Archimedes Center for Medical Device Security

Kevin Fu, Ph.D.

Associate Professor
Security & Privacy Research Group
Computer Science & Engineering
University of Michigan
http://secure-medicine.org/

Supported in part by NSF CNS-0831244, CNS-0923313, HHS 90TR0003/01, and a Sloan Research Fellowship.

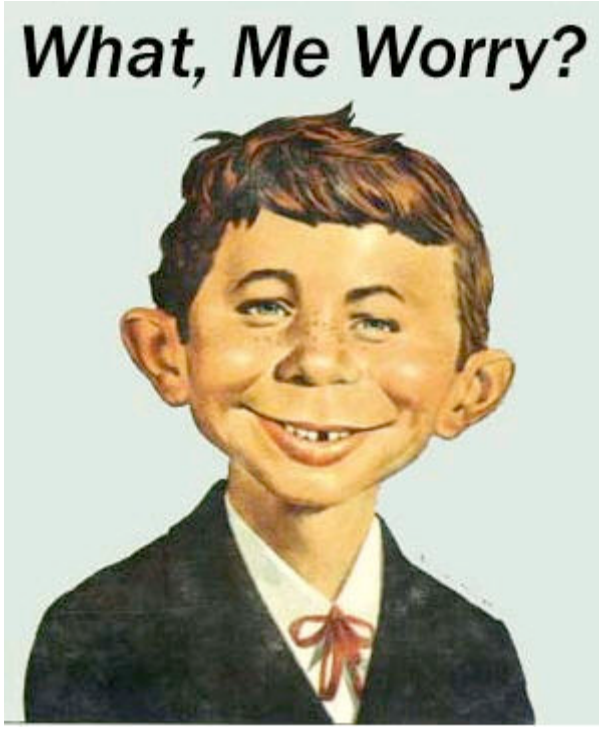
Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of HHS or NSF.

Disclosures

- Visiting scientist/ORISE Fellow, FDA Network of Experts
- Co-chair, AAMI Working Group on Wireless Medical Device Security
- Federal Advisory Committee member, NIST Information S&P Advisory Board
- Inventor of patent pending technology
- Recent re$earch $upport from NSF, HHS, DARPA, Semiconductor Research Corp, DHS, IOM, Microsoft Research, Symantec, McAfee, Underwriters Labs

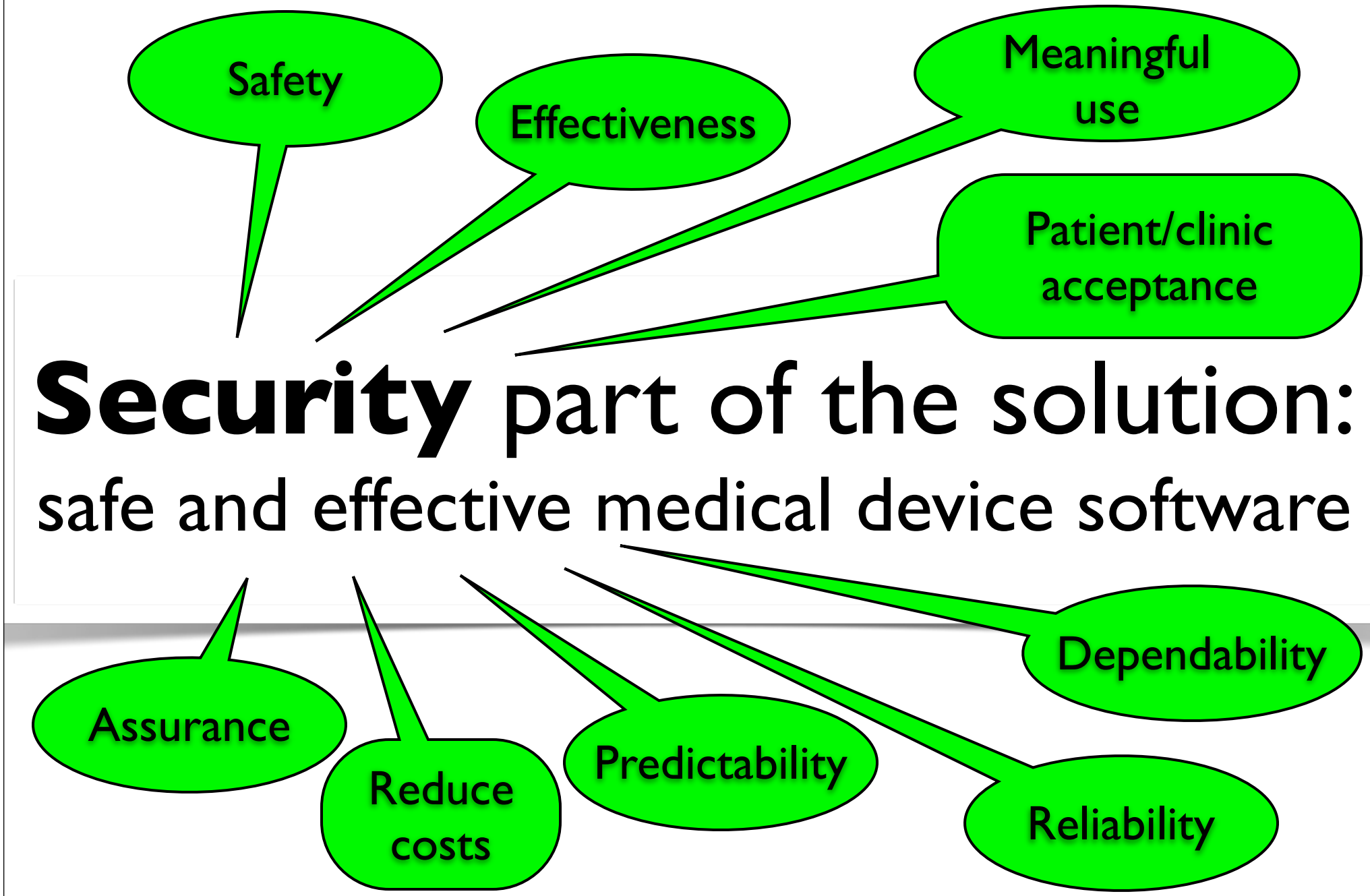
- This presentation is based on both my own research and the research of others. None of the opinions, findings, or conclusions necessarily reflect the views of my past or present employers. Any opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect the views of sponsors.

Computing risks and medical devices?



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

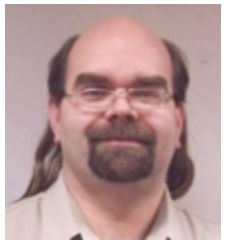
-Captain Schettino, Captain of **Costa Concordia**


Safety
Effectiveness
Meaningful use
Patient/clinic acceptance
Security part of the solution:
safe and effective medical device software
Assurance
Reduce costs
Predictability
Reliability
Dependability

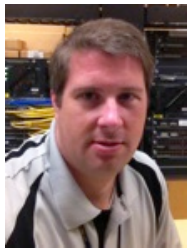
Archimedes Purpose

- What happened at Archimedes?
  - Space for 50, but 65 registered. Travel far!
  - You have all complained to me about the same security problems.
  - Highly interdisciplinary. Everyone here is smart in their field.
  - **Off the record.** Check ego at the door. No buying. No selling.
  - Why does security remain seemingly out of reach?
- Post-Workshop Documents
  - Graduate course reader on medical device security
    http://dollarbillcopying.com/
  - Workshop material on Archimedes members website
    http://secure-medicine.org/members/

Archimedes Speakers

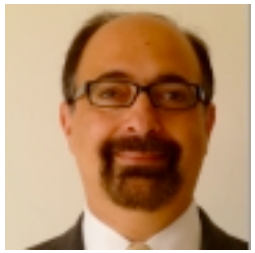


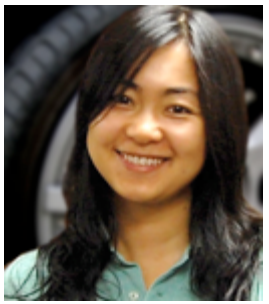











Learning From Others – Do We Repeat Our Failures?
Baxter

Archimedes Medical Device Security Workshop

May 9 – 10, 2013

University of Michigan

ARCHIMEDES

ANN ARBOR RESEARCH CENTER FOR MEDICAL DEVICE SECURITY

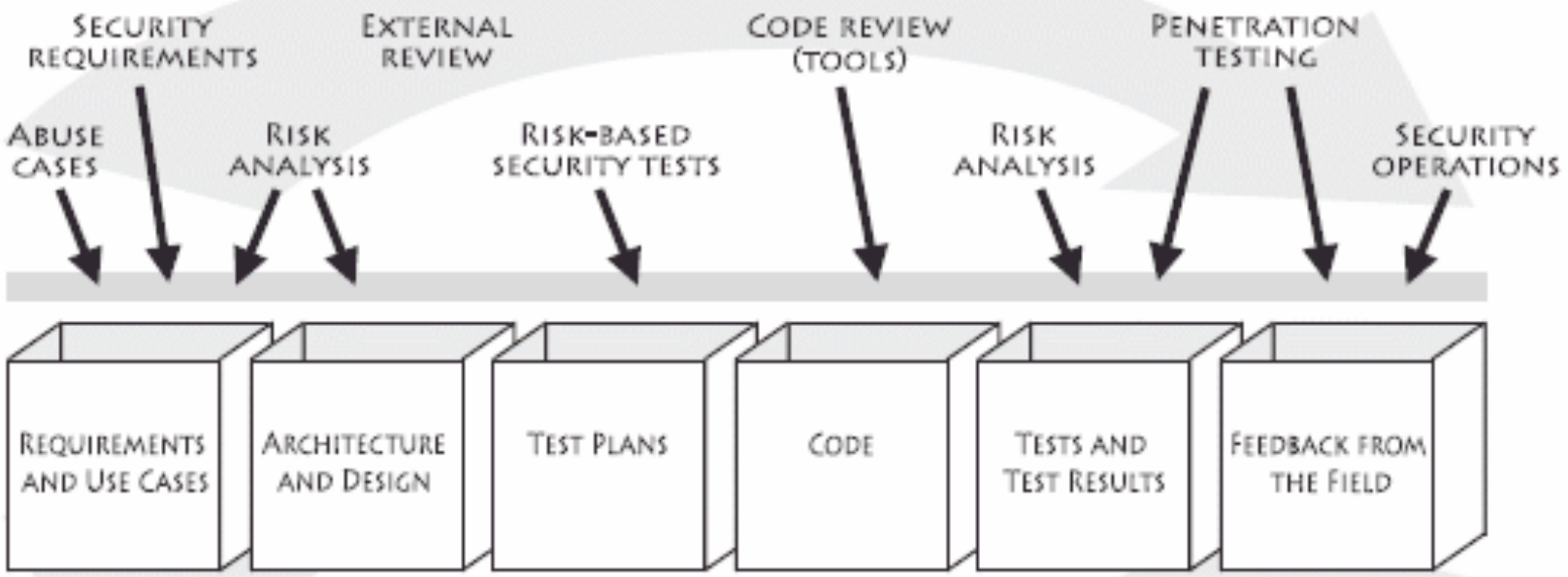
9 Break Out Topics

ARCHIMEDES
ANN ARBOR RESEARCH CENTER
FOR MEDICAL DEVICE SECURITY

- How to integrate risk mgmt w/ SW security lifecycles?
- Explaining SW security to executive mgmt?
- Interoperability and security?
- Responsibility/Accountability: Stop the finger pointing?
- Effective incident and vulnerability reporting mechanisms?
- Dealing with legacy software and software updates?
- Impact of mobile, cloud, and EHRs?
- Avoiding checkbox culture: role of regs and compliance?
- Incentivizing information sharing of threat indicators?

1. SW Security Lifecycles

- How to integrate risk mgmt w/ SW security lifecycles?
- Security development life cycle (SDLC) controls



Credit: Gary McGraw

1. SW Security Lifecycles

- Start early in the life cycle**S**
- Functional requirements often don't cover security
  - Many security requirement are non-functional
- Negative testing is hard, so...
  - Architecture risk analysis (ARA)
  - Threat model informs ARA
  - External expert help is a great idea
  - Automatic analysis for bugs in code

Architectural Risk Analysis Cont'd

- **List of known attacks not enough for sec testing/ analysis**
- Ambiguity analysis = multiple points of view
- Two system architects will always disagree
- Hints from misbehavior
  - "our garage doors are more secure than medical devices"
- Customers often don't know what they want
- **Encryption not a panacea or pixie dust, just a part.**

- **Recommendation: Plan for security in the array of software lifecycles, multi-prong approach**

2. Explaining Security to Mgmt

- Explaining SW security to executive mgmt when
  - "Can't you guys just fix that?" "You guys are in la la land."
- Challenges
  - Lack of knowledge/understanding of software security as it pertains to medical devices
  - Viewing SW security as traditional "marketable feature" triggers a rigid mindset, i.e. a feature is an investment that demands a return
  - Limited data to explain why software security for medical devices should be a priority
  - General fear of the unknown/uncertainty - software security doesn't have simple solution
- **Sad conclusion: Discussing software security in terms of ROI is difficult & often unsuccessful battle**

2. Explaining Security to Mgmt

- Recommendations
  - Stop fighting a losing battle -- avoid the "ROI" trap and frame the discussion on medical software security differently.
    - **Software security = patient safety**
    - Software security is not a "feature"; software security is insurance
    - Software security is about prevention
    - Acknowledge the ambiguity -- there is no "right" answer, only "better"
  - If you must talk about "ROI", ground discussion in **a) protecting the brand, and b) preserving customer trust**.
  - Ground discussion in examples from **other industries** and trends
    - Stuxnet virus, payment card industry data breaches
    - Automotive software vulnerabilities (e.g. tire pressure monitoring systems)
    - Additionally, draw attention to increasing emphasis on HIPAA penalties within government mandated programs (e.g. HITECH act).
  - Build **internal allies** to amplify your message on software security

3. Interoperability & Security

- Component-based security is an oxymoron
  - Secure components necessary, but insufficient
  - Security is an emergent system property
  - Most security flaws derive from unexpected interactions between components that are outside of the model
  - Composability is a hard problem
- **System-level security issues imply system-level safety issues**

- Recommendation: Start with **common language** for expressing meaningful security properties to better understand the emergent properties during composition

4. Ending Security Finger Pointing

- There are good, knowledgeable people on all sides of this issue that want to solve the problem
- Everyone is liable (Whether they know it or not)
- Compliance is not sufficient for Security
- Installations at every site is different. Don't expect it to be easy
- The core issue is **"Safety vs. Safety"**
  - Not "Safety vs. Anti-Safety"
  - Not "Safety vs. Sloth"

4. Ending Security Finger Pointing

- Manufacturers won't make changes without a **market**
- **Customers** don't always have the technical resources to fully understand the problems
- Backend Manufacturer resources are a **scarce resource**
- Customers are "staked elephants" that stopped trying
- **Drop the Myths**
  - **"It's an isolated network"**
  - **"The FDA won't let us patch"**

4. Ending Security Finger Pointing

- Recommendations:
  - **Include IT in the selection process**
  - Caveat Emptor
  - **Communicate the needs**
    - Product Requests
    - Procurement Process
    - Regulatory Process (after diligence)
  - Have Teeth
    - Remove devices that don't meet standards.
    - Think XP!
  - Take advantage of the MDS2 Forms!
  - Use the Best Practices that exist

5. Incident & Vuln. Reporting

- Effective incident and vulnerability reporting mechanisms?
- Barriers
  - **Lack of standard reporting channel**
  - Lifecycle mismatch between medical device and COTS
  - How to bootstrap an effective system with meaningful metrics?
- **Recommendation: Handle incident & vulnerability reporting separately, exploit existing CERTs**
  - http://.../security/

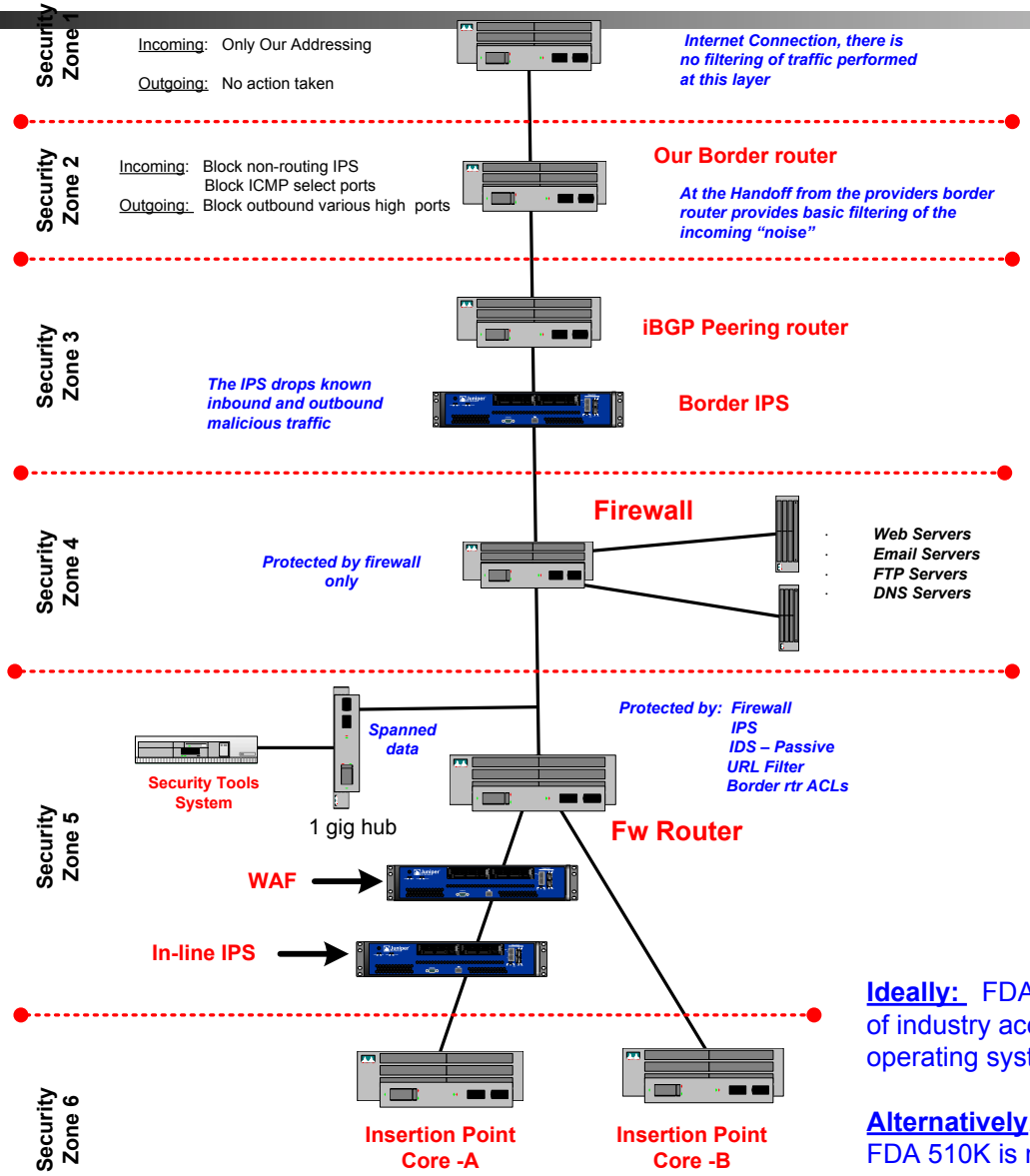
Legacy & Software Updates

- Dealing with legacy software and software updates?

- Comment from anonymous device manufacturer
  "**Need to overcome the inertia due to years of neglect in our legacy products.** Make the case with stakeholders for investing in security without an obvious threat."

Credit: http://mundabor.wordpress.com/2011/03/15/on-making-a-good-lenten-confession/

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]

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.

Windows Microsoft Office

WHY?
Why is support ending for Windows XP SP3 and Office 2003?

WHAT?
What does end of support mean to customers?

HOW?
How will Microsoft help customers?

Windows 7

Get a free IDC assessment on migrating from Windows XP to Windows 7.

See how your organization can benefit from making the switch.

GET STARTED

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 from Gartner Research suggests "many independent software vendors (ISVs) are unlikely to support new versions of applications on Windows XP in 2011; in 2012, it will become common." And it may stifle access to hardware innovation: Gartner Research further notes that in 2012, most PC hardware manufacturers will stop supporting Windows XP on the majority of their new PC models.

Get current with Windows 7 and Office 2010. This option has upside well beyond keeping you supported. It offers more flexibility to empower employees to be more productive, while increasing operational efficiency through improved PC security and management. It also enables your organization to take advantage of latest technology trends such as virtualization and the cloud.

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?

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… of app… inn… Wi…

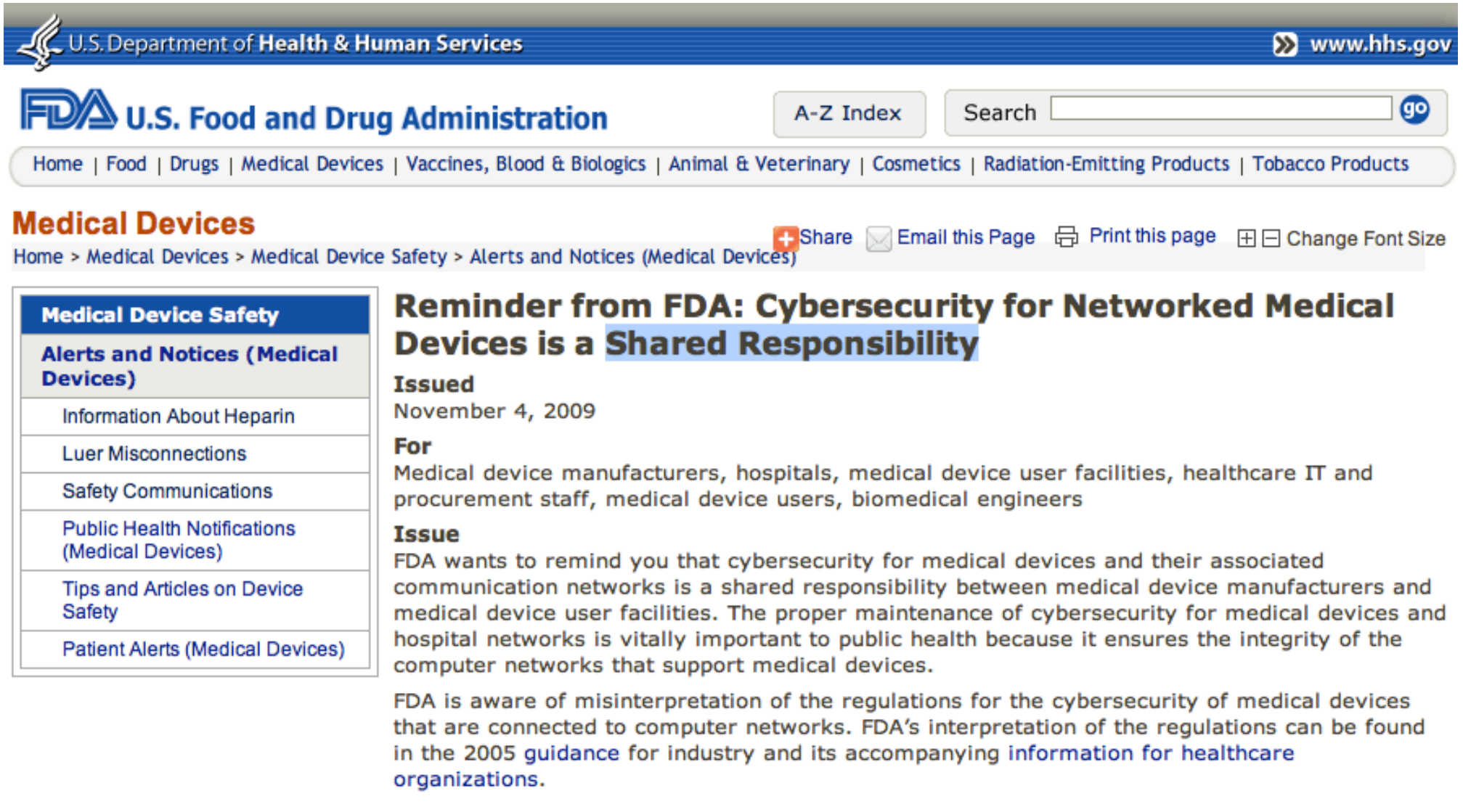
Products Released	Lifecycle Start Date	Mainstream Support End Date	Extended Support End Date	Service Pack Support End Date
Windows XP Embedded	1/30/2002	1/11/2011	1/12/2016	10/22/2004
Windows XP Professional	12/31/2001	4/14/2009	4/8/2014	8/30/2005
Windows XP Service Pack 1	8/30/2002	Not Applicable	Not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

Get cu… …rs more fle… …d PC 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?

Going Beyond: Please Get Along



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.

Mobility, Cloud, EHRs…

- Impact of mobile, cloud, EHRs, apps, etc?

- Recommendation:
  Follow a system of systems engineering approach

Med Dev to Mobile Dev & Cloud

Different security requirements

Traditional Security

Each device/target has different security requirements. This is reflective of traditional security for mobile devices, cloud, & big data

Problem = Giving up control, chain reaction

Problem is in complexity of an expanding system. We are, by definition, giving up control; this also has a chain reaction.

What is a med dev & a mobile device?

Problem environment is in the integration of medical devices with mobile devices

Assurances

Cloud

- Associates
- Private
- Public

Cloud: needs, assurance, trust and SLAs, little other control

Solution

- Systems Approach
- Device Approach

Solution: Whilst a device approach is necessary independently, a systems approach is required to at least try to control some of the variable. A layered solution (as is traditional for security)

Semantic Interoperability

Big data has its own issues of semantics, context, interpretation (not solely the domain of medical devices data collection.

- Big Data
- Clinical Safety
- Problem of integration to mobile
- (Traditional Failure)

A new and bigger problem we introduce when integrating to mobile and big data, is semantic interoperability. This directly may impact clinical safety.

"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

8. Role of Regs & Compliance

- **Avoiding checkbox culture**: role of regs & compliance?
- Regulations less necessary when voluntary market driven self regulations fulfill the needed compliance to **prevent chaos and harm**.
- Instill confidence in health care providers to **Trust Their Instruments.**
- FDA & FCC to facilitate creation of new class of Computing platforms that pertains to healthcare and incentivize adoption of security standards.
- Healthcare providers: Secure/Isolate, best Practices for infrastructures for medical devices connectivity
- …


6. BLUETOOTH FOR HEALTH
STANDARD
7. REGULATION, GUIDANCES
STANDARDS, BEST PRACTICES
8. BUSINESS CASE FOR

badness-ometer != security meter

badness-ometer

cigital

9. Solving the Bad News Diode

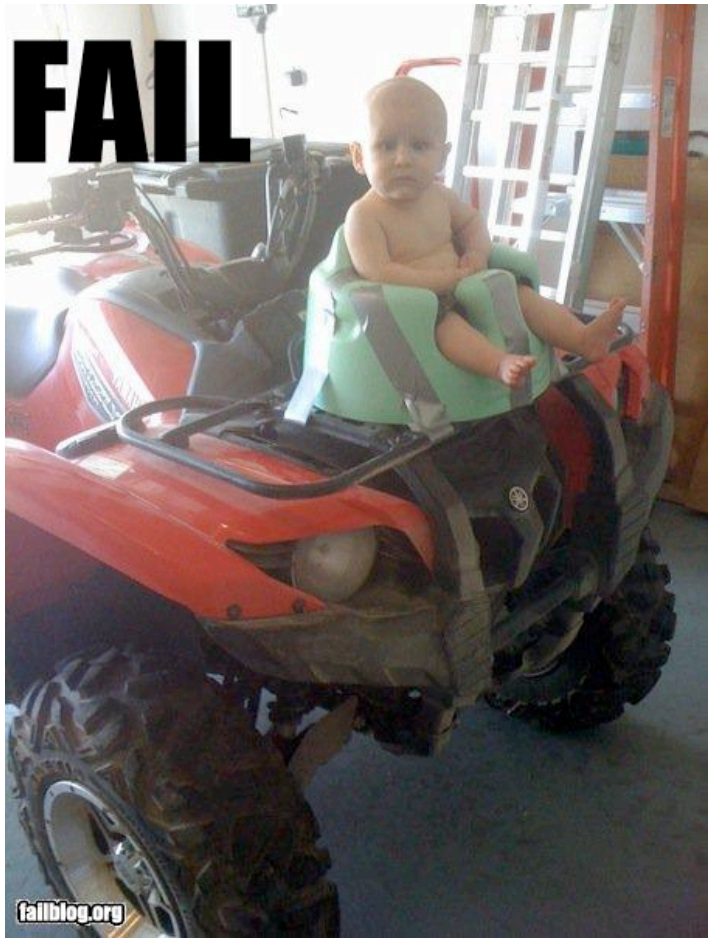
- Incentivizing information sharing of threat indicators?
- Barriers to learning from history
  - Acquiring data, trend, and comparison to other industries
  - How to take data to do decision making
  - Time to take action/close vulnerabilities
  - Large capital-replacement cycles

- Recommendation:
  A security risk and reporting system is needed
  - But who funds?
  - But who owns?

←Ways Forward ↗

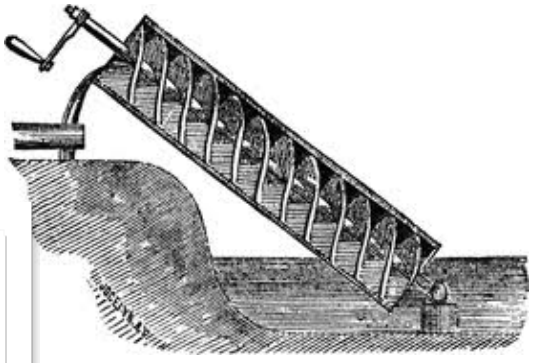
Security should be **designed** in

not **bolted** on



Cybersecurity: A Foreseeable Risk

- Biggest risk:
  - ~~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
- Stay informed
  - Individuals: Read **blog.secure-medicine.org**
  - Institutions: Join Archimedes



Archimedes Screw was invented to be the first bilge pump for a sinking ship.

Ann Arbor Research Center for Medical Device Security

secure-medicine.org

Industrial membership program: briefings, training, networking for engineers and executives in medical device manufacturing