Medical Device Security: Hack or Hype?

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 re$earch $upport 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.

MedSec Beginning in 2006…

In 2006…

Invited talk.
Computer system security and medical devices, U.S. Food and Drug Administration Center for Devices and Radiological Health (FDA CDRH), October 2006.

A Heart Device Is Found Vulnerable to Hacker Attacks

By BARNABY J. FEDER MARCH 12, 2008

The New York Times

Hack: 2008

Of Fact, Fiction and Cheney's Defibrillator

By GINA KOLATA
Published: October 27, 2013

The New York Times

Hype: 2013

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Daniel Halperin[1] University of Washington
Thomas S. Heydt-Benjamin[2] University of Massachusetts Amherst
Benjamin Ransford[2] University of Massachusetts Amherst
Shane S. Clark University of Massachusetts Amherst
Benessa Defend University of Massachusetts Amherst
Wil Morgan University of Massachusetts Amherst
Kevin Fu, PhD[2] University of Massachusetts Amherst
Tadayoshi Kohno, PhD[1] University of Washington
William H. Maisel, MD, MPH[3] BIDMC and Harvard Medical School

Abstract—Our study analyzes the security and privacy properties of an implantable cardioverter defibrillator (ICD). Introduced to the U.S. market in 2003, this model of ICD includes pacemaker technology and is designed to communicate wirelessly with a nearby external programmer in the 175 kHz frequency range. After partially reverse-engineering the ICD's communications protocol with an oscilloscope and a software radio, we implemented several software radio-based attacks that could compromise patient safety and patient privacy. Motivated by our desire to improve patient safety, and mindful of conventional trade-offs between security and power consumption for resource-constrained devices, we introduce three new zero-power defenses based on RF power harvesting. Two of these defenses are human-centric, bringing patients into the loop with respect to the security and privacy of their implantable medical devices (IMDs). Our contributions provide a scientific baseline for understanding the potential security and privacy risks of current and future IMDs, and introduce human-perceptible and zero-power mitigation techniques that address those risks. To the best of our knowledge, this paper is the first in our community to use general-purpose software radios to analyze and attack previously unknown radio communications protocols.

I. Introduction

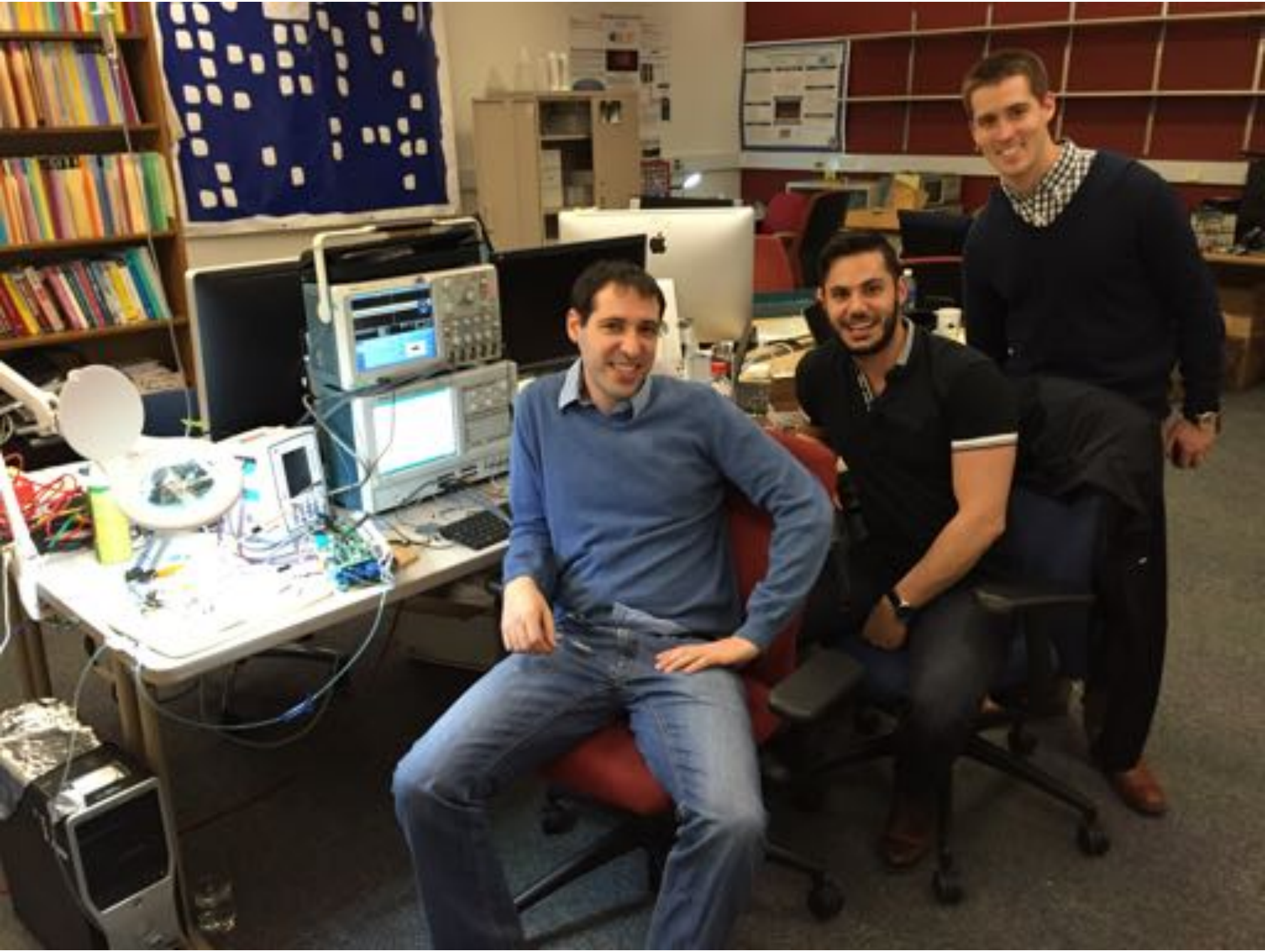
Wirelessly reprogrammable implantable medical devices (IMDs) such as pacemakers, implantable cardioverter defibrillators (ICDs), neurostimulators, and implantable drug pumps use embedded computers and radios to monitor chronic disorders and treat patients with automatic therapies. For instance, an ICD that senses a rapid heartbeat can administer an electrical shock to restore a normal heart rhythm, then later report this event to a health care practitioner who uses a commercial device programmer[1] with wireless capabilities to extract data from the ICD or modify its settings without surgery. Between 1990 and 2002, over 2.6 million pacemakers and ICDs were implanted in patients in the United States [19]; clinical trials have shown that these devices significantly improve survival rates in certain populations [18]. Other research has discussed potential security and privacy risks of IMDs [11, 10], but we are unaware of any rigorous public investigation into the observable characteristics of a real commercial device. Without such a study, it is impossible for the research community to assess or address the security and privacy properties of past, current, and future devices. We address that gap in this paper and, based on our findings, propose and implement several prototype attack-mitigation techniques.

Our investigation was motivated by an interdisciplinary study of medical device safety and security, and relied on a diverse team of area specialists. Team members from the security and privacy community have formal training in computer science, computer engineering, and electrical engineering. One team member from the medical community is a practicing cardiologist with hundreds of pacemaker and implantable defibrillator patients and was past chairperson of the FDA's Circulatory System Medical Device Advisory Panel. Our technical contributions toward understanding and improving the security, privacy, and safety of these devices include: analyses, software radio-based methodologies, and human-perceptible and zero-power (battery free) defenses.

Overview of contributions. We assess the security and privacy properties of a common ICD and present attacks on privacy, integrity, and availability. We show that the ICD discloses sensitive information in the clear (unencrypted); we demonstrate a reprogramming attack that changes the operation of (and the information contained in) the ICD; and

[1] This reader should not confuse the term "device programmer" with a person who programs computers. The former is an external device that communicates with and adjusts the settings on an IMD.

This paper, copyright the IEEE, will appear in the proceedings of the 2008 IEEE Symposium on Security and Privacy. 1




1
2
scrub

Hack or Hype?

Was a defibrillator hacked?

Yes in 2007, but we did it in a lab without patients

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]

Patients are far safer with these implantable devices than without, even if there are security vulnerabilities.

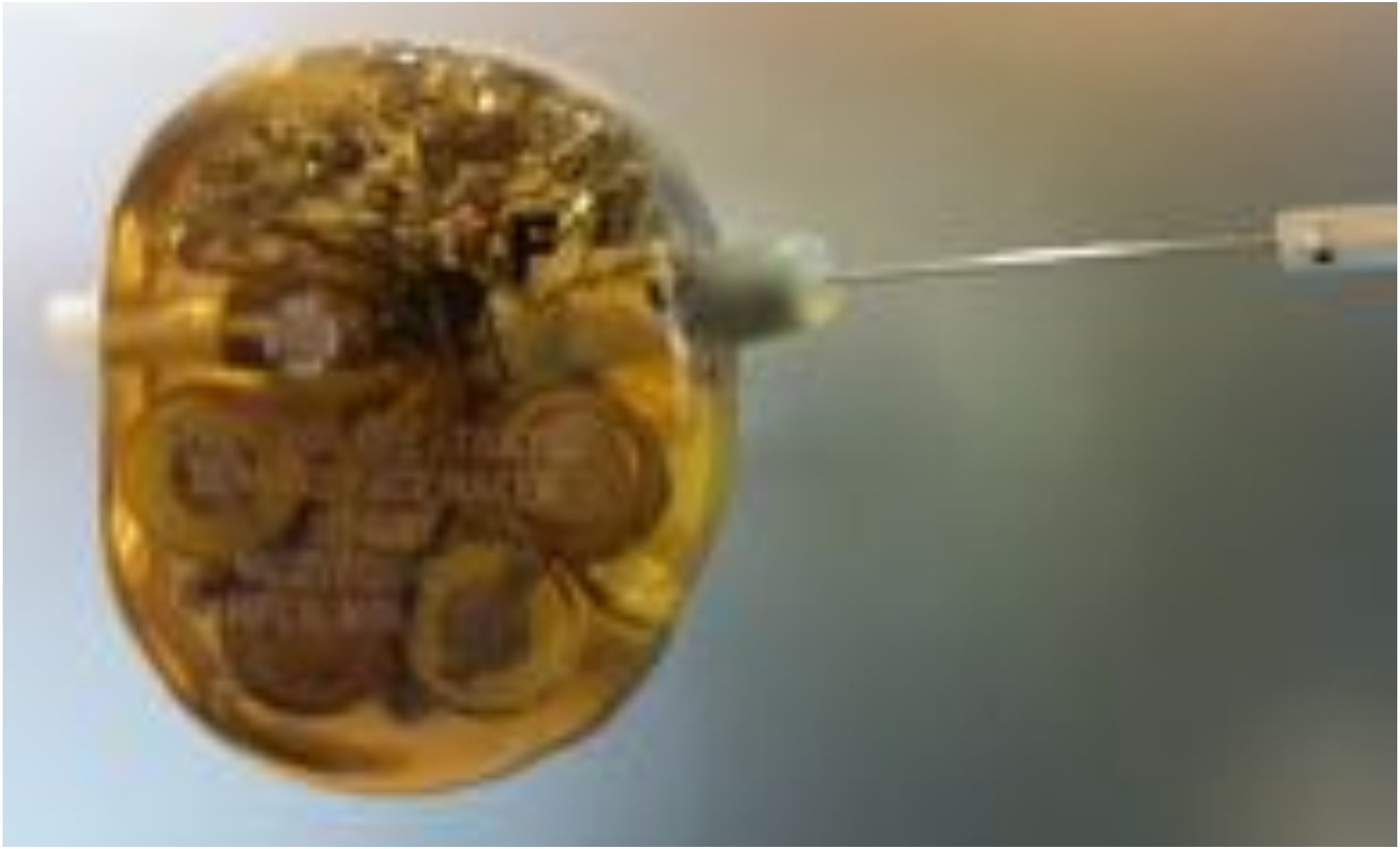


Photo by Kevin Fu @ Medtronic museum

Hack or Hype?

Darth Vader is an FDA regulated medical device

No, but Emperor Palpatine is first victim of hacking Vader's neuro-prosthetic arms.


You will remove these restraints and leave this crypto with the backdoor closed!
-Prof. Kevin Fu

Hack or Hype?

Medical device manufacturers are doing nothing about security?

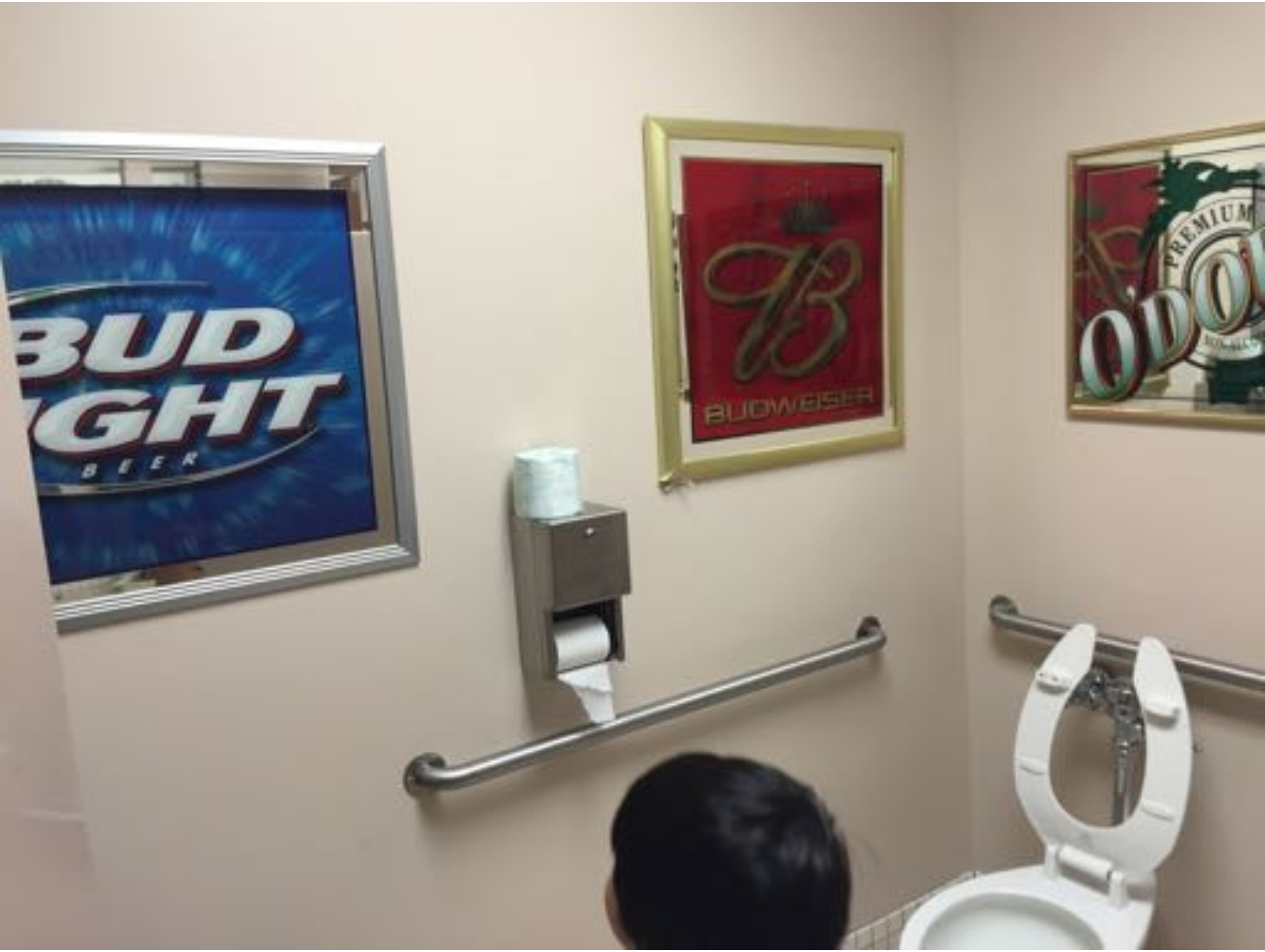
FALSE!

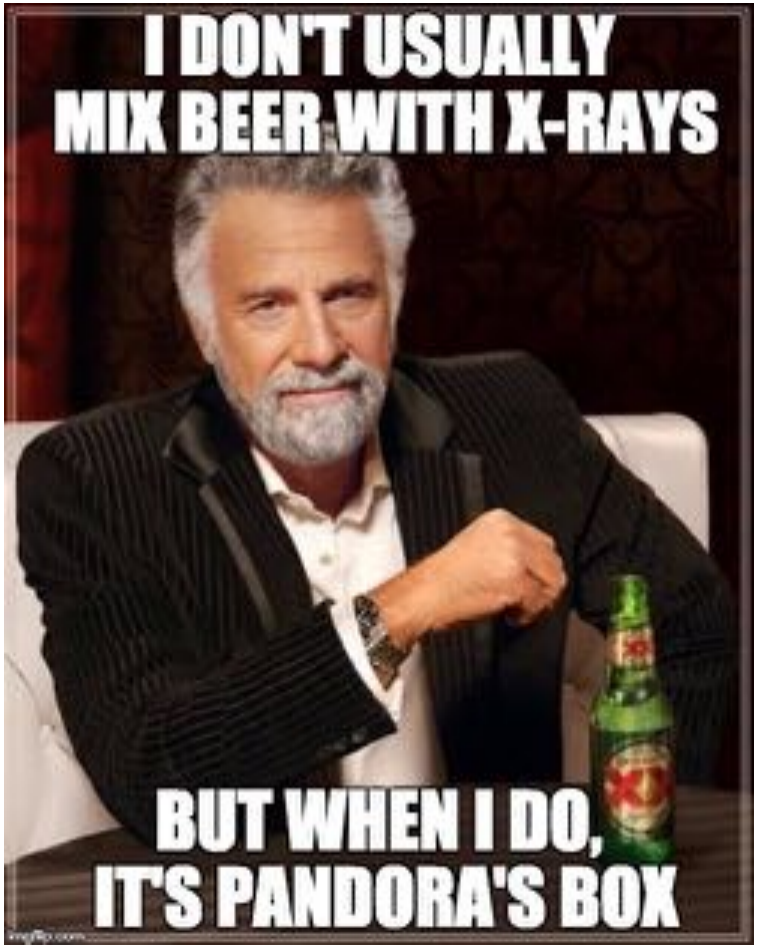

MEDICAL DEVICES SECURITY WORKSHOP
Kevin Fu and team from University of Michigan's Archimedes Center for Medical Device Security
Boulder Surgical Innovations Campus, Bldg #2
Pike/Evans Conference Room
Feb 11th & 12th - 9.00 AM to 5.00 PM
Medtronic

Hack or Hype?

Dental x-ray monitors serve beer ads

Actual beer mug from TROOPERS

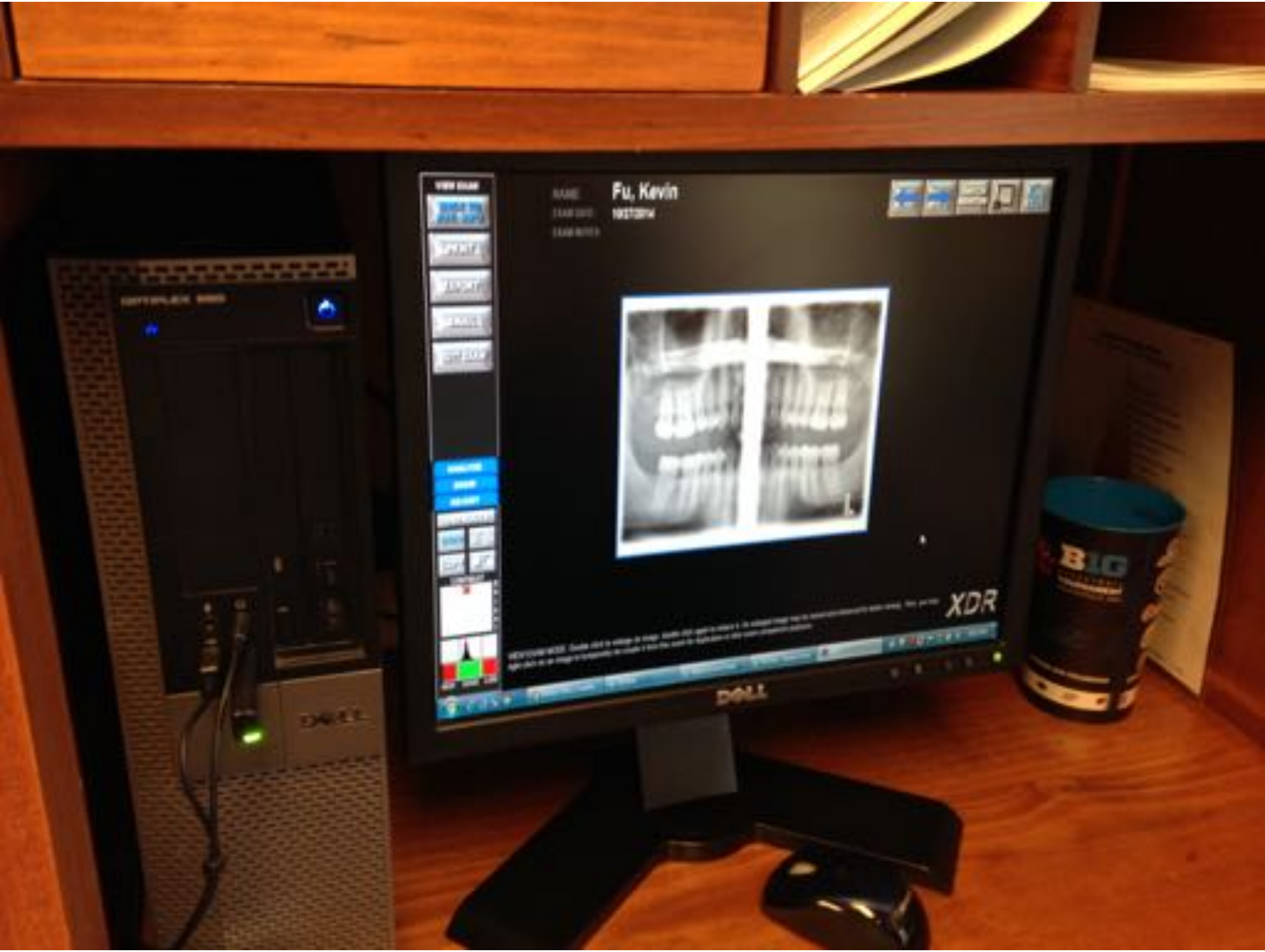

BUD
GHT
BEER
BUDWEISER
PREMIUM

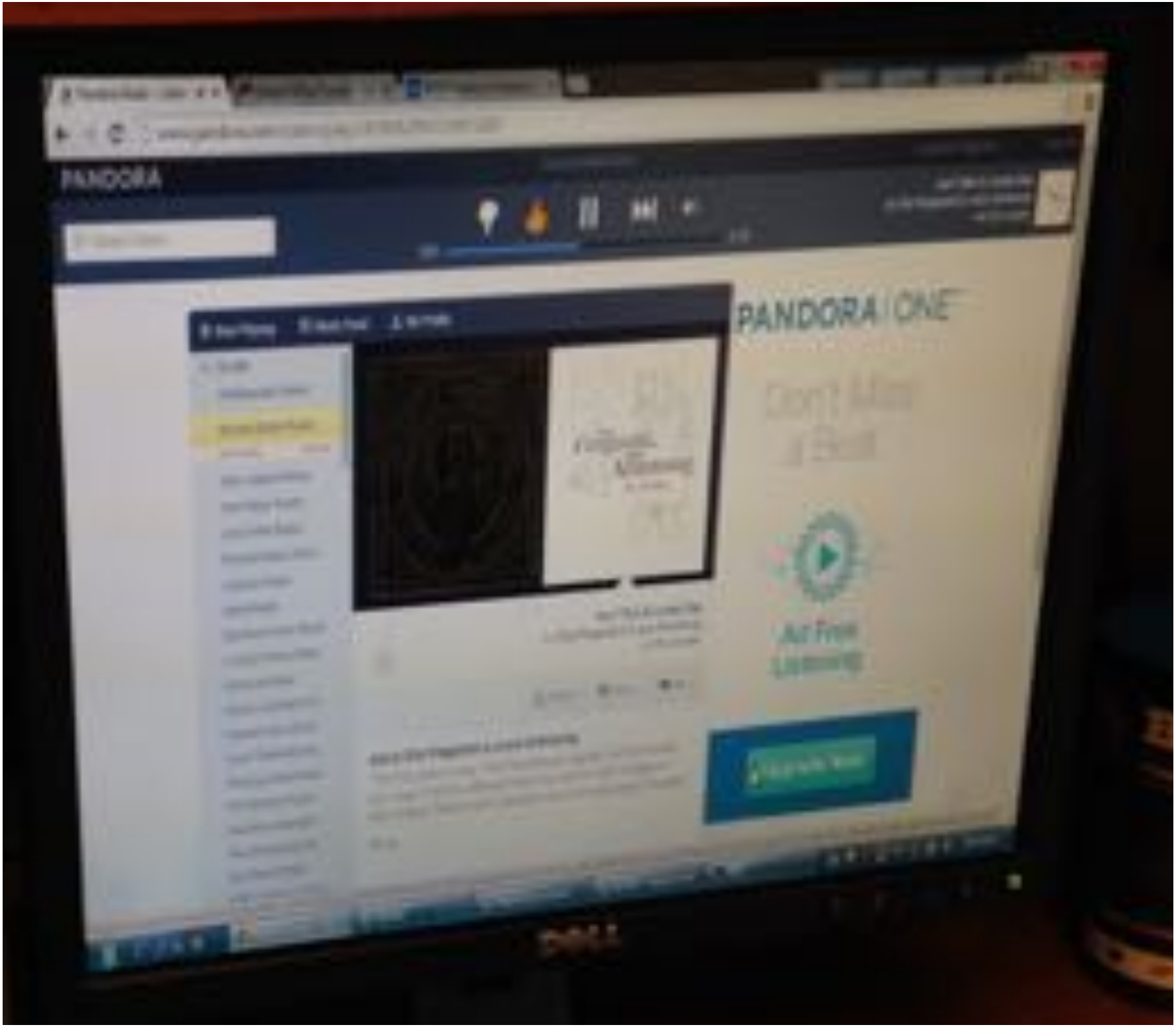


Hack or Hype?

Dental x-ray monitors serve beer ads

True! I saw Dos Equis.


Fu, Kevin
XDR
DELL
DELL


PANDORA
PANDORA | ONE
Ad Free
Listening

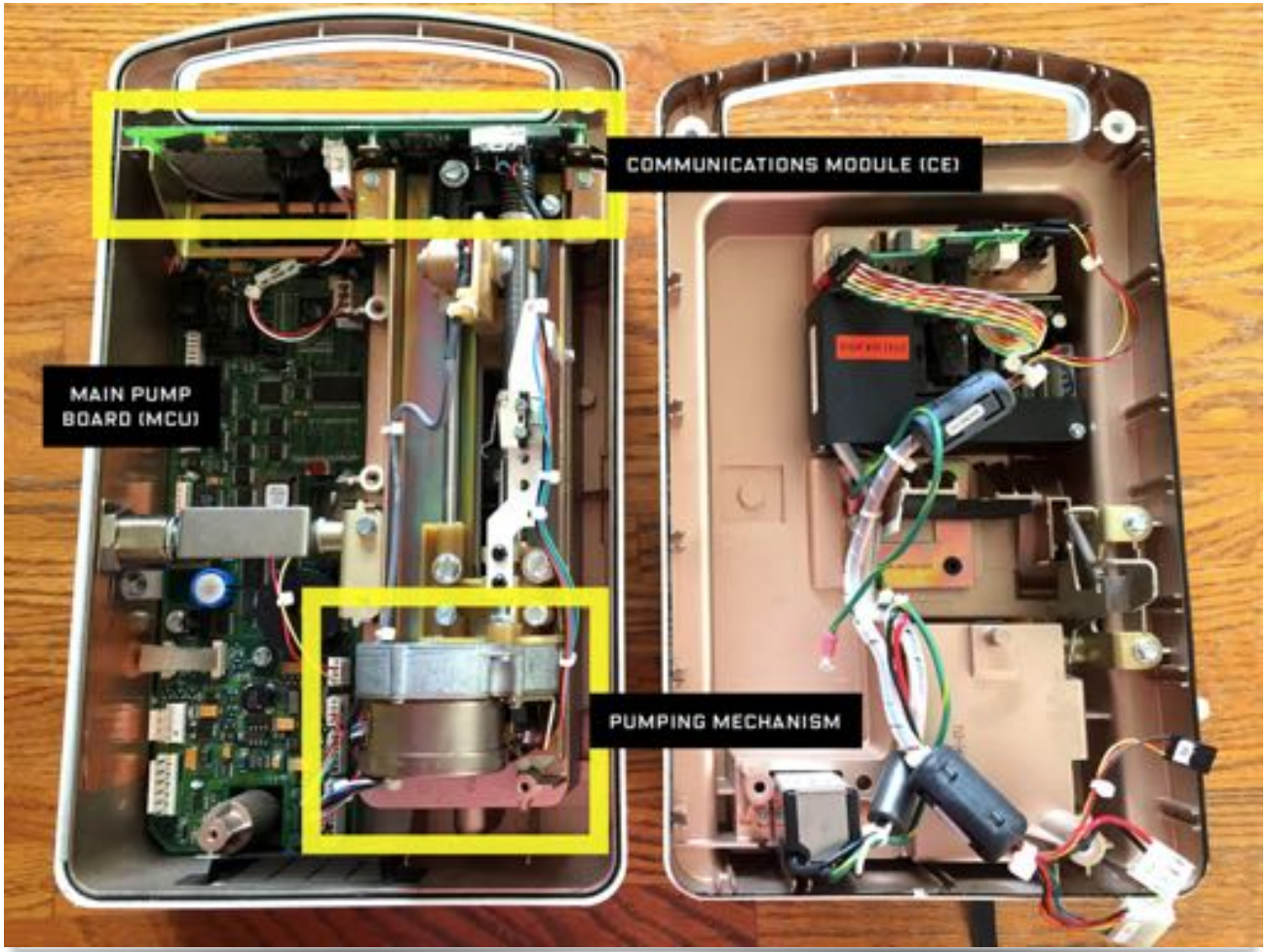
Hack or Hype?

Has FDA issued security warnings?

Yes, against an infusion pump

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 V abilities [Billy Rios and more

Wireless keys stored unencrypted, accessible via telnet/FTP!

U.S. Food and Drug Administratio
Protecting and Promoting *Your* Heal

LifeCare PCA3 and P
Pump Systems by Hospi
Safety Communication - Security
Vulnerabilities

[Posted 05/13/2015]

AUDIENCE:Pharmacy, Nursing, Risk

ISSUE: The FDA and Hospira have beco pira's LifeCare PCA3 and PCA5 Infusion Pump Systems. A sed information about these vulnerabilities, including software c uld allow an unauthorized user to interfere with the pump's func ed user with malicious intent could access the pump remotely and modify the vers, which could lead to over- or under-infusion of critical therapies. The FDA is not of any patient adverse events or unauthorized device access related to these vulnerabilities.

Root shell on port 23!

Hard-coded local accounts!

Photos: Wired

FDA Warns That Commonly Used Medical Device Can Be Hacked

More

00:00 CC SHARE

Hack or Hype?

FDA has a way to report security vulnerabilities

Half true, they are working on it

Colony forming units
Color Variation, Lens
Communication or transmission issue
Compatibility
Complete heart block
Component failing
Component incompatible
Component missing
Component or accessory incompatibility
Component(s), broken
Component(s), overheating of
Component(s), worn
Computer failure
Computer hardware error
Computer operating system issue
Computer software issue
Computer system security issue
Concentrate
Conductivity
Connection error
Connection issue
Connector pin failure


Plenary Panel:
Situational Awareness of
Current Activities in the Healthcare
Public Health Sector to Enhance
Medical Device Cybersecurity
January 21, 2016
Dr. Julian Goldman

FDA Cybersecurity Guidance

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

---

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

Life before FDA's security guidance document was schieße.

In 2016: Vulnerability Reporting!

Postmarket Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Document issued January 2016

Understanding MedSec Risks

⚠️ Vulnerabilities

🔪 Threats

→ 💩 Exploits → ☠️ Harm

🔨 Compensating Controls

👀 Continuous Measurement

Understanding MedSec Risks

⚠️ Vulnerabilities

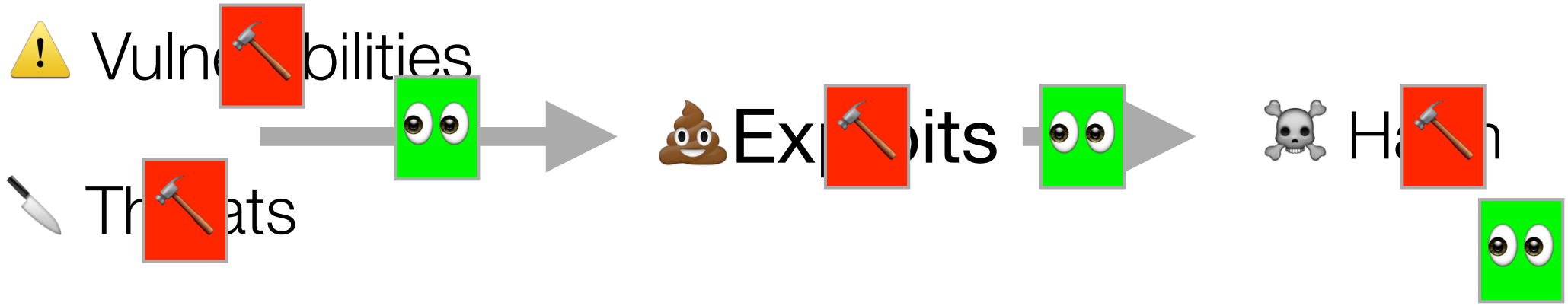
🔪 Threats

→ 💩 Exploits → ☠️ Harm

🔨 Compensating Controls

👀 Continuous Measurement

Understanding MedSec Risks



Compensating Controls

Continuous Measurement

Hack or Hype?

Hospitals have been disabled by malware?

Yes, many times

The New York Times

California: Hospital Pays Bitcoin Ransom to Hackers

By THE ASSOCIATED PRESS FEB. 17, 2016

Hollywood Presbyterian Medical Center paid a ransom in bitcoins equivalent to about $17,000 to hackers who infiltrated and disabled its computer network, the hospital's chief executive said Wednesday. It was in the hospital's best interest to pay the ransom of 40 bitcoins after the hacking that began Feb. 5, the C.E.O., Allen Stefanek said. The F.B.I. is investigating the attack, often called "ransomware," in which hackers encrypt a computer network's data to hold it hostage, providing a digital decryption key to unlock it for a price. "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Mr. Stefanek said. Bitcoins, an online currency, are hard to trace. The Los Angeles hospital network was operating fully again Monday, and patient care was not affected by the hacking, Mr. Stefanek said. Neither law enforcement officials nor the hospital gave any indication of who might have been behind the attack or whether there were any suspects.

February 17, 2016

I am writing to talk to you about the recent cyber incident which temporarily affected the operation of our enterprise-wide hospital information system.

It is important to note that this incident did not affect the delivery and quality of the excellent patient care you expect and receive from Hollywood Presbyterian Medical Center ("HPMC"). Patient care has not been compromised in any way. Further, we have no evidence at this time that any patient or employee information was subject to unauthorized access.

On the evening of February 5th, our staff noticed issues accessing the hospital's computer network. Our IT department began an immediate investigation and determined we had been subject to a malware attack. The malware locked access to certain computer systems and prevented us from sharing communications electronically. Law enforcement was immediately notified. Computer experts immediately began assisting us in determining the outside source of the issue and bringing our systems back online.

The reports of the hospital paying 9000 Bitcoins or $3.4 million are false. The amount of ransom requested was 40 Bitcoins, equivalent to approximately $17,000. The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this.

HPMC has restored its electronic medical record system ("EMR") on Monday, February 15th. All clinical

immediately began assisting us in determining the outside source of the issue and bringing our systems back online.

The reports of the hospital paying 9000 Bitcoins or $3.4 million are false. The amount of ransom requested was 40 Bitcoins, equivalent to approximately $17,000. The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this.

HPMC has restored its electronic medical record system ("EMR") on Monday, February 15th. All clinical operations are utilizing the EMR system. All systems currently in use were cleared of the malware and thoroughly tested. We continue to work with our team of experts to understand more about this event.

I am very proud of the dedication and hard work of our staff who have maintained the highest level of service, compassion and quality of care to our patients throughout this process. I am also thankful for the efforts of the technical staff as the EMR systems were restored, and their continued efforts as other systems are brought back online.

And of course, I want to thank our patients and community for their continued trust in Hollywood Presbyterian Medical Center.

Thank you,

Allen Stefanek, President & CEO
Hollywood Presbyterian Medical Center

Hackers who brought down Hollywood Presbyterian's computer system are demanding a huge ransom.

By: Christine O'Donnell

POSTED:FEB 12 2016 07:34PM PST
UPDATED:FEB 12 2016 07:34PM PST

Ransom payments in Hollywood

Blackmailing hospitals into paying ransom has also been reported in other parts of the world, most notably in the US state of California where a Hollywood hospital paid about $17,000 (15,000 euros) in the digital currency bitcoins to hackers this month.

"The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Hollywood Presbyterian Medical Center's President Allen Stefanek said in a statement.

CYBER ATTACK

Hackers hold German hospital data hostage

Several hospitals in Germany have come under attack by ransomware, a type of virus that locks files and demands cash to free data it maliciously encrypted. It will take weeks until all systems are up and running again.

The incident happened over two weeks ago, but the hospital's website still advises patients to call them or send a fax - the email system is still not up and running. Malware has brought the hospital's computer system to a halt.

Monday Jan 18, 2016 in Australia

Royal Melbourne Hospital attacked by damaging computer virus

THE AGE
Victoria

January 18, 2016

Julia Medew
Health Editor

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.

19 JANUARY 2016

News Category: Media releases

Melbourne Health is managing a computer virus which infected its computer network.

While the virus has been disruptive to the organisation, due to the tireless work of staff we have been able to minimise this disruption to our patients and ensure patient safety has been maintained.

Computers running on most of our systems are now clear of the virus and IT staff are working to restore the remaining Windows XP computers as quickly as possible.

As of 10am this morning, many programs affected by the virus are up and running including pathology and pharmacy.

"restore the remaining Windows XP computers… pathology and pharmacy."

Wednesday Jan 20, 2016 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, 2016

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

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Friday Jan 22, 2016 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

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."

Hack or Hype?

2,000 x-rays were stolen to somewhere in China

True, likely selling.


Dr. John Halamka, CIO of Beth
Israel Deaconess Medical Center in Boston
geekdoctor.blogspot.com

Hack or Hype?

AngryBirds took down a hospital

No, but an authentic binary led to spambot

Hack or Hype?

A hospital downgraded from SSH to telnet for compliance.

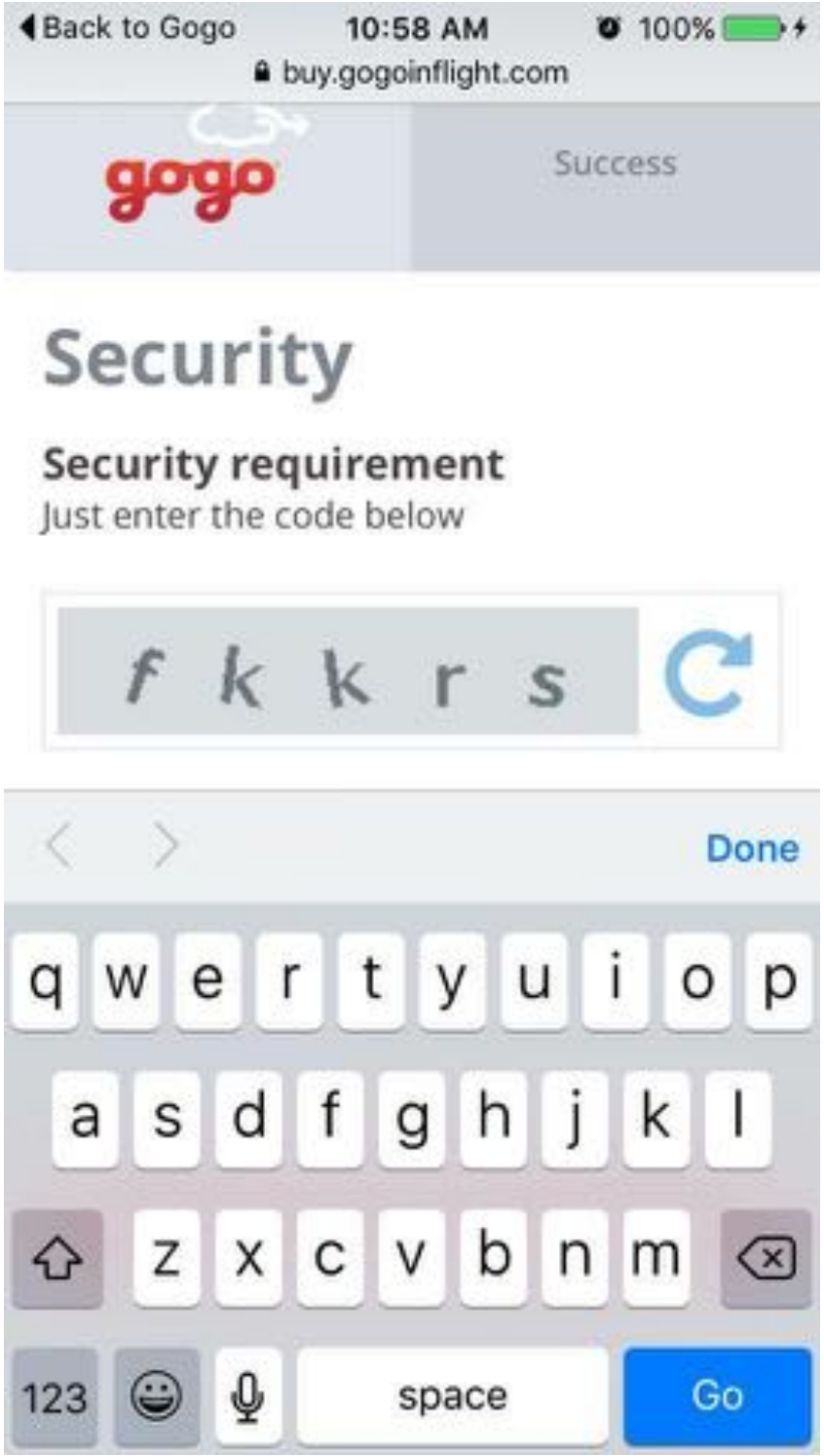
Sadly, true.

Hack or Hype?

Vulnerability scanning knocks over medical devices?

True if tools used haphazardly

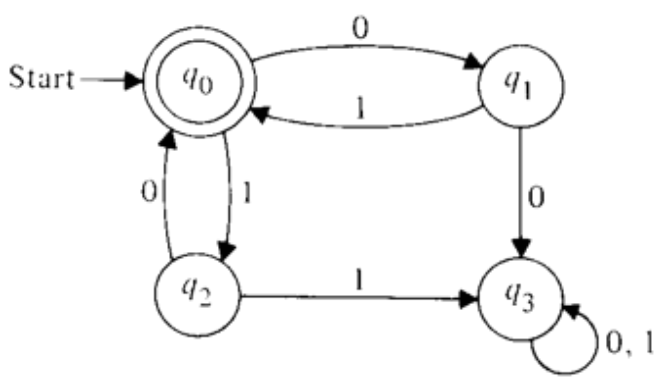
Ways Forward: Usable Security

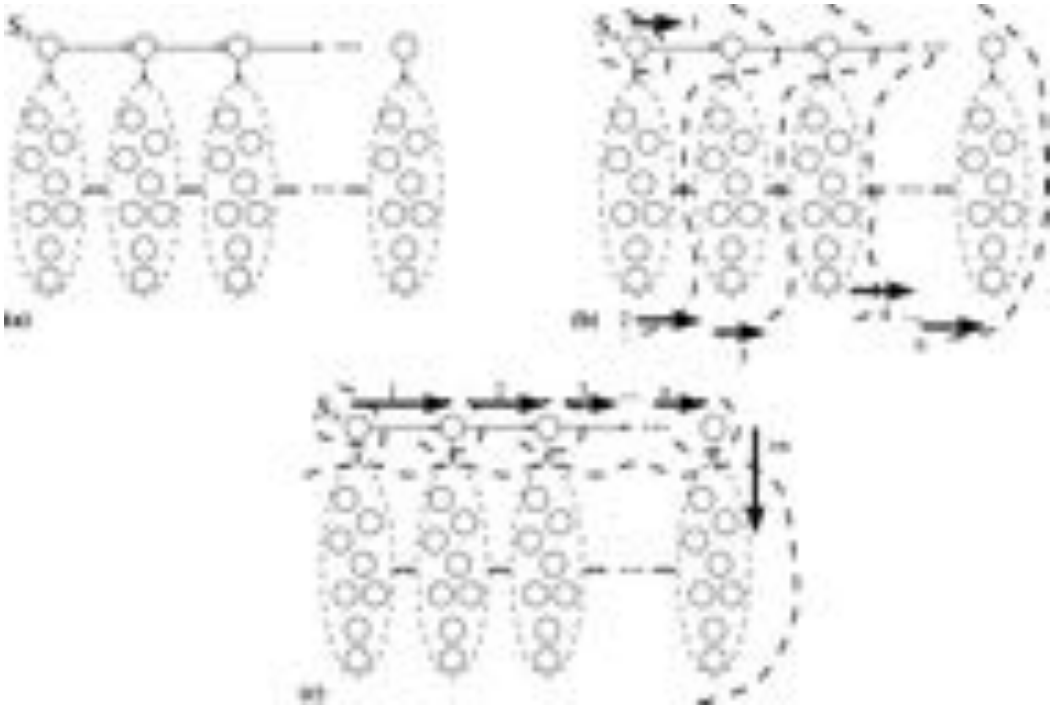


Intuition

Embedded

General-purpose



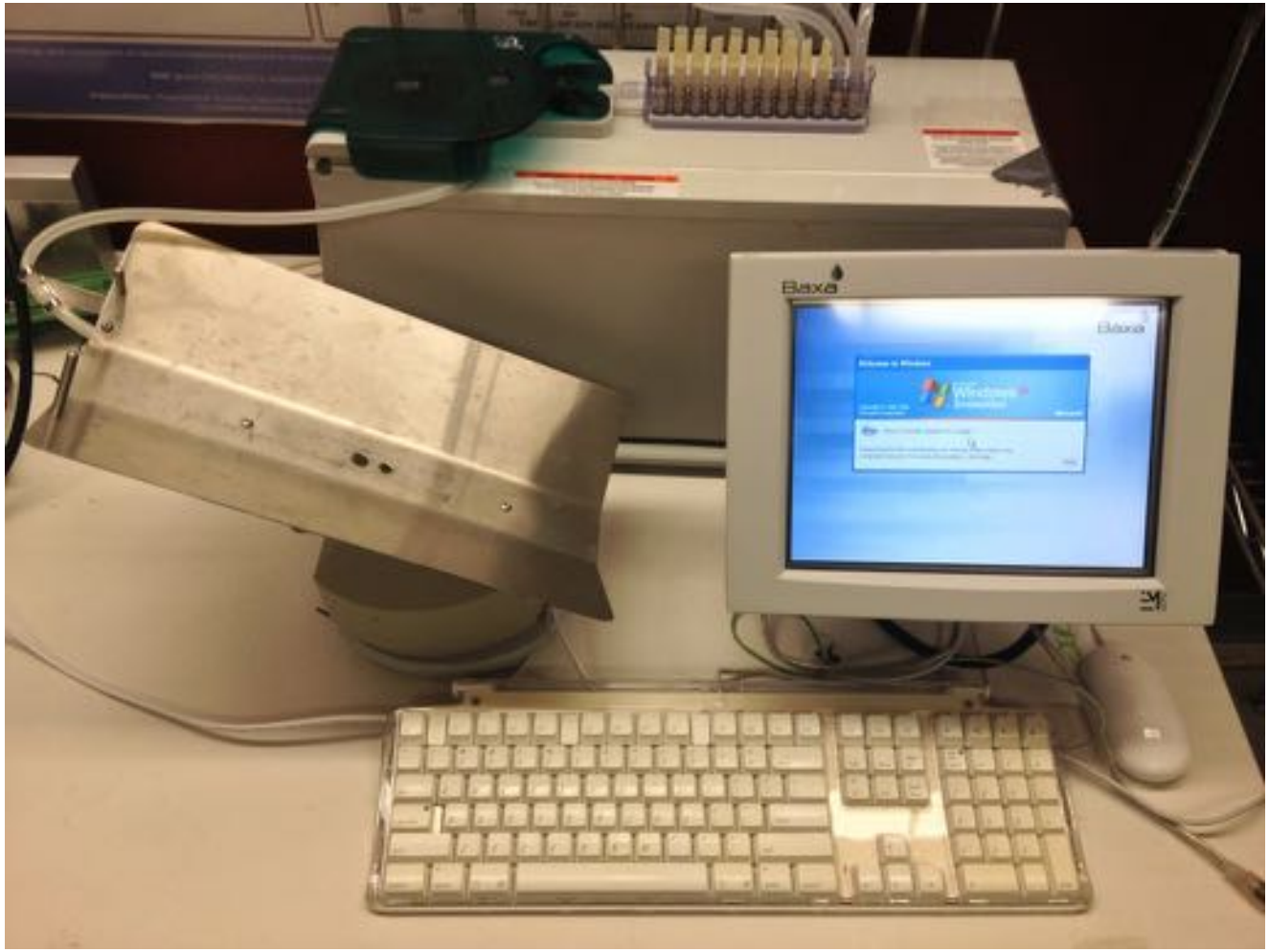


Devices Tested

Device	Configuration
Baxa ExactaMix 2400 compounder	WinXP Embedded, Via 664 MHz , 512 MB RAM
Schweitzer SEL3354 substation computer	WinXP Embedded, Athlon 2600+, 2 GB RAM

Pharmaceutical Compounder

- Mixes solutions, verifies output
- Flushes inputs
- Idles




VIRTA LABORATORIES
UNKNOWN MALWARE

Conficker Coffee

A maliciously delicious single varietal from the Sulawesi region of Indonesia and roasted to full city++, sure to keep you up while cleaning out Conficker from your cath labs. Virta security analytics to keep you alert.

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

Want to Learn More?

- Are you a security consultant?
- Are you a manufacturer?
- Are you a clinician?

Archimedes Center for Medical Device Security

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

2013

2014

2015

Members

Learn more at…

secure-medicine.org


MEDSEC
SECURITY RESEARCH
Follow me on Twitter @DrKevinFu
WHAT'S MISSING??

Coming Up Later: Marie Moe