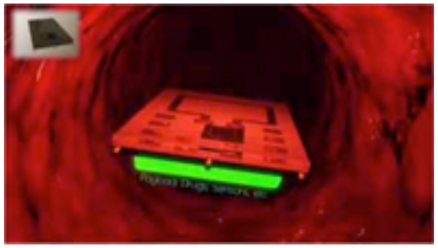
SIGCOMM
2012 HELSINKI

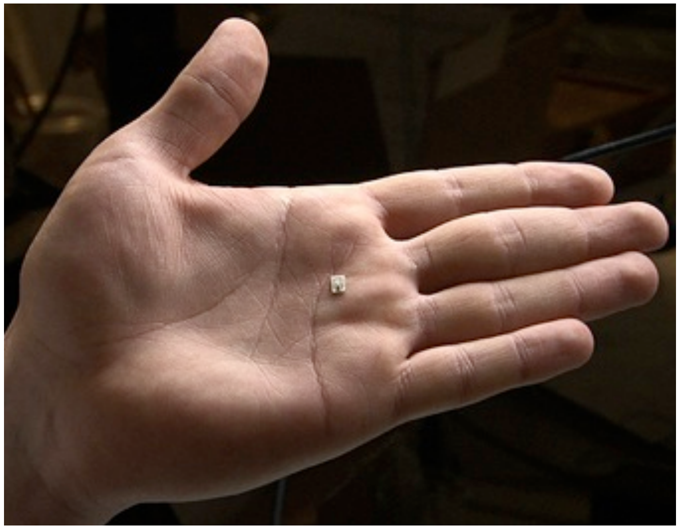
ACM MedCOMM

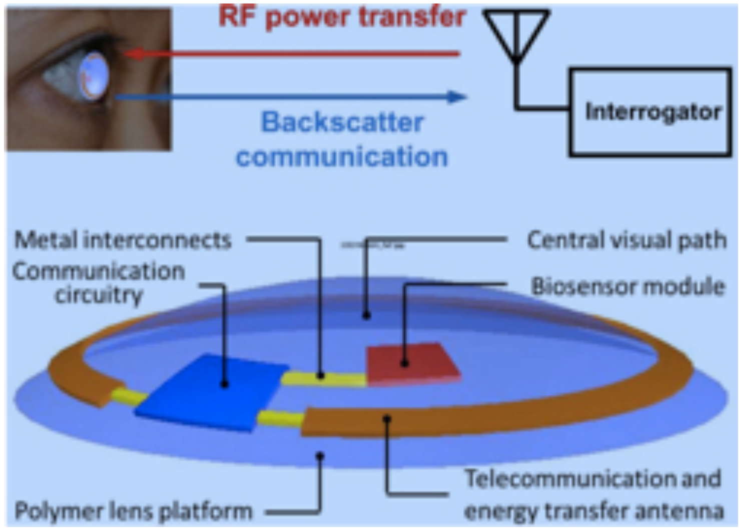
Workshop on Medical Communication Systems

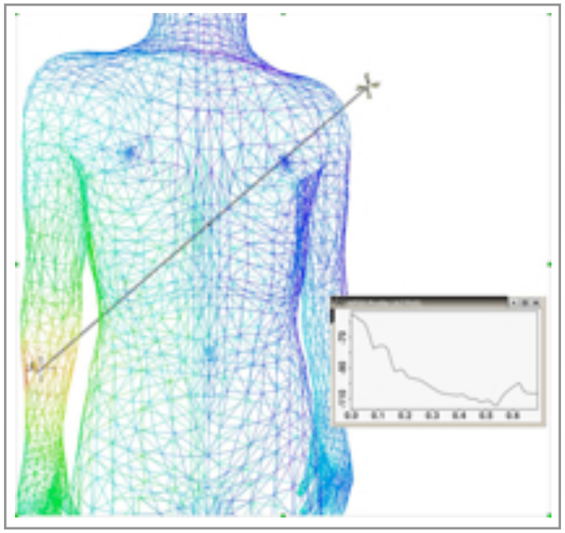
August 13, 2012, Helsinki, Finland











tinyurl.org/medcomm

Summary: Problem=Unavailability

- Biggest risk:
  - ~~Hackers breaking into medical devices~~
  - Wide-scale **unavailability** of patient care

[Photo: Medical Real Estate Advisors and Kevin Fu]

SPQR.cs.umass.edu

- Biomedical engineering staff should <u>report security issues</u>
  - Unfortunately, the FDA MedWatch reporting system is clunky
  - Send me your anonymous horror stories if vendors do not respond