



Medical Device Security



Kevin Fu

Associate Professor
Computer Science & Engineering
University of Michigan

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



Disclosures/Background

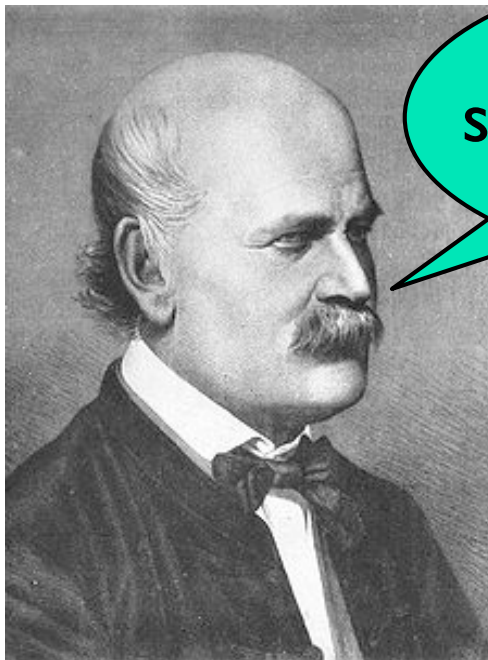
- Co-founder, Virta Labs, Inc.
- Security & Privacy Research Group @ Michigan
- Director, Archimedes Center for Medical Device Security
- Security Advisor to Samsung Strategy & Innovation Ctr
- Consultant to MicroCHIPS Biotech
- Fmr. visiting scientist, U.S. Food and Drug Administration
- Recent research support from NSF, HHS, SRC, DARPA, MARCO, UL, Medtronic, Philips, Siemens, WelchAllyn

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



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.

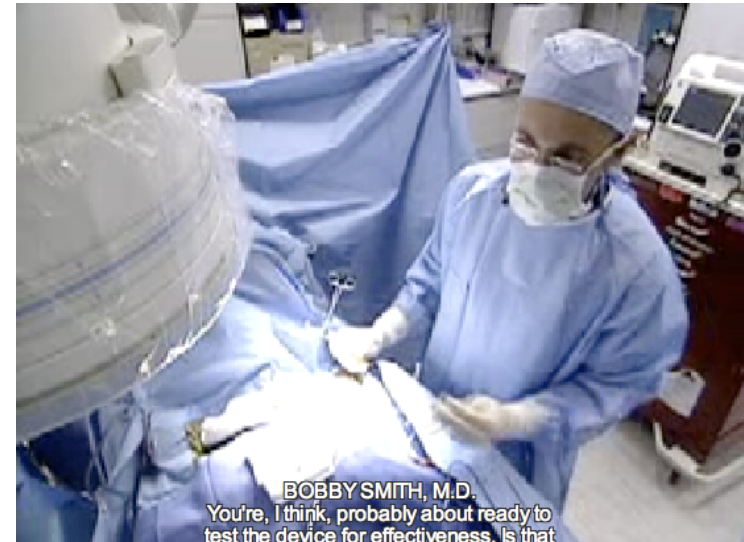
Dr. Charles Meigs
1792-1869



Photo by Kevin Fu @ Medtronic museum

Implantation of Defibrillator

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



Photos: Medtronic; Video: or-live.com

Privacy

Implanting
physician

Diagnosis

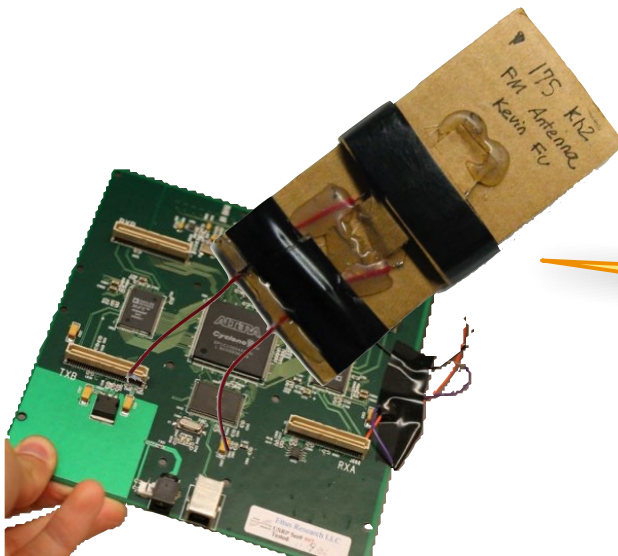
Hospital

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

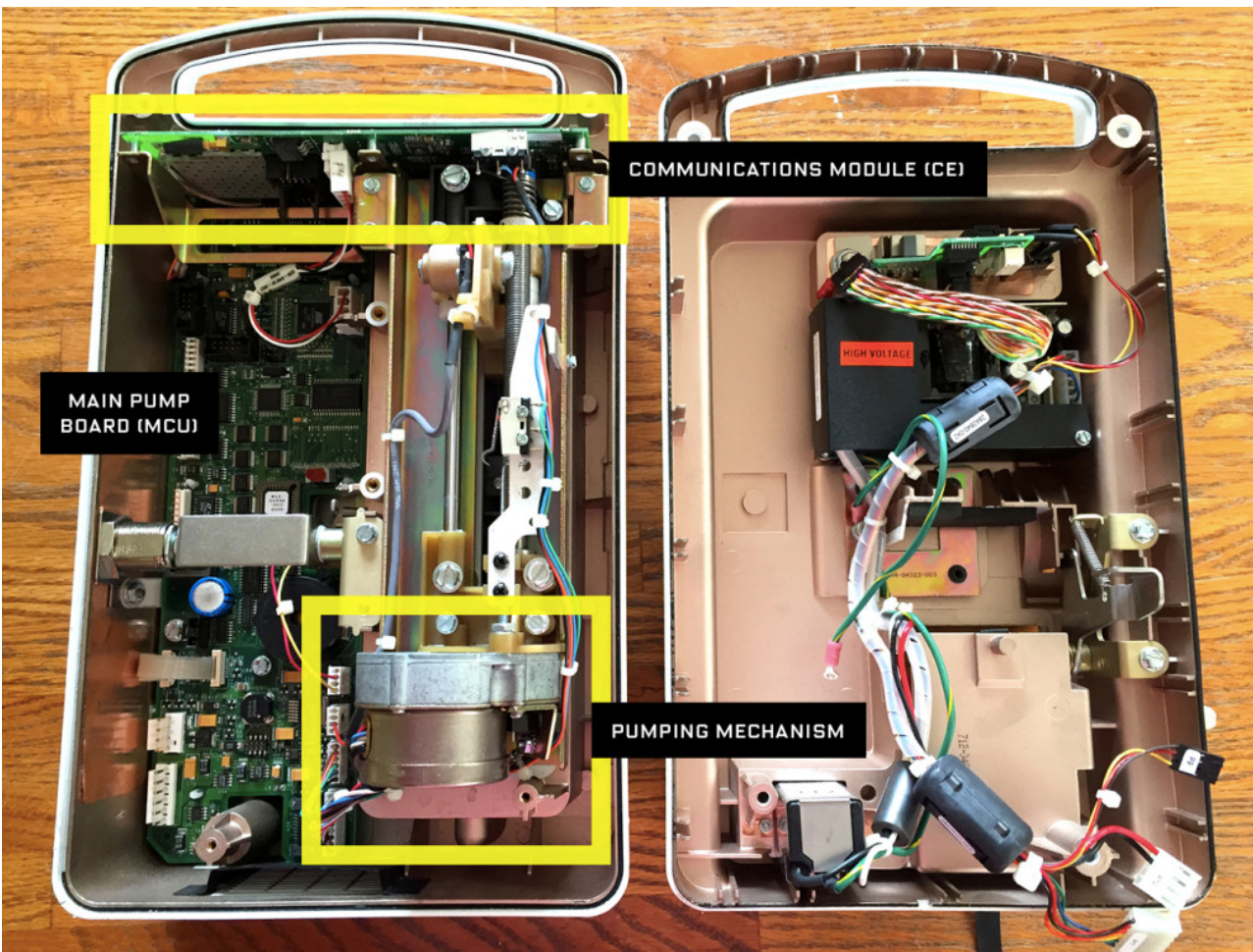
**(Risks mitigated
a long time ago)**



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

First FDA Cybersec Product Advisory

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



Photos: Wired

First FDA Cybersec Product Advisory

- 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

First FDA Cybersec Product Advisory

- Hospira Infusion Pump Vulnerabilities
[Billy Rios and more]

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

LifeCare PCA3 and PCA5 Infusion 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 security 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 exploit these vulnerabilities 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.

Wireless
keys stored
unencrypted, accessible
via telnet/FTP!

Root
shell on port
23!

Hard-
coded local
accounts!

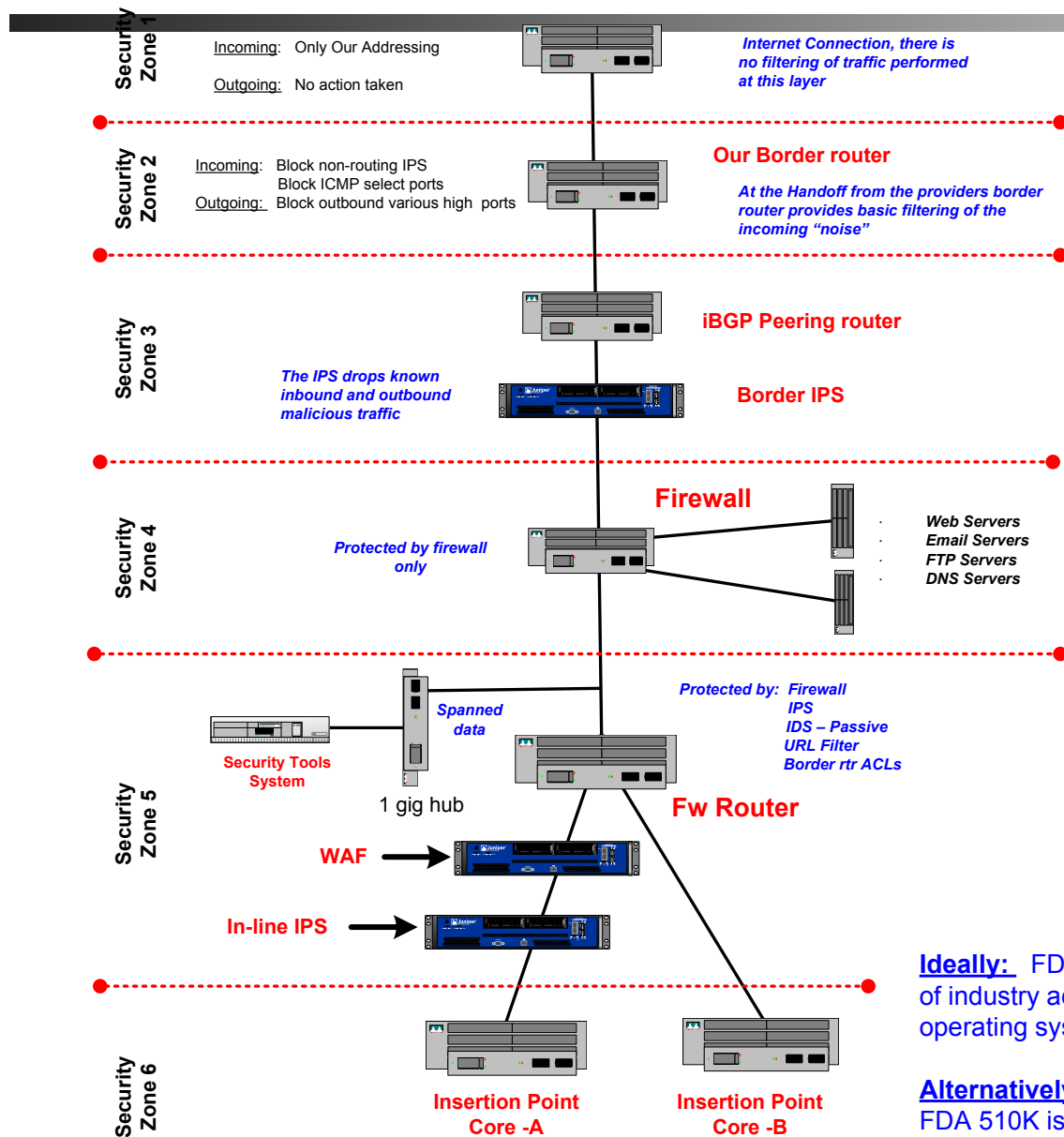


Photos: Wired

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

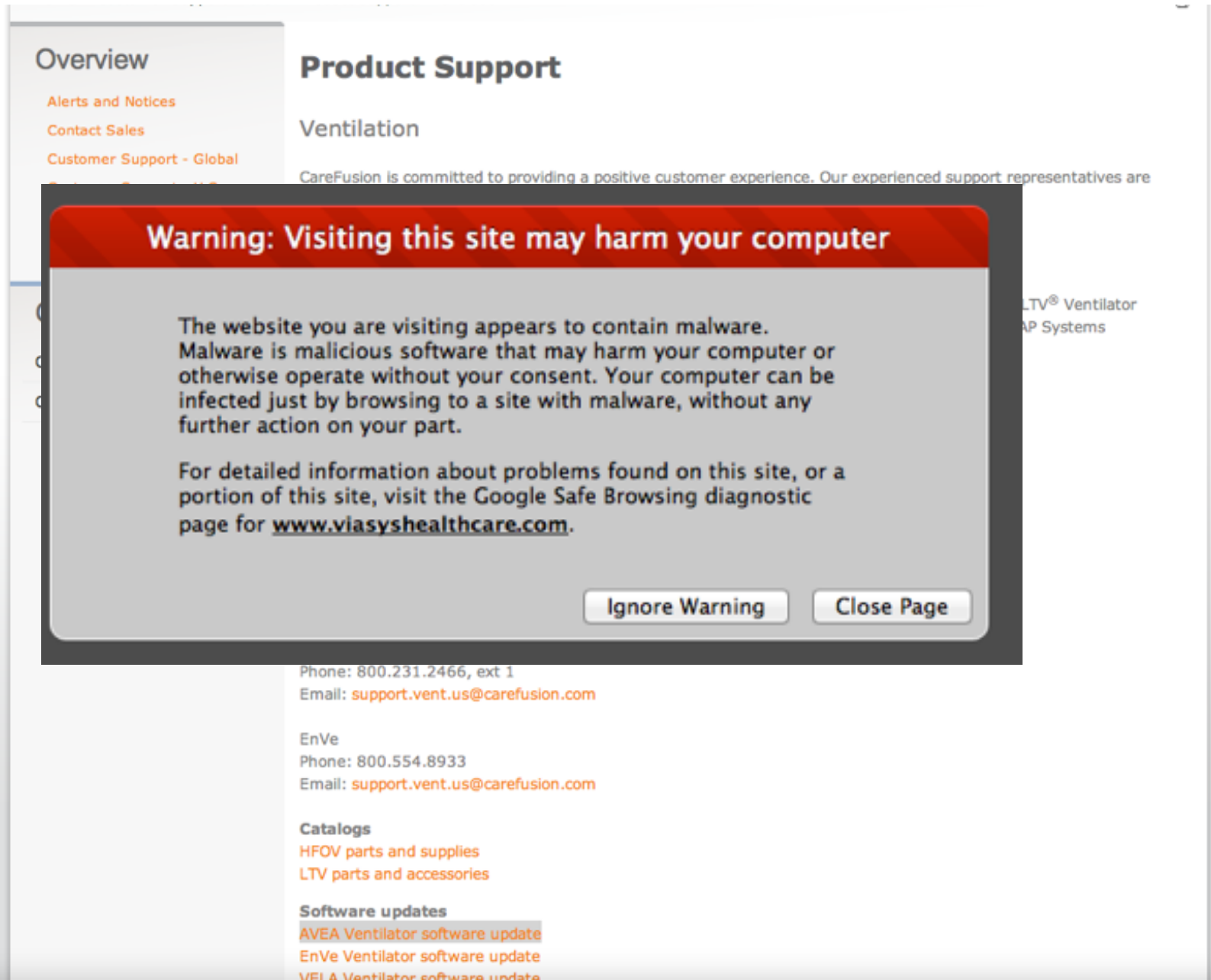
Alternatively: The FDA issues a clear statement to the community that FDA 510K is not jeopardized by permitting Anti-Virus or Operating System patching to the supporting systems associated with a certified medical device

Shoot P0wn Foot w/ Software Update



[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 [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



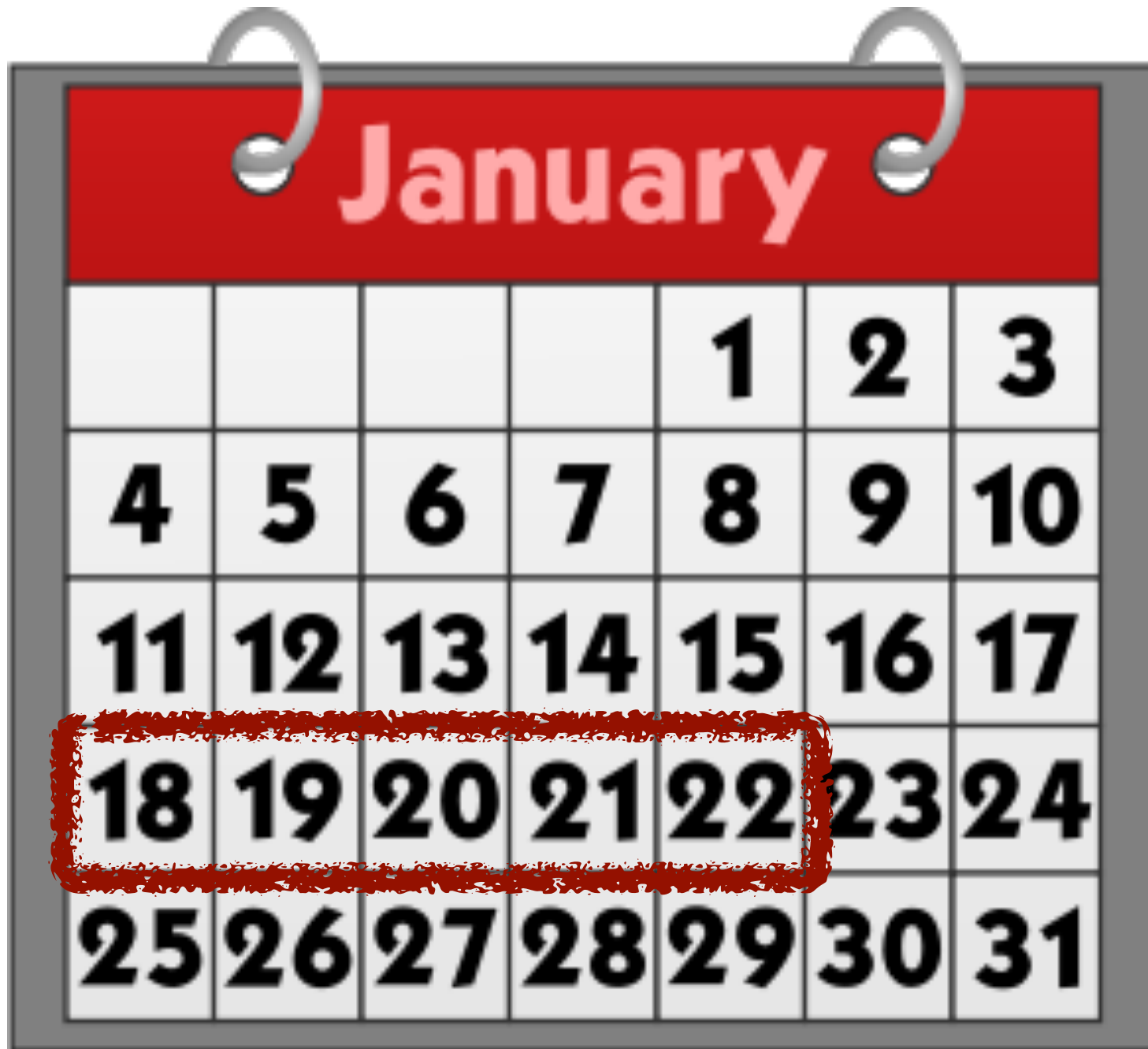
EnVe Ventilator software update
VELA Ventilator software update

Factory-installed malware?

More common than you might think

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

Last Week: Medical Device Security





Monday Jan 18, 2015 in Australia

Royal Melbourne Hospital attacked by damaging computer virus

January 18, 2016

Julia Medew

Health Editor

THE  AGE
Victoria

A virus has attacked the computer system of one of Melbourne's largest hospital networks, causing chaos for staff and patients who may face delays as a result.

Staff at Melbourne Health - the network which runs the Royal Melbourne Hospital - are urgently trying to repair damage to its IT system after a virus infected Windows XP computers.

An email sent to staff today said the virus had hit Melbourne Health's pathology department, causing staff to manually process specimens such as blood, tissue and urine samples instead of computers aiding the registration, testing and entry of results.

HAPPY
DAYS

Wednesday Jan 20, 2015 in Texas

THE DAILY TRIBUNE

Virus hits TRMC computers

By MARCIA DAVIS Managing editor

TRMC CEO John Allen said the hospital experienced a network issue that was revealed about 7:30 p.m. Friday, Jan. 15.

TRMC public information officer Shannon Norfleet said a computer ransomware virus encrypted files on several of the TRMC database servers within the health system, which affects the TRMC access to the computer files.



Thursday Jan 21, 2015

Advisory (ICSA-15-337-02)

Hospira Multiple Products Buffer Overflow Vulnerability

Original release date: January 21, 2016

- Hospira manufactures networkable drug infusion pumps
- Remotely accessible buffer overflow via port 5000/TCP
- Difficulty: Low skill attacker





Friday Jan 22, 2015 in Michigan

Flint hospital confirms 'cyber attack,' Anonymous threatens action over water crisis



on January 21, 2016 at 9:43 PM, updated January 22, 2016 at 9:59 AM

By [Gary Ridley | gridley@mlive.com](mailto:gridley@mlive.com)

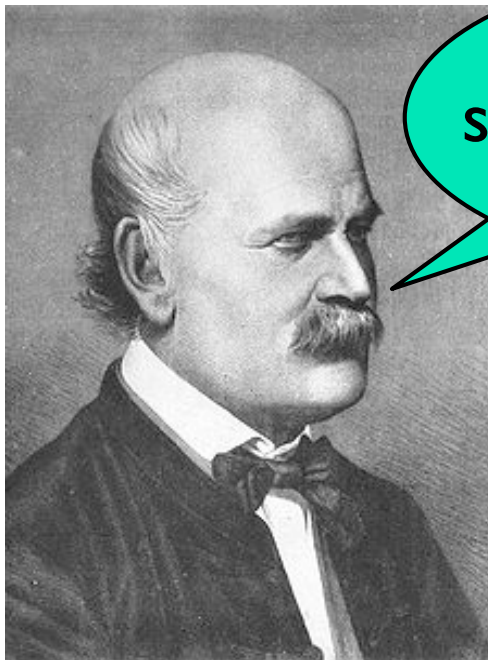
FLINT, MI – Hurley Medical Center has confirmed it was the victim of a "cyber attack" a day after hacktivists threatened action over Flint's water crisis.

The hospital confirmed the attack Thursday, Jan. 21, but few details were released.

"Hurley Medical Center has IT systems in place, which aid in detecting a virus or cyber attack," hospital spokeswoman Ilene Cantor said. "As such, all policies and protocols were followed in relation to the most-recent cyber attack on our system. Patient care was not compromised and we are closely monitoring all systems to ensure IT security is consistently maintained."

Semmelweis to Software Sepsis

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



Physicians
should wash their
hands.

Doctors
are gentlemen and
therefore their hands are
always clean.

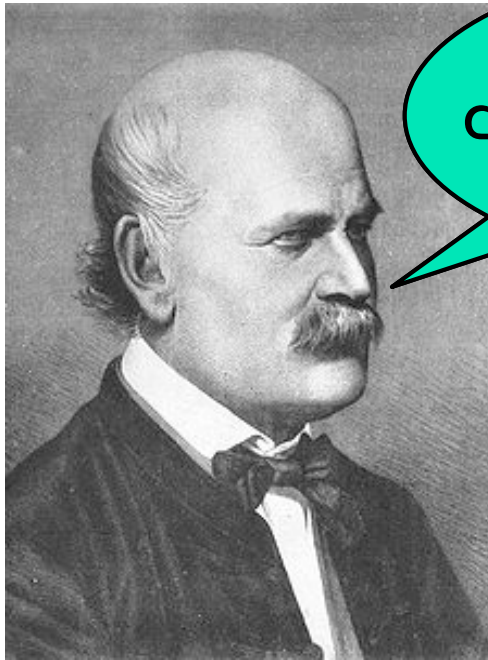


Dr. Ignaz Semmelweis
1818-1865

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.

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





120VAC 15A MAX

PowerGuard

Virta Labs
VIRTA LABORATORIES, INC.
HW1.0

Virta Labs

Cybersecurity: A Foreseeable Risk

- Biggest risk at the moment:
 - ~~Hackers breaking into medical devices~~
 - Wide-scale **unavailability** of patient care
 - **Integrity** of medical sensors
- Gaps
 - Don't interrupt clinical workflow
 - Many security specialists focus on technical controls
 - Many safety specialists focus on risk management
 - Trustworthy medical device software requires both





Archimedes Center for Medical Device Security



2013

Collaboration: Industry, Academia, Government,
Clinicians, Health Care Providers



2014



2015

Learn more at...

secure-medicine.org

Members



Medtronic

SIEMENS

WelchAllyn®