



Interdisciplinary Security: Medical Devices



Kevin Fu

Associate Professor
Computer Science & Engineering
University of Michigan

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



Supported in part by NSF
CNS-1330142 and CNS-1331652.
Any opinions, findings, and
conclusions expressed in this material
are those of the authors and do not
necessarily reflect the views of NSF.

Correctness is easy.

Security is hard.



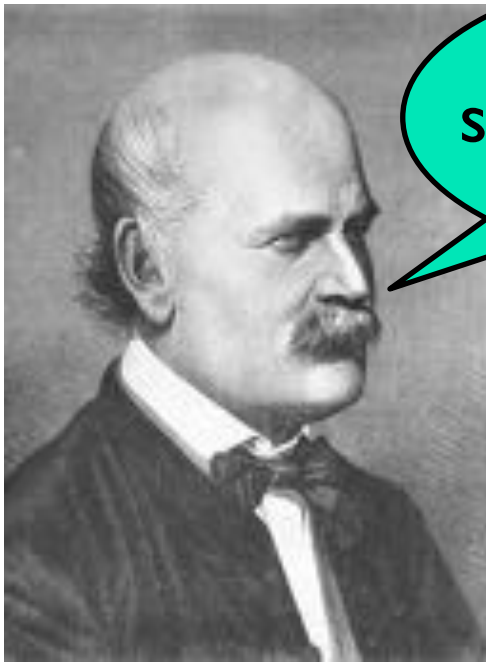
Photo by Kevin Fu

Background & Disclosures

- Co-founder, Virta Labs
- Security & Privacy Research Group @ Michigan
- Director, Archimedes Center for Medical Device Security
- Co-chair, AAMI Working Group on Medical Device Security
- Member, NIST Information S&P Advisory Board
- Consultant to Samsung, MicroCHIPS Biotech
- Fmr. visiting scientist, U.S. Food and Drug Administration
- Recent research support from NSF, HHS, SRC, DARPA, MARCO, UL, Medtronic, Philips, Siemens, WelchAllyn

Semmelweis to Software Sepsis

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



Physicians
should their wash
hands.

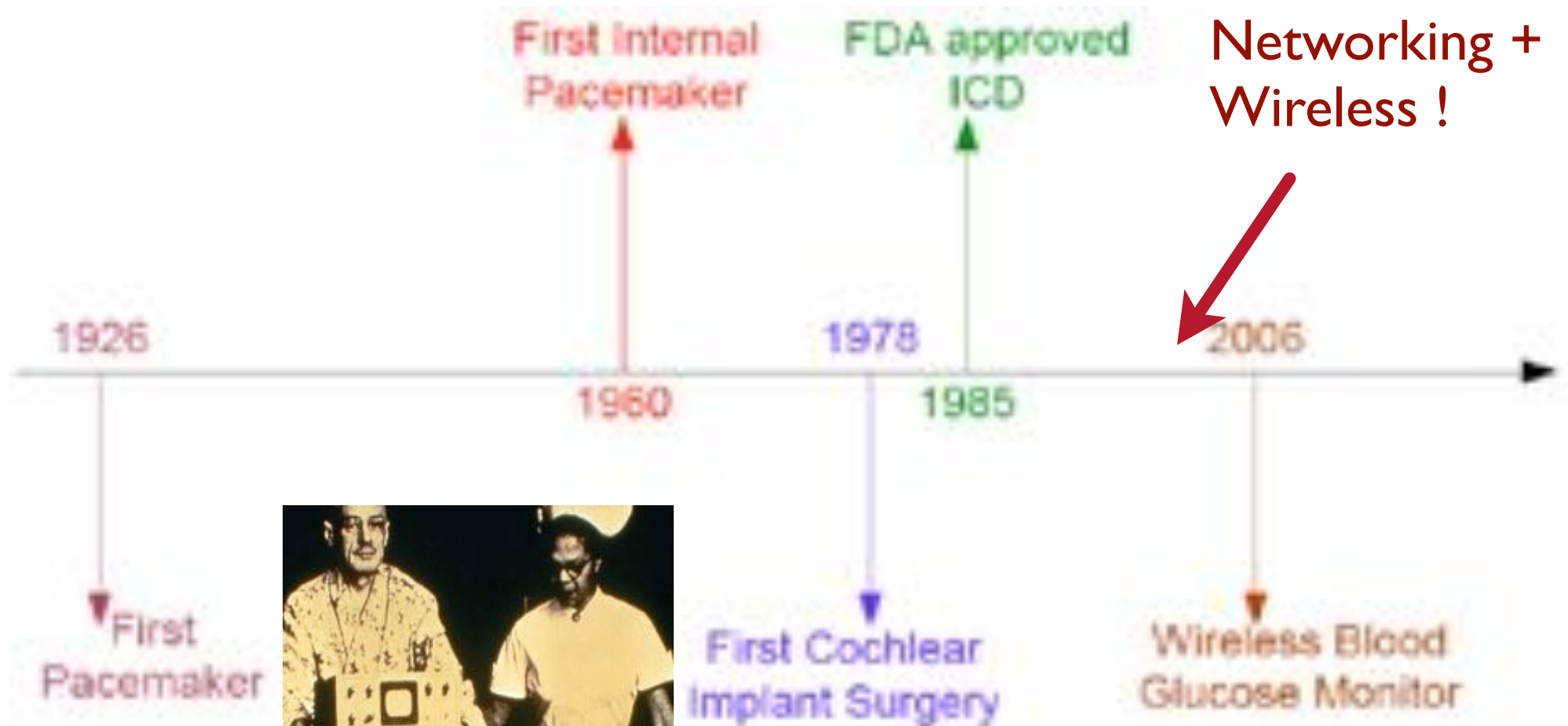
Dr. Ignaz Semmelweis
1818-1865



Doctors
are gentlemen and
therefore their hands are
always clean.

Dr. Charles Meigs
1792-1869

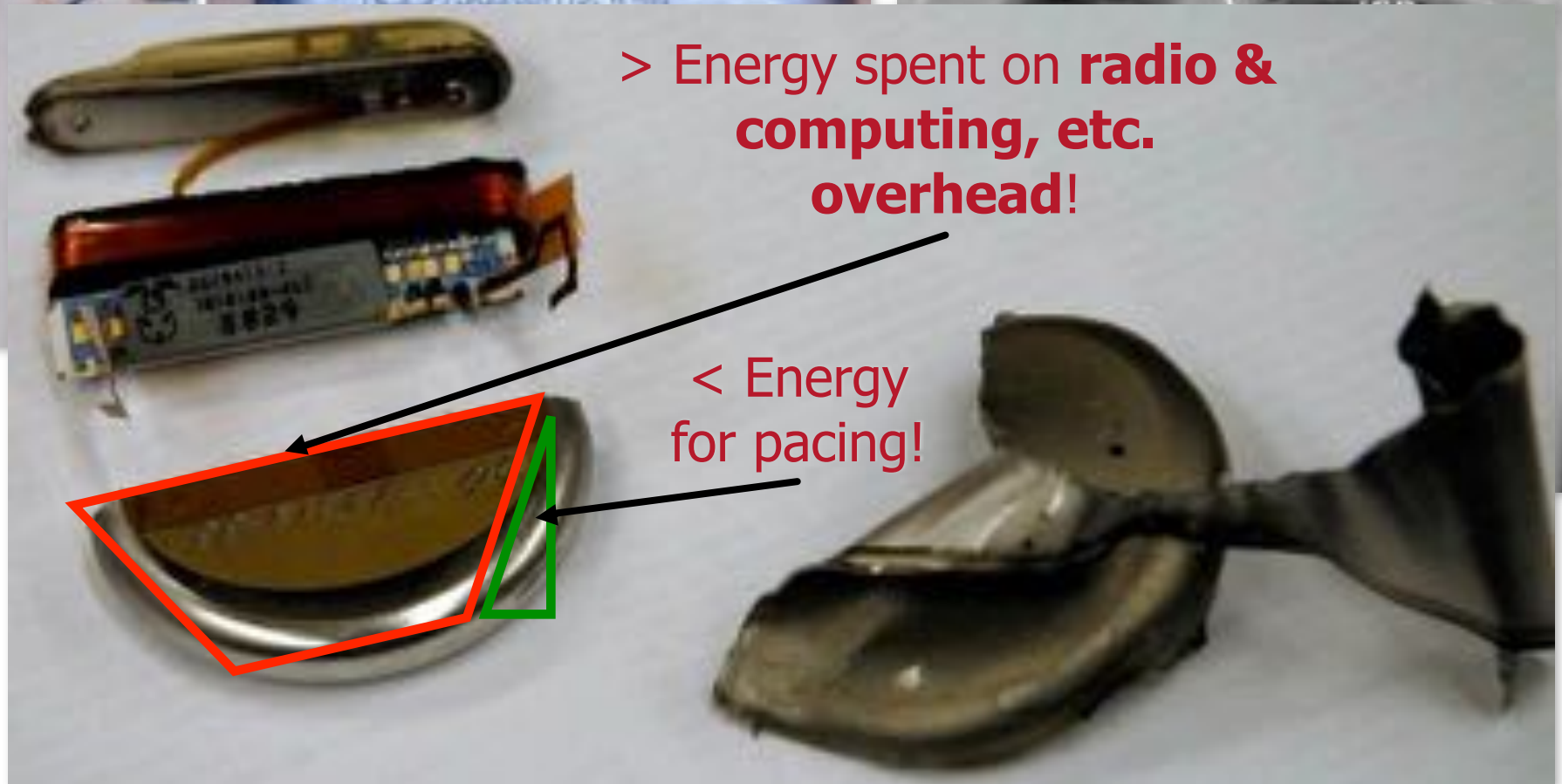
Networking +
Wireless !



Photos from:
Medtronic



Pacemakers: Regulate heartbeat



Wireless medical devices:
great benefits.
subtle inconvenient risks.

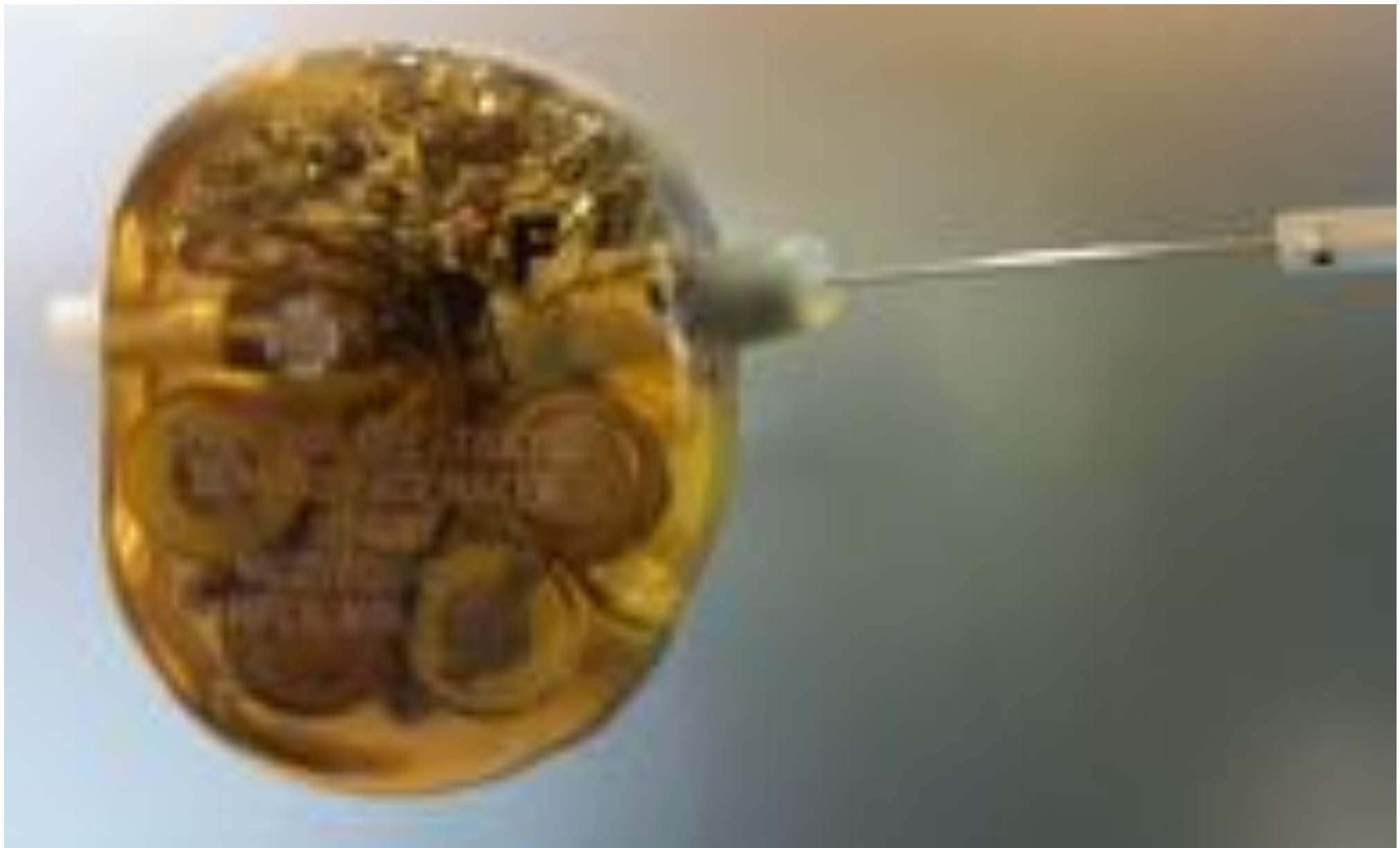
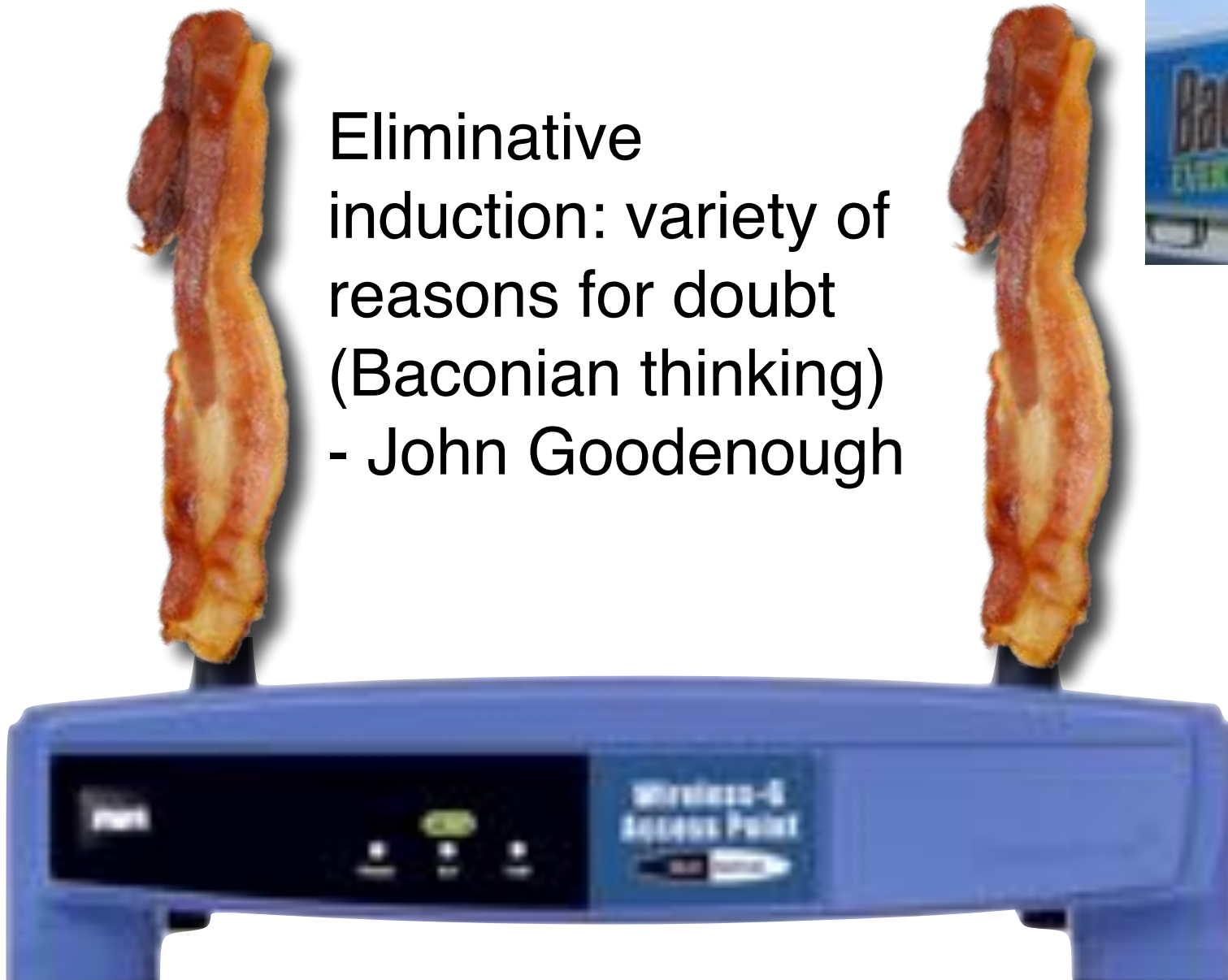


Photo by Kevin Fu @ Medtronic museum

Wireless Makes Everything Better?

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



Short History: Medical Devices & SW

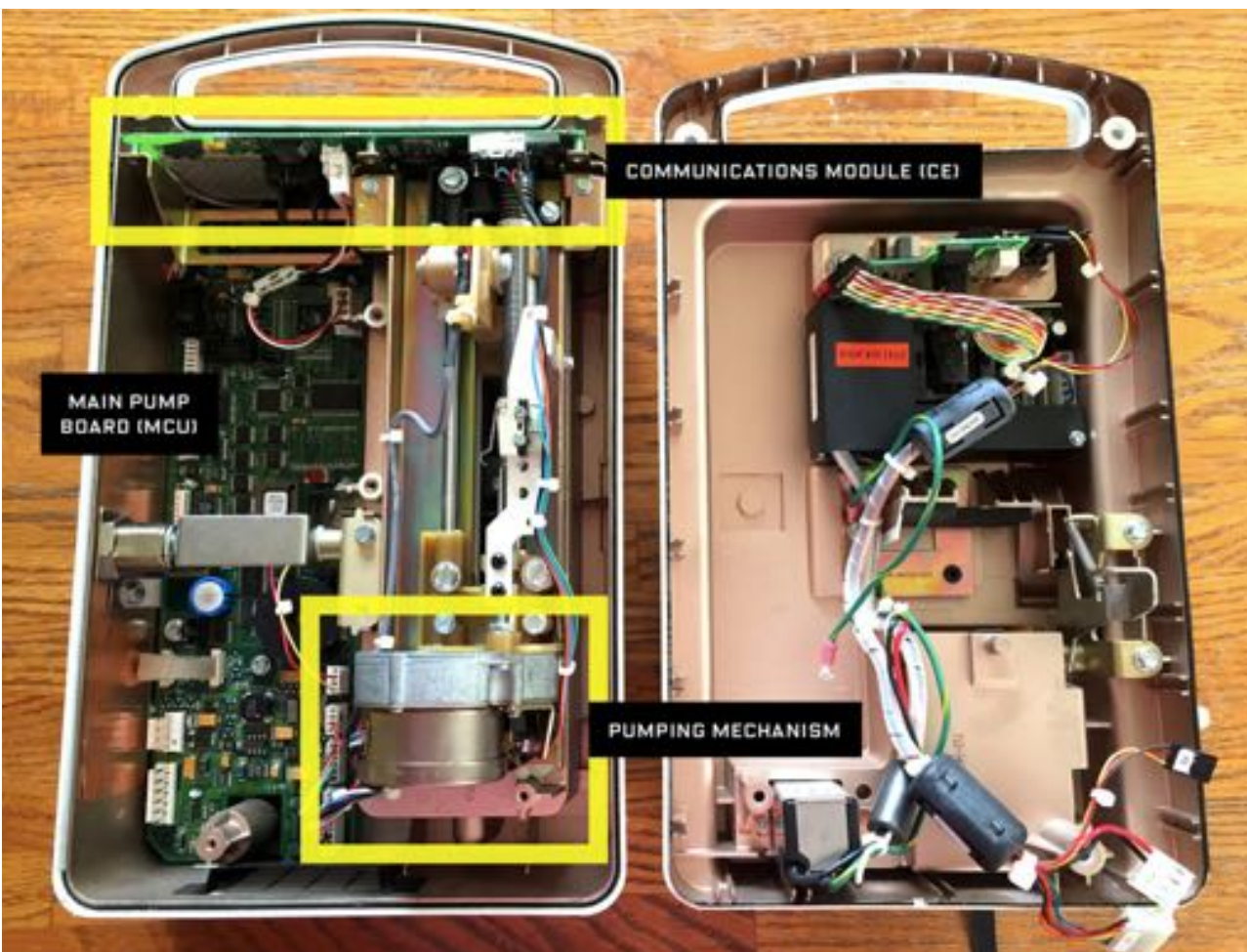
- Therac-25 analysis
[Leveson & Clark, IEEE Computer, 1993]
- Defibrillator cybersecurity
[Halperin et al., IEEE Symposium on Security & Privacy, 2008.]
- Insulin pump analysis, 2011 [several]
- Defib jamming defense
[Gollakota et al., ACM SIGCOMM 2011]
- Pacemaker hack reproduced
[Barnaby Jack, BlackHat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



Photos: Leveson, Fu

Short History: Medical Devices & SW

- Hospira Infusion Pump Vulnerabilities [Billy Rios and more, 2014-2015]



Photos: Wired

Short History: Medical Devices & SW

- Hospira Infusion Pump Vulnerabilities
[Billy Rios and more, 2014-2015]

U.S. Food and Drug Administration
Protecting and Promoting *Your* Health

LifeCare PCA3 and PCA5 Infusion Pump Systems by Hospira: FDA Safety Communication - Security Vulnerabilities

[Posted 05/13/2015]

AUDIENCE: Pharmacy, Nursing, Risk Manager, Engineering

ISSUE: The FDA and Hospira have become aware of security vulnerabilities in Hospira's LifeCare PCA3 and PCA5 Infusion Pump Systems. An independent researcher has released information about these vulnerabilities, including software codes, which, if exploited, could allow an unauthorized user to interfere with the pump's functioning. An unauthorized user with malicious intent could access the pump remotely and modify the dosage it delivers, which could lead to over- or under-infusion of critical therapies. The FDA is not aware of any patient adverse events or unauthorized device access related to these vulnerabilities.



Photos: Wired

Short History: Medical Devices & SW

- Hospira Infusion Pump Vulnerabilities
[Billy Rios and more]

Wireless
keys stored
unencrypted, accessible
via telnet/FTP!

U.S. Food and Drug Administration
Protecting and Promoting Your Health

LifeCare PCA3 and PCA5 Pump Systems by Hospira Safety Communication - Security Vulnerabilities

[Posted 05/13/2015]

AUDIENCE: Pharmacy, Nursing, Risk Management

ISSUE: The FDA and Hospira have become aware of vulnerabilities in Hospira's LifeCare PCA3 and PCA5 Infusion Pump Systems. An unauthorized user with access to information about these vulnerabilities, including software code, could use this information to allow an unauthorized user to interfere with the pump's function. An unauthorized user with malicious intent could access the pump remotely and modify the pump's settings, which could lead to over- or under-infusion of critical therapies. The FDA is not aware of any patient adverse events or unauthorized device access related to these vulnerabilities.

Hard-
coded local
accounts!



Photos: Wired

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

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 ~ 1 msec to the T-wave
- Designed to induce ventricular fibrillation
- No RF amplification necessary

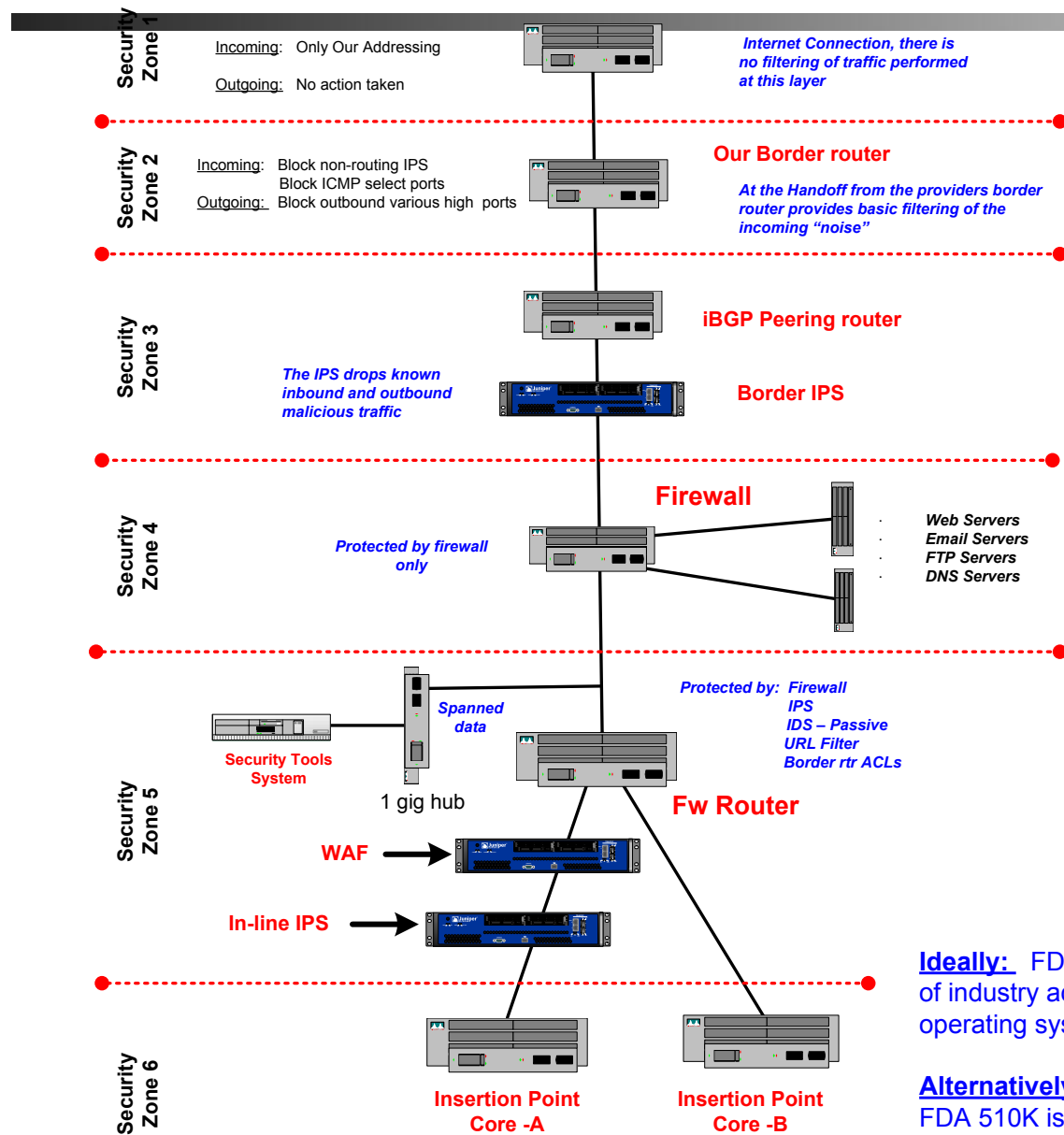


[Halperin et al., IEEE Symposium on Security & Privacy 2008]

Hospitals & Malware



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 9815
Windows 2000.....23
Windows CE.....9
Windows Vista0
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

Factory-installed malware?

More common than you might think

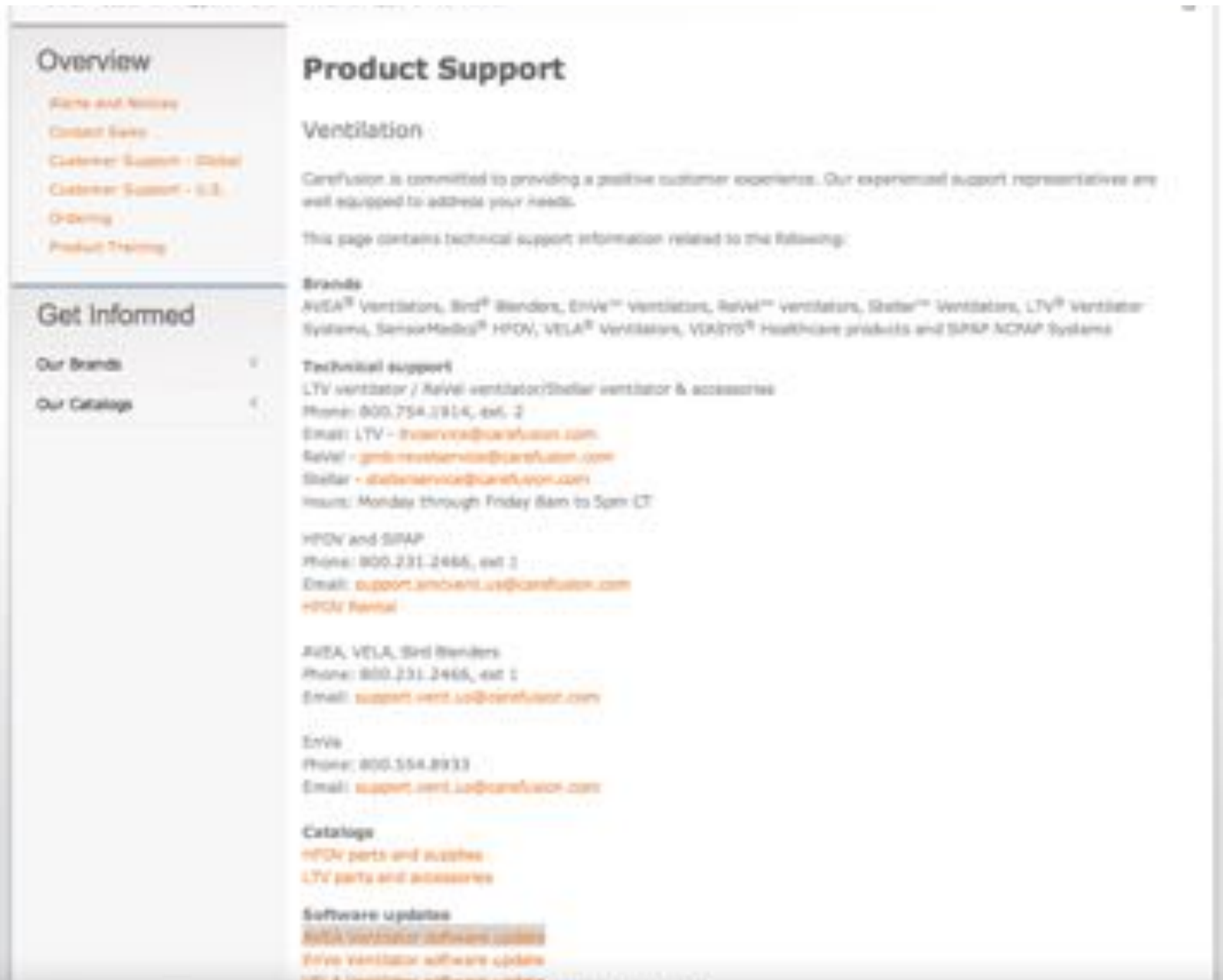
- Vendors with USB drives
- Vendors repairing infected machines
- Product assembly line

Shoot P0wn Foot w/ Software Update



[Photo: Care Fusion, Niels Provos]

Shoot P0wn Foot w/ Software Update



The screenshot shows the 'Product Support' section of the CareFusion website. On the left is a navigation menu with 'Overview' (containing links for Home and News, Contact Sales, Customer Support - Global, Customer Support - U.S., Ordering, and Product Training) and 'Get Informed' (containing links for Our Brands and Our Catalogs). The main content area is titled 'Product Support' and 'Ventilation'. It states that CareFusion is committed to providing a positive customer experience and that the page contains technical support information. It lists various brands supported, including AvEA, Bird, Enve, ReVe, Stellar, LTV, SensorMedics, HFOV, VELA, VEAUTO, and SPPAP. It provides technical support details for LTV, ReVe, and Stellar ventilators, including phone numbers, email addresses, and hours of operation. It also provides support details for HFOV and SPPAP systems, and for rental services. Finally, it lists catalog links for HFOV parts and supplies, LTV parts and accessories, and software updates for AvEA, ReVe, and Enve ventilators.

Overview

- [Home and News](#)
- [Contact Sales](#)
- [Customer Support - Global](#)
- [Customer Support - U.S.](#)
- [Ordering](#)
- [Product Training](#)

Get Informed

- [Our Brands](#)
- [Our Catalogs](#)

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[®] Ventilators, Enve[™] Ventilators, ReVe[™] Ventilators, Stellar[™] Ventilators, LTV[®] Ventilator Systems, SensorMedics[®] HFOV, VELA[®] Ventilators, VEAUTO[®] Healthcare products and SPPAP ACNP Systems

Technical support

LTV ventilator / ReVe ventilator/Stellar ventilator & accessories
Phone: 800.754.3914, ext. 2
Email: ltservice@carefusion.com
ReVe - rmbservice@carefusion.com
Stellar - stellerservice@carefusion.com
Hours: Monday through Friday 8am to 5pm CT

HFOV and SPPAP
Phone: 800.231.2446, ext 1
Email: support.ambvent.us@carefusion.com
[HFOV Rental](#)

AvEA, VELA, Bird Ventilators
Phone: 800.231.2446, 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 updates](#)
- [ReVe ventilator software updates](#)
- [Enve ventilator software updates](#)

[Photo: Care Fusion, Niels Provos]

Shoot P0wn Foot w/ 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 nikju.com/, lilupophilupop.com/, koklik.com/.

This site was hosted on 1 network(s) including [AS28851 \(CAREFUSION\)](#).

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



[Photo: Care Fusion, Niels Provos]

Cures Worse Than the Disease

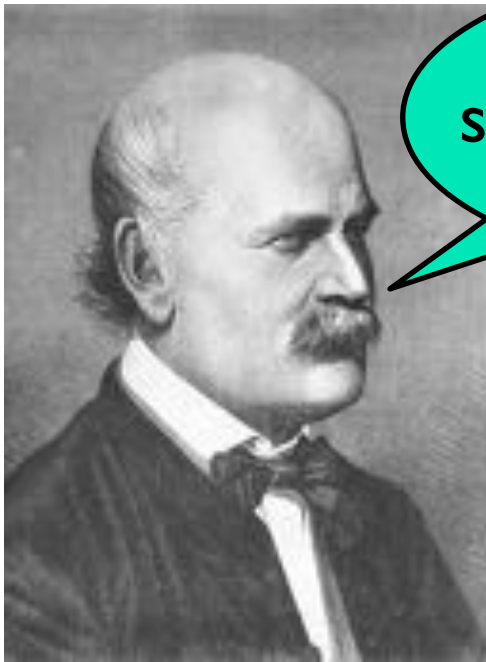
- Health Information Technology (HIT) devices globally rendered unavailable
- Cause: Automated software update went haywire
- Numerous hospitals were affected April 21, 2010
 - Rhode Island: a third of the hospitals were forced ``to postpone elective surgeries and stop treating patients without traumas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

Semmelweis to Software Sepsis

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



Physicians
should wash their
hands.

Dr. Ignaz Semmelweis
1818-1865

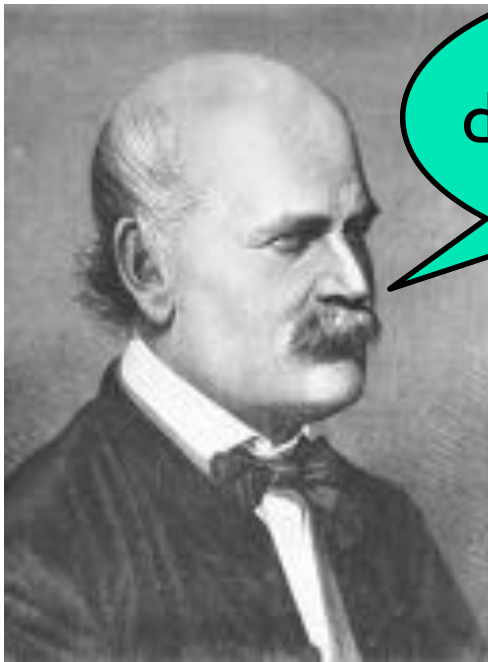


Doctors
are gentlemen and
therefore their hands are
always clean.

Dr. Charles Meigs
1792-1869

Semmelweis to Software Sepsis

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



Medical devices should be secure.

Dr. Ignaz Semmelweis
1818-1865



Doctors are gentlemen and therefore their computers are always secure.

Dr. Charles Meigs
1792-1869

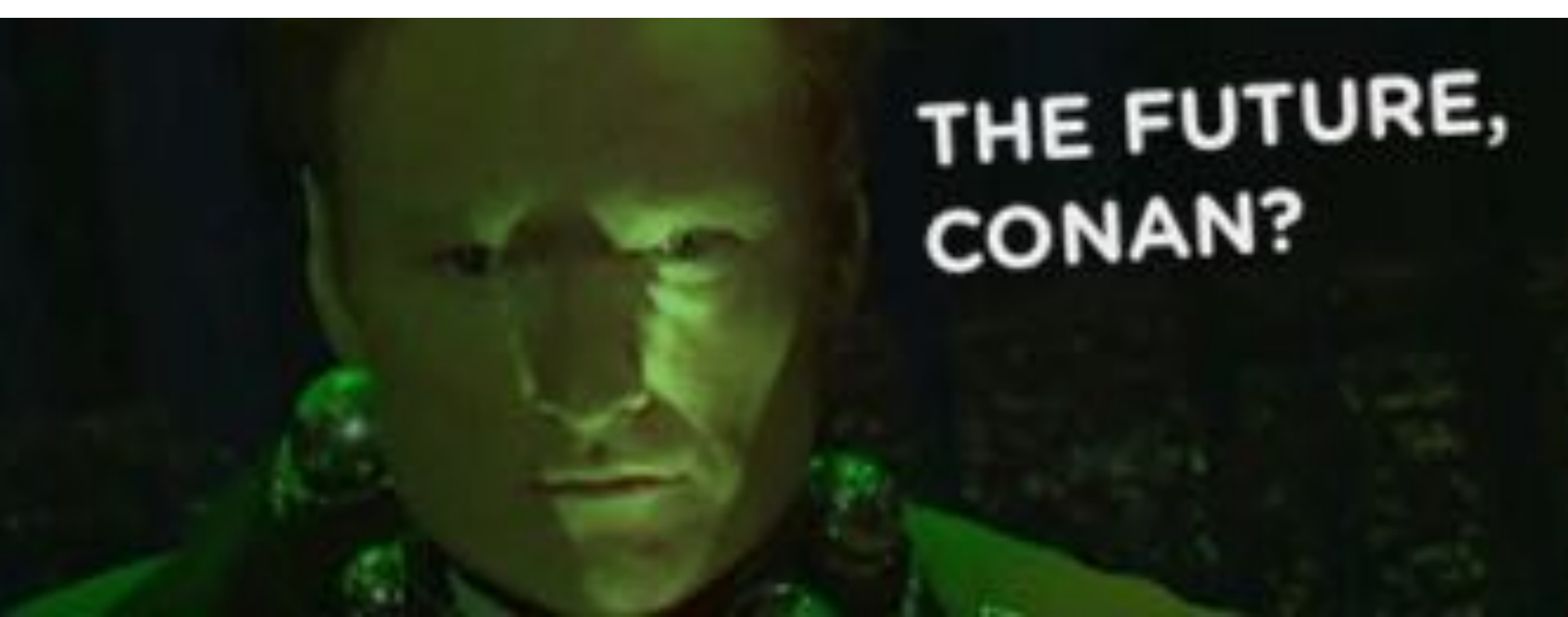
← Ways Forward ↗

Security should
be designed in



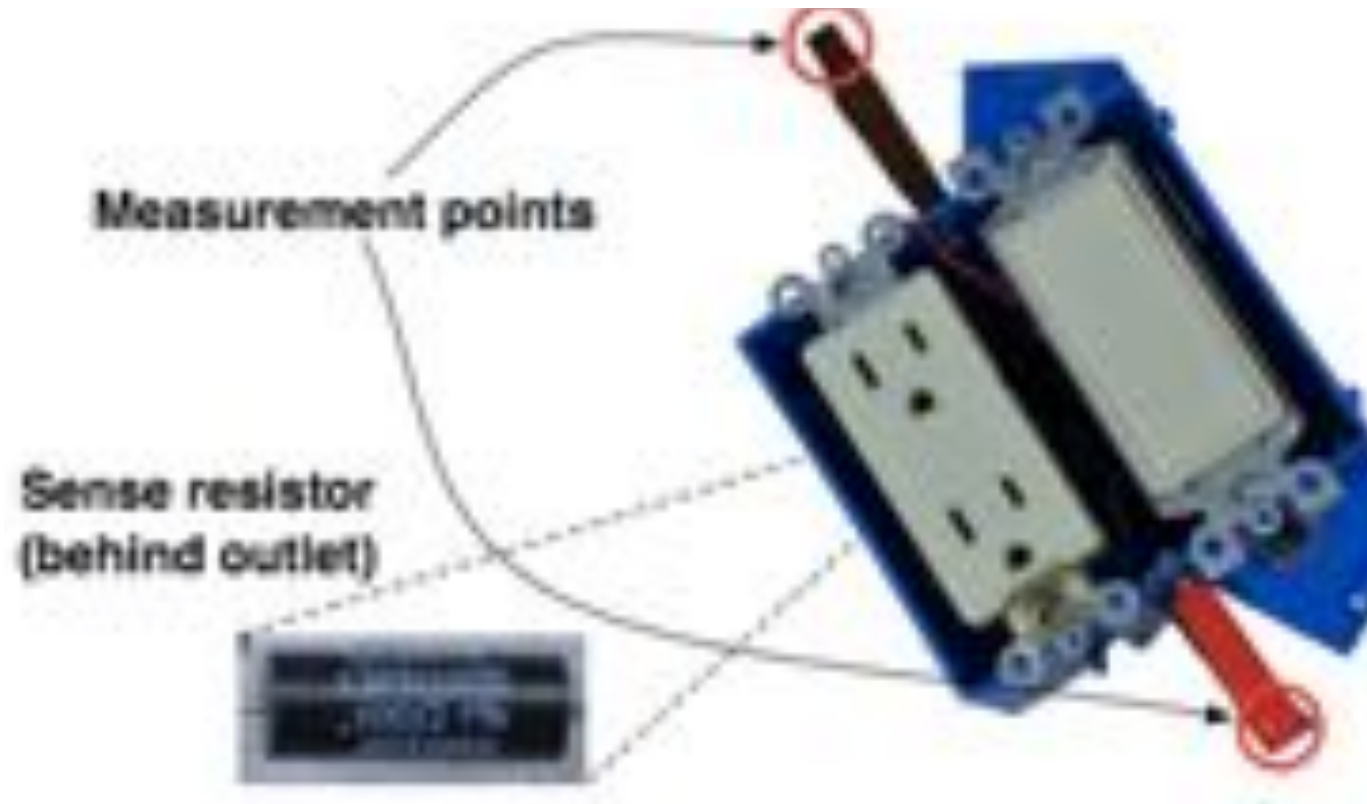
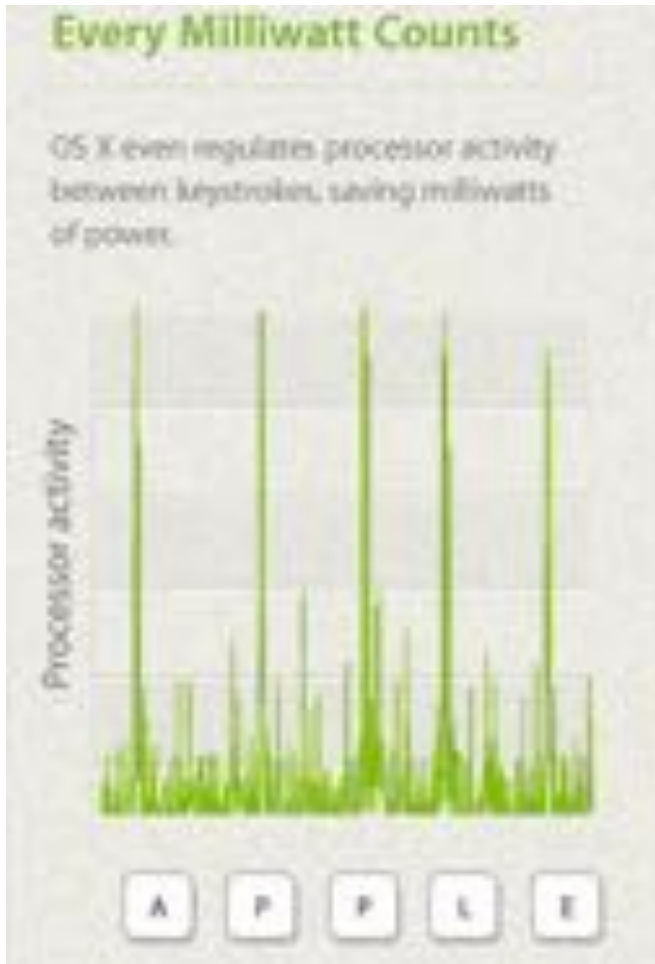
not bolted on





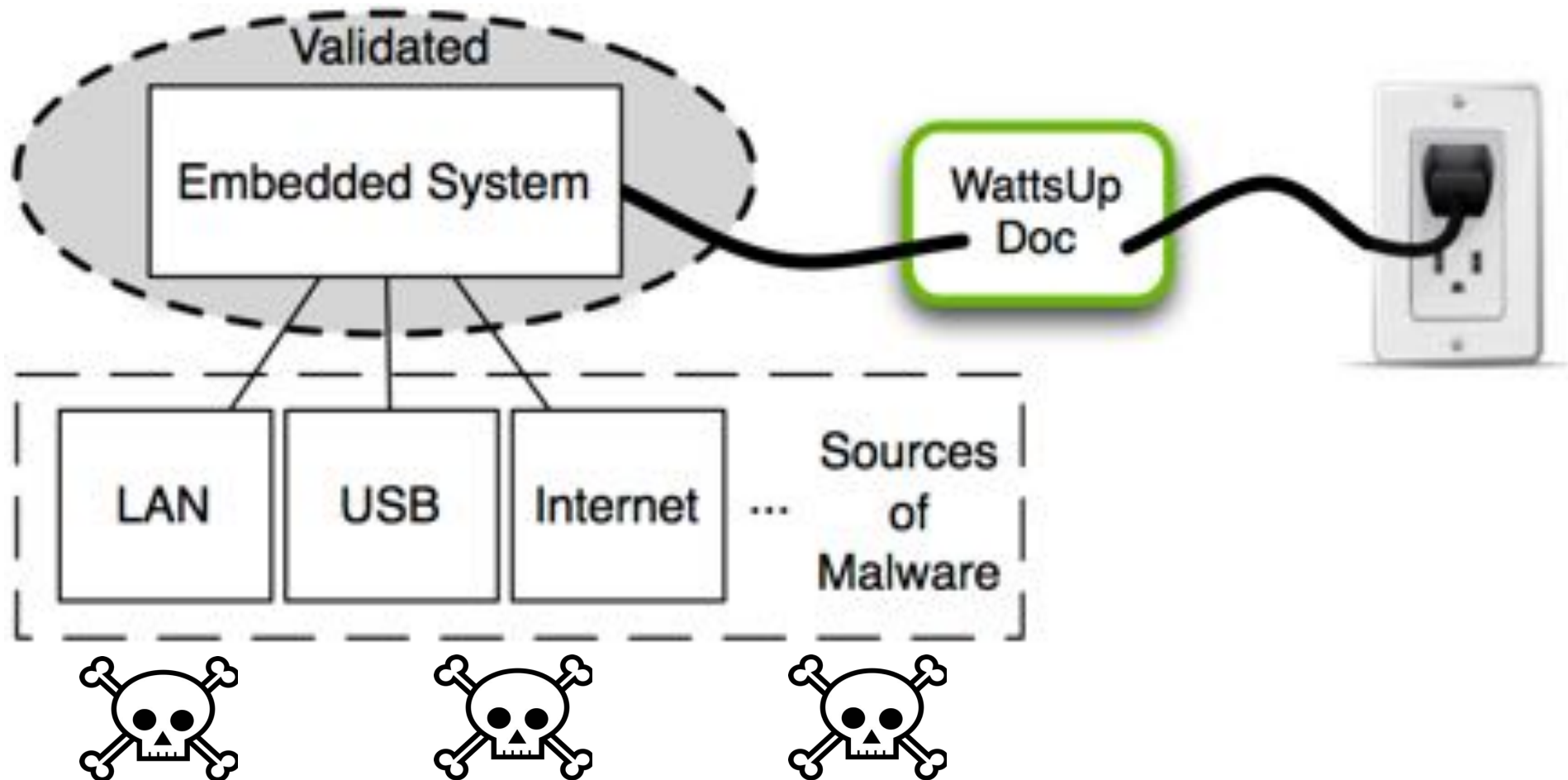
Emerging Research: Analog Cybersecurity

Detecting Malware at Power Outlets



(a) An Apple advertisement from 2009 [6] touts energy-efficiency gains that also happen to reveal keystrokes in power traces.

Research: WattsUpDoc





120VAC 1.5A MAX

PowerGuard

VirtaLabs

VIRTA LABORATORIES, INC.
HW1.0

VirtaLabs

Why do you trust the
SENSOR?

Many reports of accidental interference

“Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors” by Foo Kune et al. In Proc. IEEE Symposium on Security and Privacy, 2013.

Joint work with Denis Foo Kune (U. Michigan),
John Backes (U. Minnesota), Shane Clark (U. Mass Amherst),
Dr. Dan Kramer (Beth Israel Deaconess Medical Center),
Dr. Matthew Reynolds (Harvard Clinical Research Institute),
Yongdae Kim (KAIST), Wenyan Xu (U. South Carolina)



Many reports of accidental interference

Cellphone
+
Oven

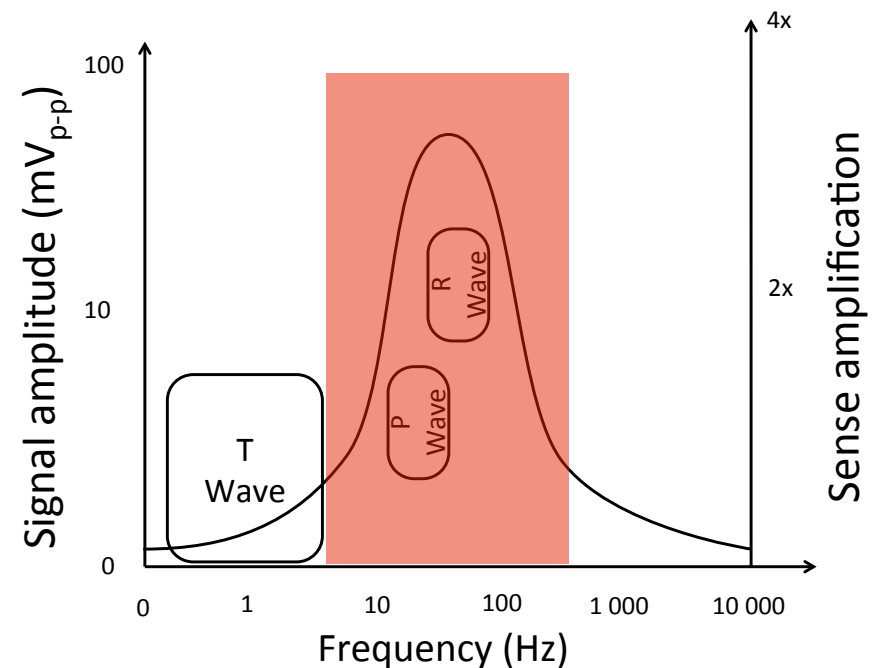
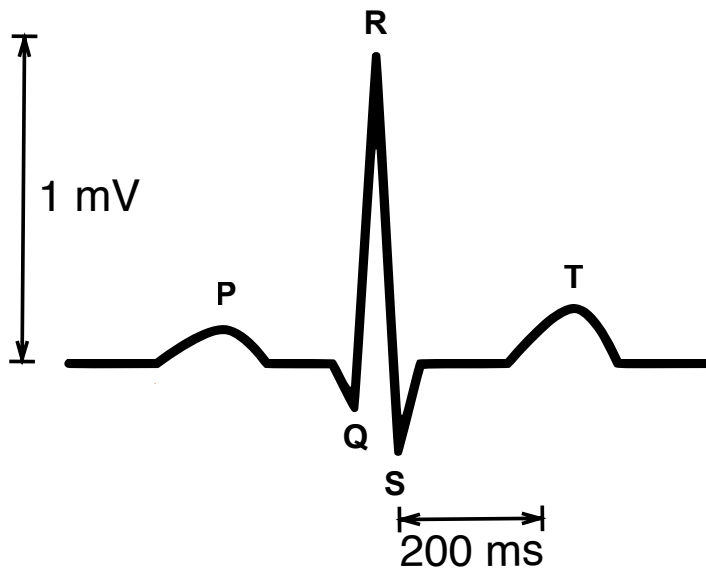


New York Times
Aug 21 2009



Cardiac devices vulnerable to baseband EMI

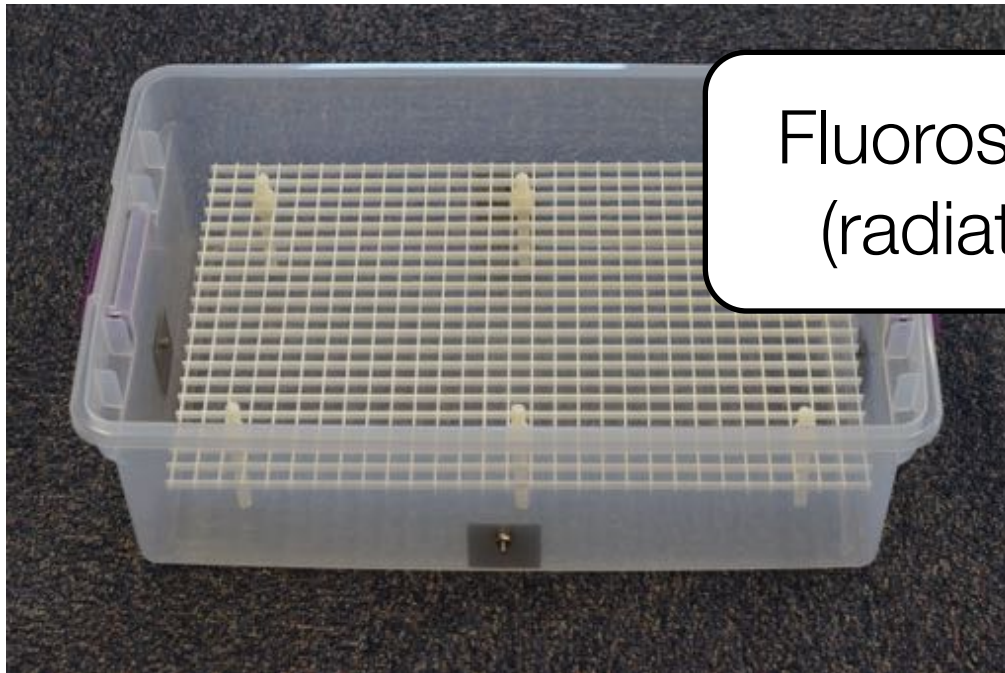
- Filter high frequency
 - 800MHz and GHz range: attenuation of up to 40dB
- Can't filter baseband



Cohan et al, 2008

Experimental setup: Simulators

Saline bath



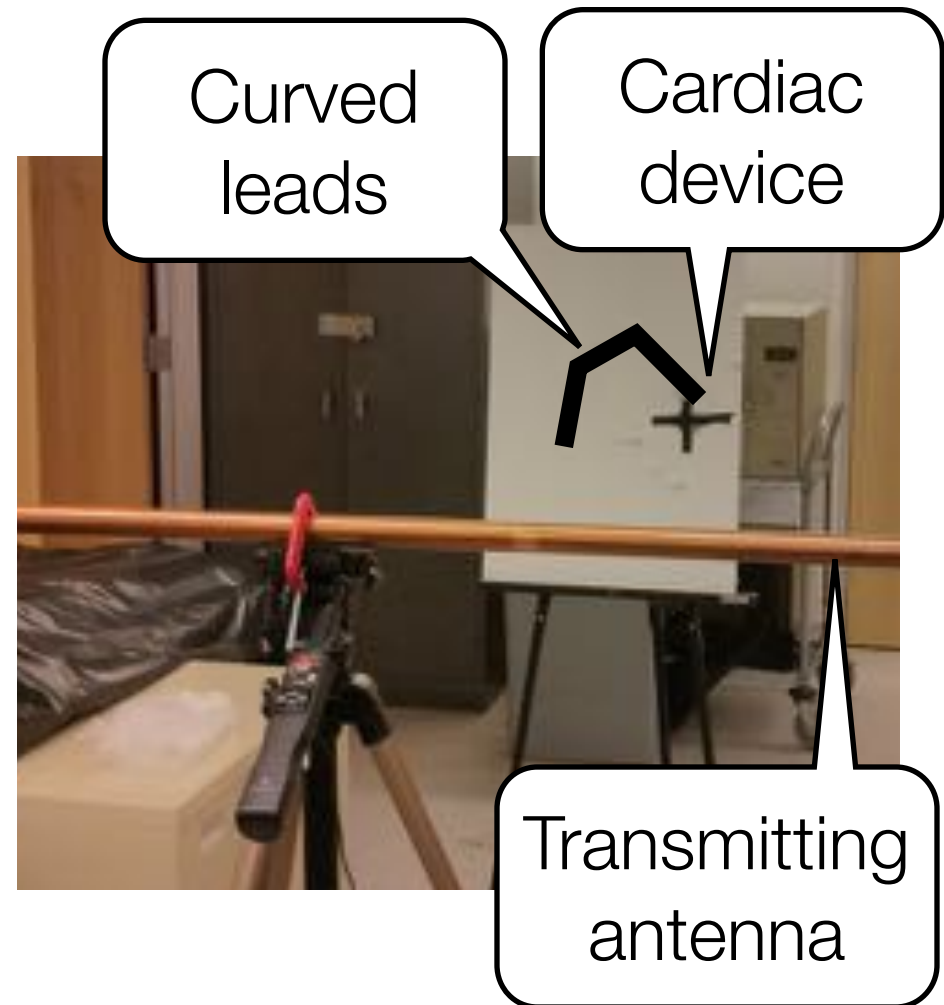
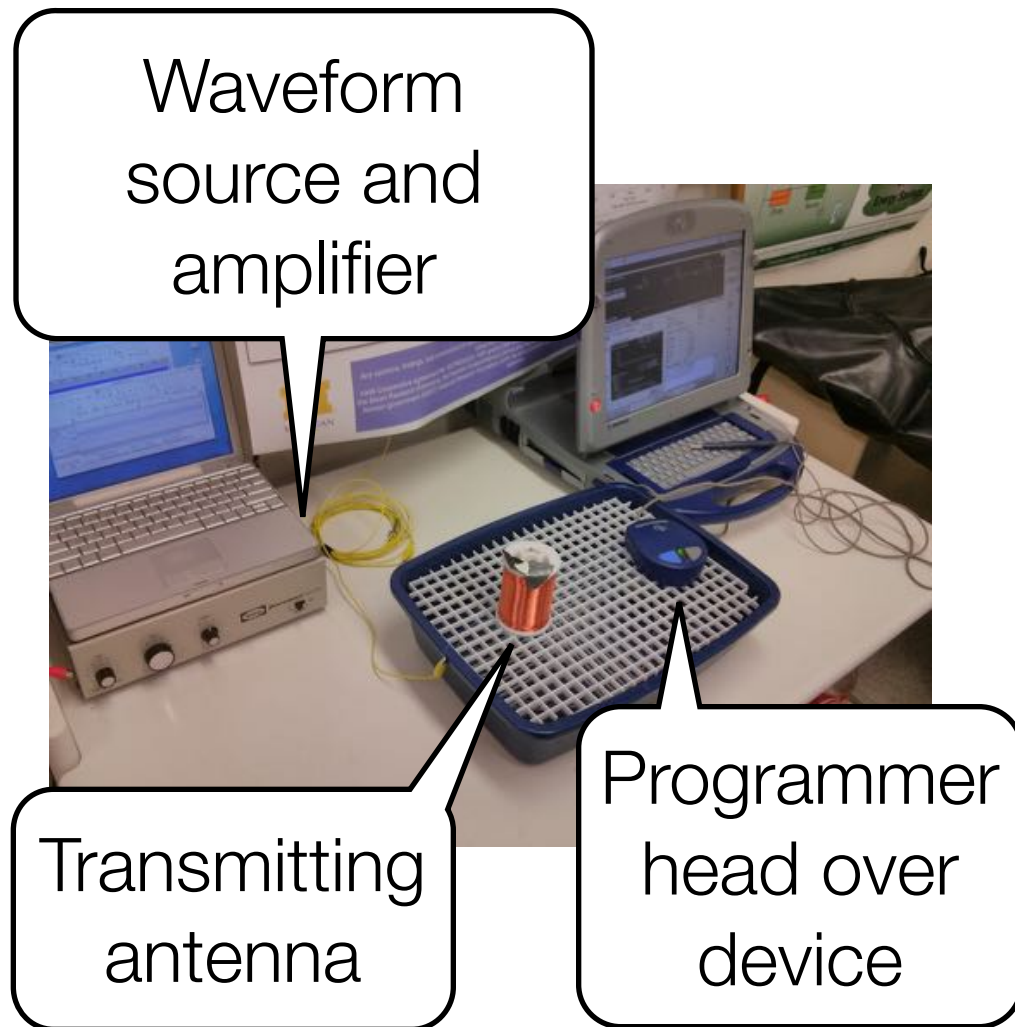
Fluoroscope
(radiation)

Synthetic human



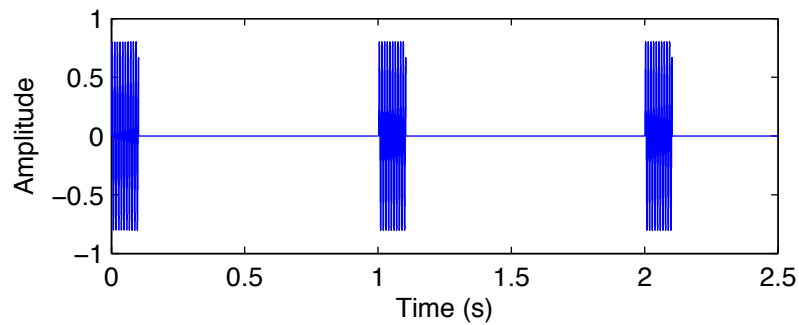
Lead
vests

Experimental setup: Devices and emitters

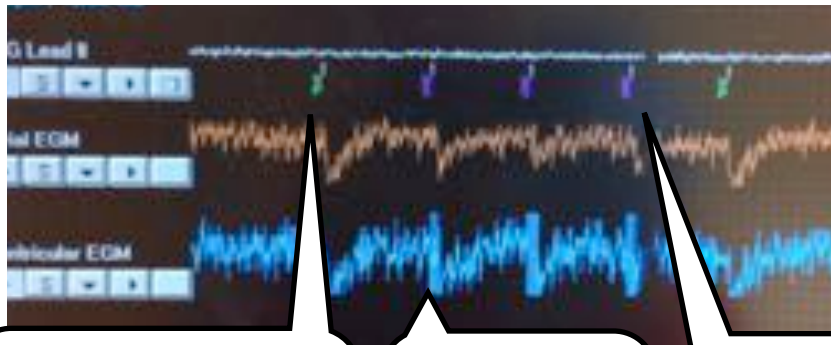
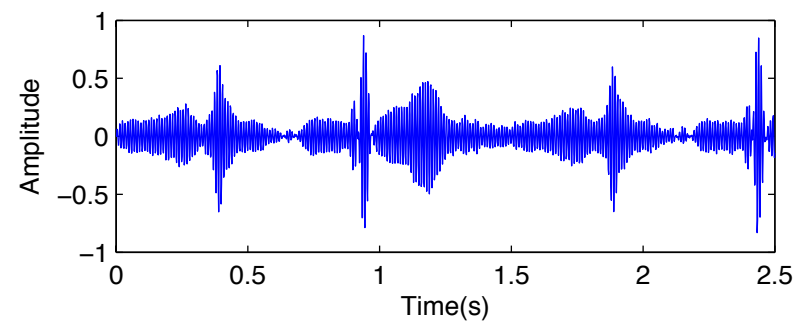


Results: Waveforms and responses

Pulsed sinusoid



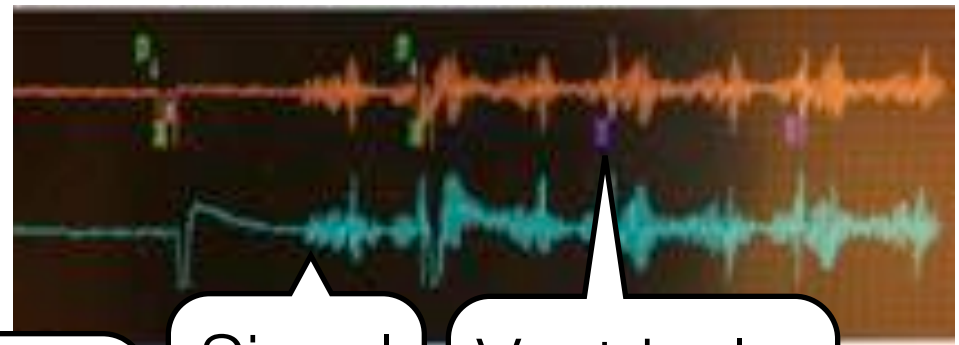
Modulated heart beat



Ventricle
pace

Signal
onset

Ventricle
sense



Signal
onset

Ventricle
sense

Z-axis of MEMS gyroscopes



- 8 kHz acoustic tone hits resonant frequency of MEMS gyroscope
- Disturbs PID feedback control
- Drone falls from sky

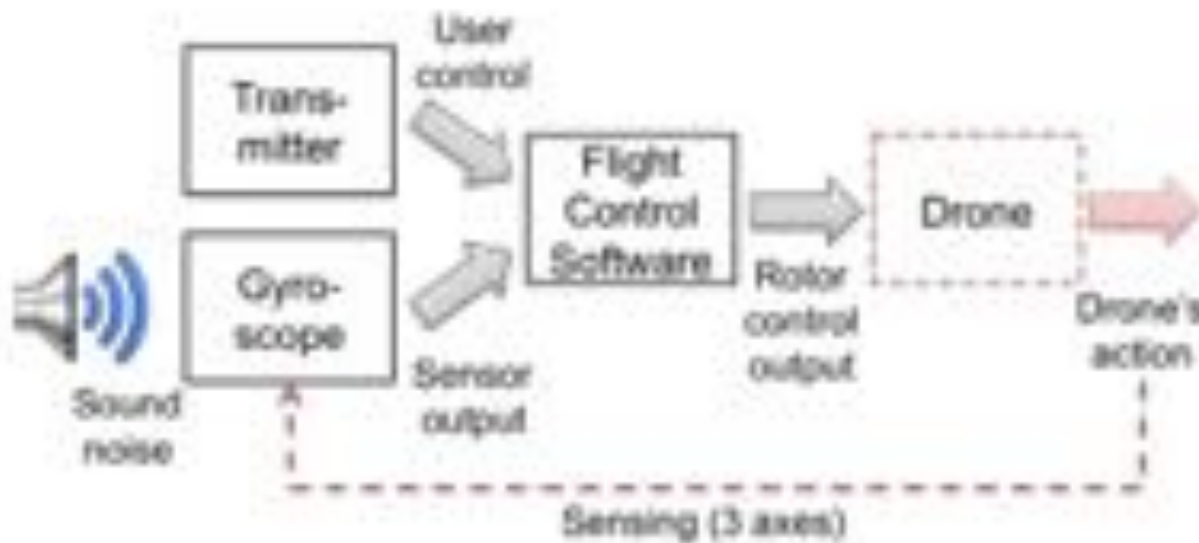


Figure 8: Propagation of the effect of sound noise

[Son et al., USENIX Security' 15]

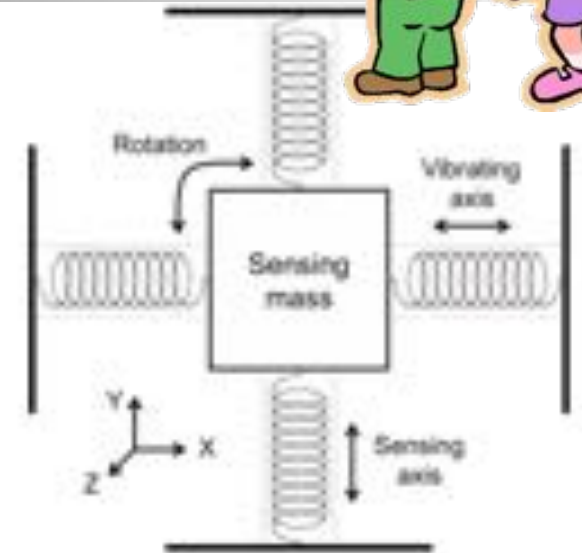


Figure 2: Concept of MEMS gyroscope structure for one axis

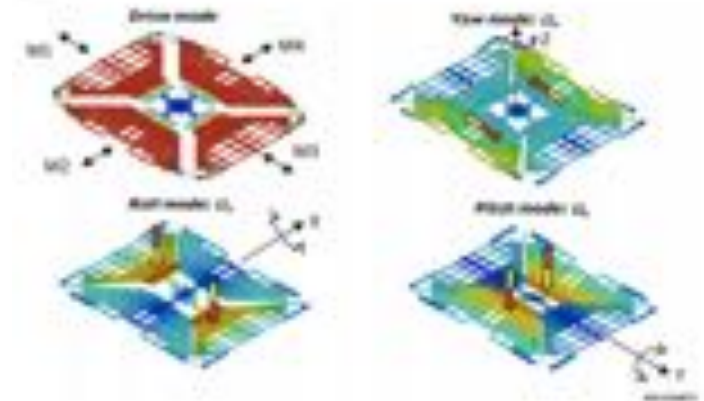
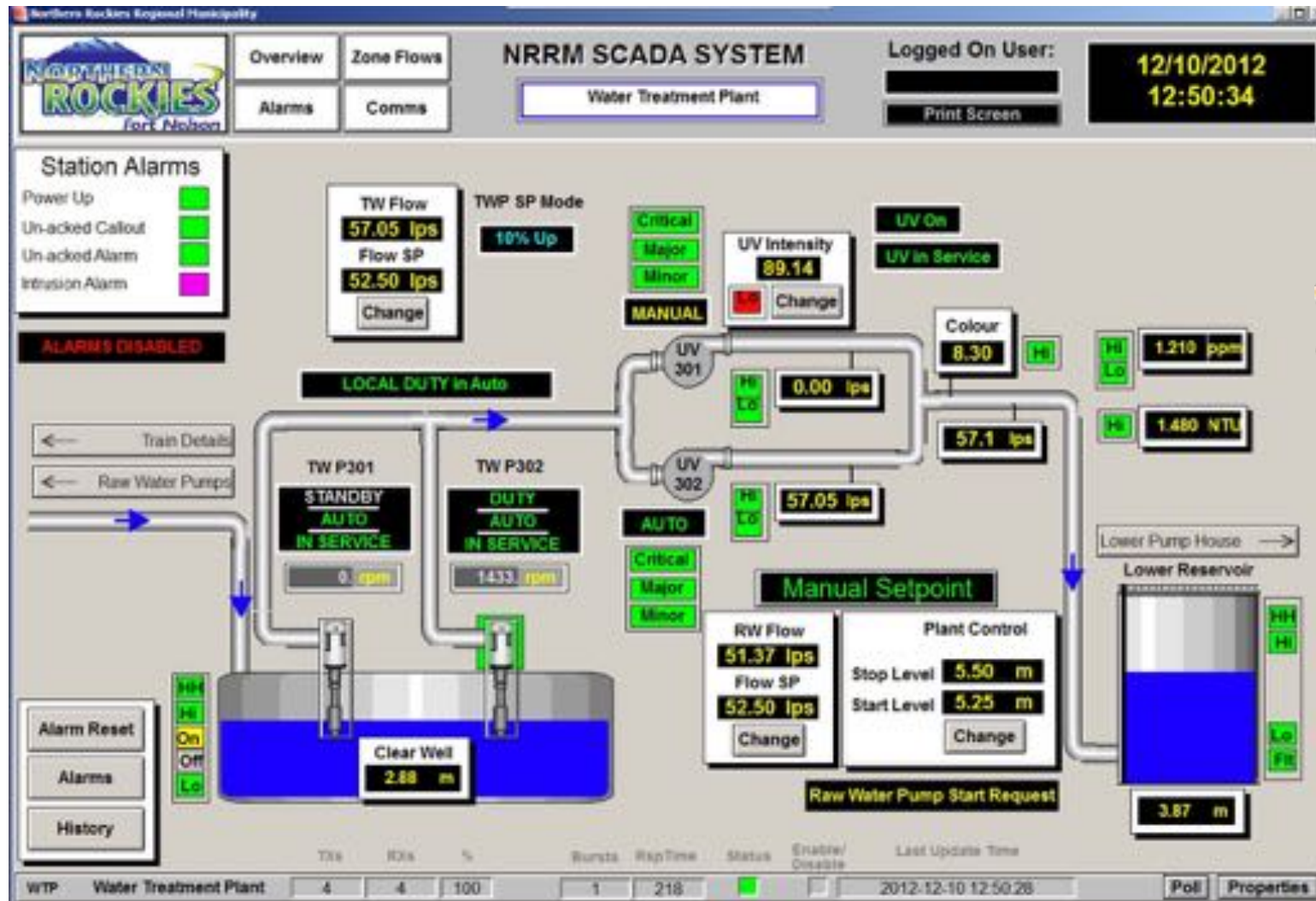


Figure 3: Operation of a three-axis MEMS gyroscope [10] (the X-, Y-, and Z-axes are defined as the pitch, roll, and yaw, respectively.)

Sensors: Water Treatment Plant

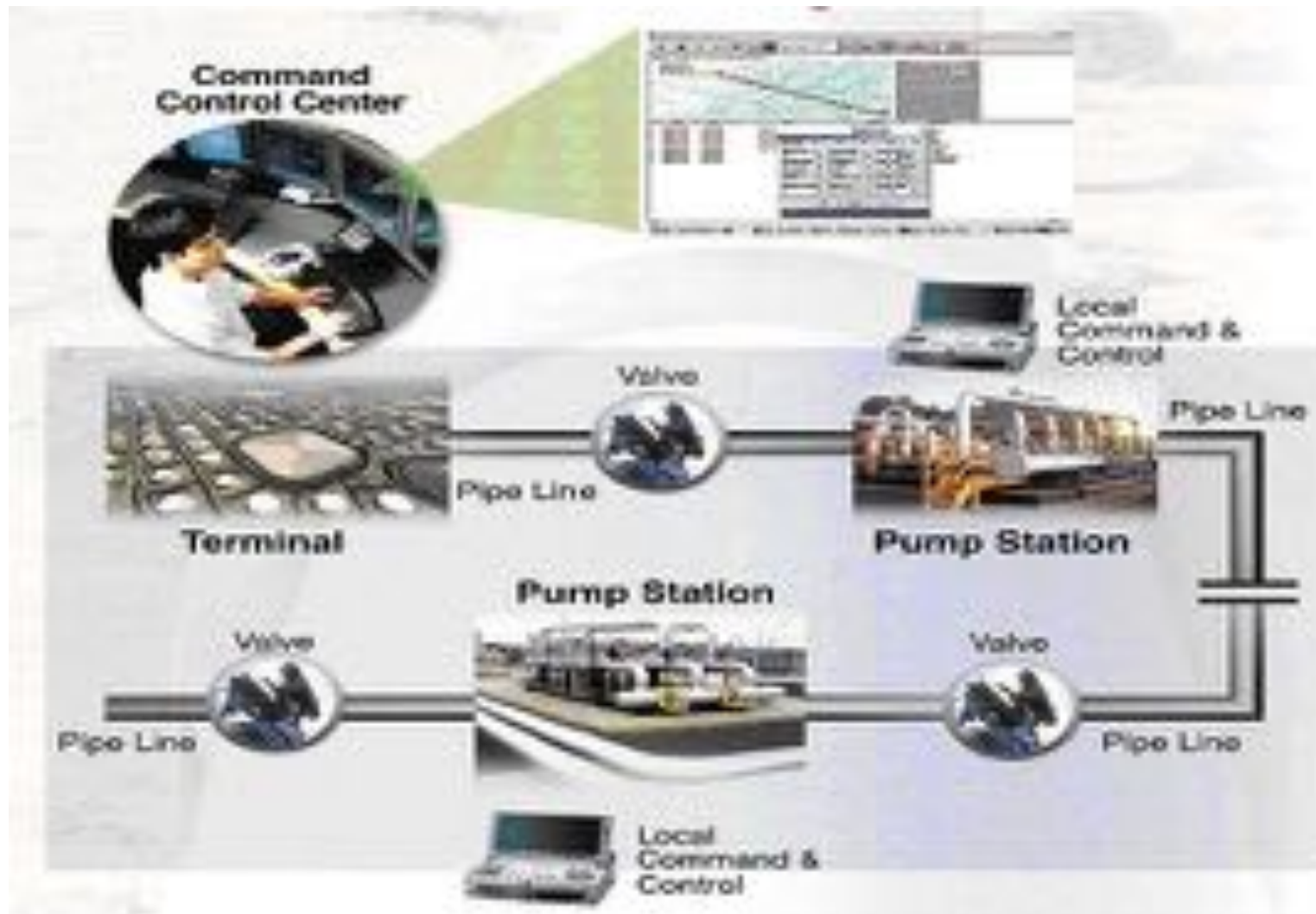


Sensors: Dams



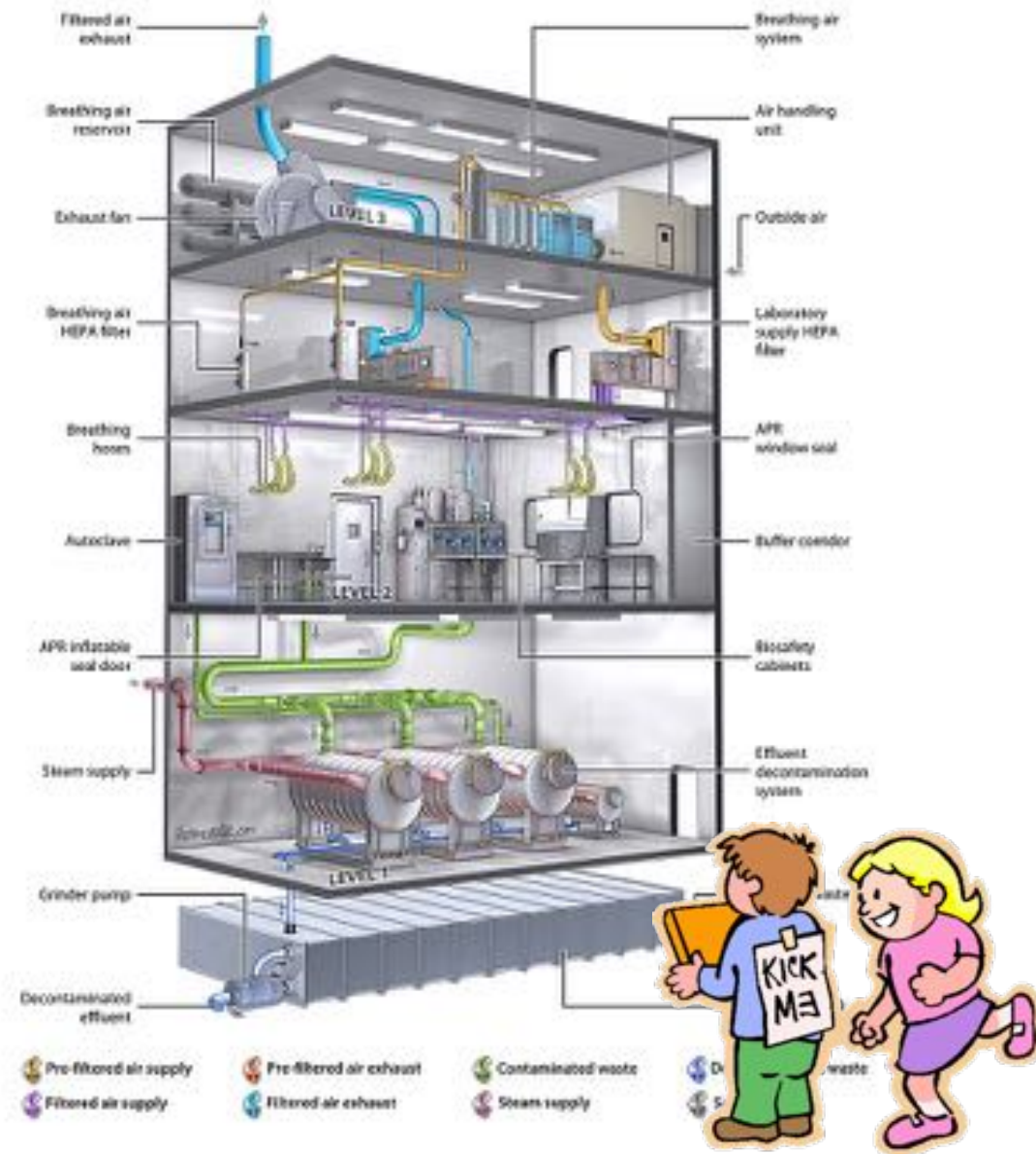
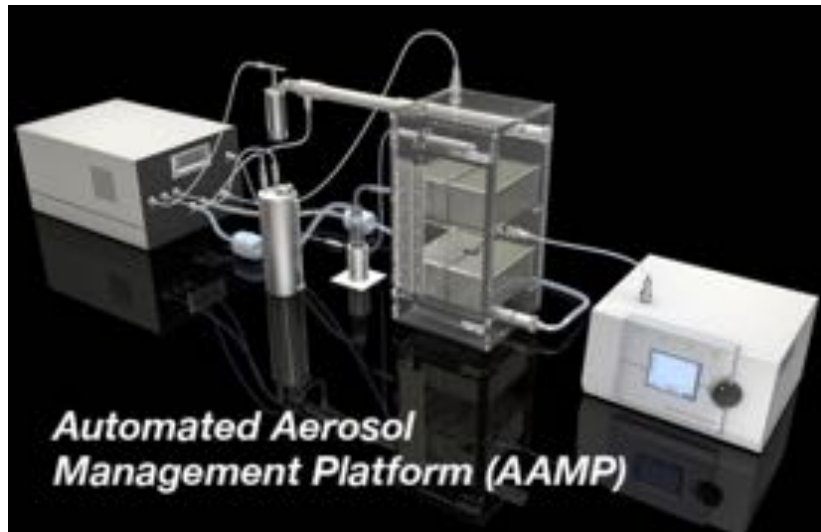
http://www.mpe.ca/project_experience/projects.php?view=28

Sensors: Oil Pipelines



<http://www.modcon-systems.com/applications/pipelines/pipeline-scada-security/>

Sensors: BSL-4 Negative Pressure HVAC



IAEA sensors for treaty compliance



Nuclear inspectors must learn to trust their colleagues, but during their training they must learn not to trust others...you never know who might be siphoning off nuclear material to build a bomb or sell on the black market....



**Don't Trust
Your Sensors.
Verify!**

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
- Culture gap
 - Security specialists often focus on technical **controls**
 - Safety specialists often focus on **risk management**
 - Trustworthy medical device software requires **both**
- Emerging research: Analog Cybersecurity
 - **Trust your sensors? Trust, but verify!**

