On the Technical Debt of Medical Device Security

Kevin Fu, Associate Professor, University of Michigan EECS
kevinfu@umich.edu
https://web.eecs.umich.edu/∼kevinfu/

September 13, 2015

Introduction

This document provides background for my NAE FOE talk on "Interdisciplinary Security: Medical Devices."

Cybersecurity shortfalls in medical devices trace to decisions made during early requirements engineering and design. The industry is now paying the cybersecurity technical debt for the shortsightedness.

Complexity breeds insecurity. In the last few decades, medical devices have evolved from simple analog components to complex digital systems containing an amalgam of software, circuits, and advanced power sources that are more difficult to validate and verify. Whereas a classic stethoscope depended on well understood analog components, modern devices such as linear accelerators, pacemakers, drug infusion pumps, and patient monitors depend critically on computer technology. Computer networking, wireless communication, wireless power, the Internet, and a host of other engineering innovations combined with electronic health records and re-engineering of clinical workflow have enabled innovative therapeutics and diagnostics, but at the cost of technical debt for information security and privacy (known as *cybersecurity*).

When a medical device is compromised, its behavior becomes unpredictable. The device may deliver incorrect diagnostic information to clinicians as a result of damage to device integrity, may become unavailable to deliver patient care during repair, and in extreme cases may contribute to patient harm. Lack of security introduces an unconventional dimension of risk to safety and effectiveness: intentional harm.

Much cybersecurity risk is attributable to legacy medical devices depending on Windows XP and other unmaintainable operating systems that no longer receive security patches. Proprietary embedded systems are no less vulnerable. Design-time complexity, not hackers, is the root cause of many cybersecurity problems. Complexity increases the *attack surface*, the points where an adversary may gain a foothold into a computer system. Hackers represent the messengers or collectors of cybersecurity technical debt by uncovering the implications of the flaws baked in from early engineering choices.

Abridged History of Medical Device Security

There's a rich history [5] of trustworthy medical device software.[1] The classic and eye-opening Therac-25 study discusses how a linear accelerator caused a number of injuries and deaths by massive radiation overdoses in the late 1980s and early 1990s. While project mismanagement, complacency, and overconfidence in unrealistic probabilities played a role, the most interesting root cause was the adoption of poorly designed software rather than well understood analog components to safely control the radiation delivery [11].

Research in medical device security began with an interdisciplinary paper on the security of an implantable cardiac defibrillator [8]. The paper took several years of effort because of the interdisciplinary nature of the problem, and the clinical challenges such as attending live surgery to fully understand the threat model. The paper demonstrates that it is possible to wirelessly disable the life saving shocks and then induce ventricular fibrillation (a deadly heart rhythm). Contrary to the popular press, the research actually advises that patients are far safer accepting devices than not because patients are already predisposed to medical risk. The paper suggested the engineering principle that a secure medical device should not run an operation that causes a medical device to enter a known hazardous state (ventricular fibrillation) with a known recovery mechanism, if the software is not guaranteed to run the recovery mechanism (defibrillation). The paper includes a number of defensive approaches primarily centered on the concept of zero-power security where the external entity must provide wireless power such that the implant can protect the availability of its precious battery. The device has not been sold for several years, and the manufacturer now trains its engineers on security engineering.

After a lull for several years, the hacker community began to replicate academic experiments. Barnaby Jack famously replicated our pacemaker/defibrillator experiment in a manner more appealing to the general public. Although formal peer-reviewed proceedings were rare, the hackers gave captivating talks and demonstrations that attracted attention to the subject. The hacker community began to find new security flaws in medical devices such as insulin pumps and infusion pumps (e.g., demonstrations by Billy Rios, Barnaby Jack, Jay Radcliffe, Scott Erven, and others).

To promote deeper intellectual inquiry into medical device security, the author created the Open Medical Device Research Library (OMDRL) to share hard-to-find implants with security researchers. Unfortunately, the demand did not justify the high cost of biohazard decontamination, and computer science staff were uncomfortable with managing biohazard facilities. Thus the library was short lived. However, researchers from MIT did engage with the OMDRL to invent a novel RF jamming protocol that blocks legacy implanted

[1] blog.secure-medicine.org

cardiac devices from transmitting insecure “plaintext” messages and overlays an encrypted version [6].

In 2015, a couple days after the National Highway Traffic Safety Administration issued the first recall of an automobile solely because of a cybersecurity risk[2], Hospira became the first company to receive an FDA safety communication[3] as a singular result of a cybersecurity risk. While not legally a recall, the FDA notice was pragmatically a recall in that FDA strongly discouraged health care facilities from purchasing a particular infusion pump because of a cybersecurity vulnerability that could lead to patient harm via hacking to over-infuse or under-infuse drugs.

On the Horizon

The bleeding edge developments include new FDA pre-market guidance on cybersecurity[4] and the first FDA advisory to cease purchasing an infusion pump because of a cybersecurity risk.

FDA reviewers now expect to see a technical cybersecurity risk analysis in all applications for pre-market clearance to sell medical devices in the United States. FDA is expected to release a post-market guidance document on coordinated vulnerability disclosure, incident reporting, and continuous surveillance of emerging cybersecurity risks. This document is more complicated because of the workflow that involves a number of unusual bedfellows ranging from the vulnerability research community to the Department of Homeland Security to the U.S. Computer Emergency Response Team.

The Association for the Advancement of Medical Instrumentation (AAMI) sets the major standards that affect medical device safety. The AAMI medical device security working group consists of both healthcare providers and medical device engineers who have written Technical Information Report (TIR) 57. This document currently under ballet provides much needed advice to engineers on how to reason methodically about cybersecurity across the product development lifecycle of a medical device.

[2] http://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html

[3] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm

[4] http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

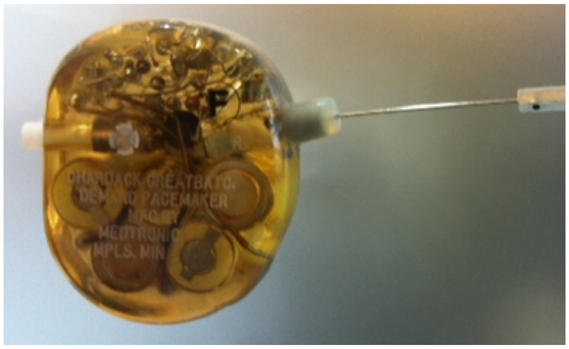


Figure 1: *Pacemaker before wireless control. A needle was inserted thru the patient's skin to twist a dial that controls the heart rate. Photo copyright Kevin Fu, taken in Medtronic's Mounds View, MN museum.*

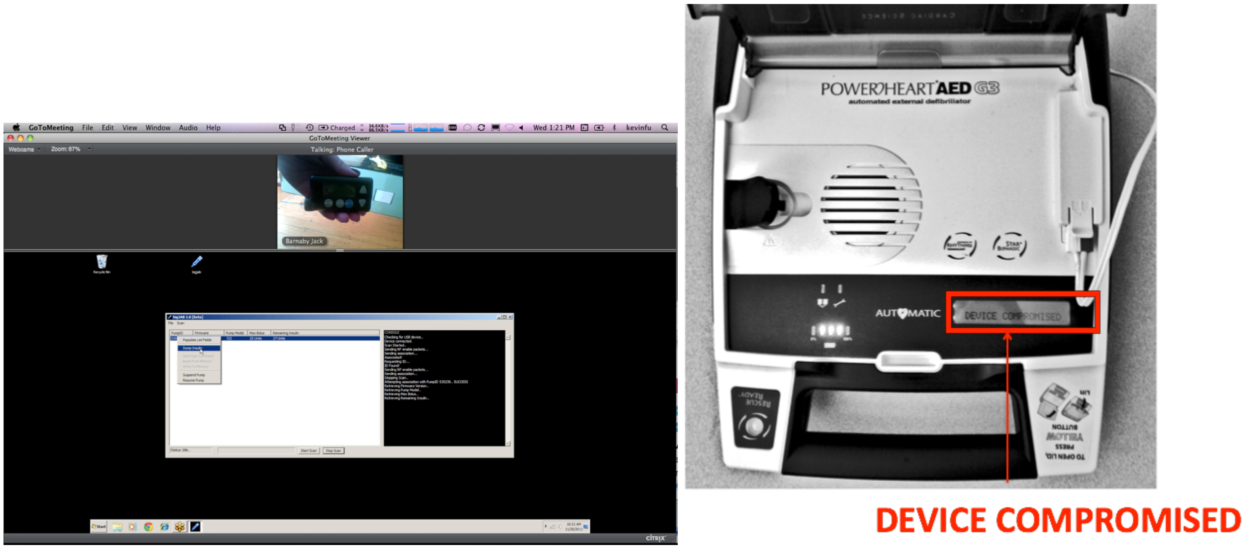
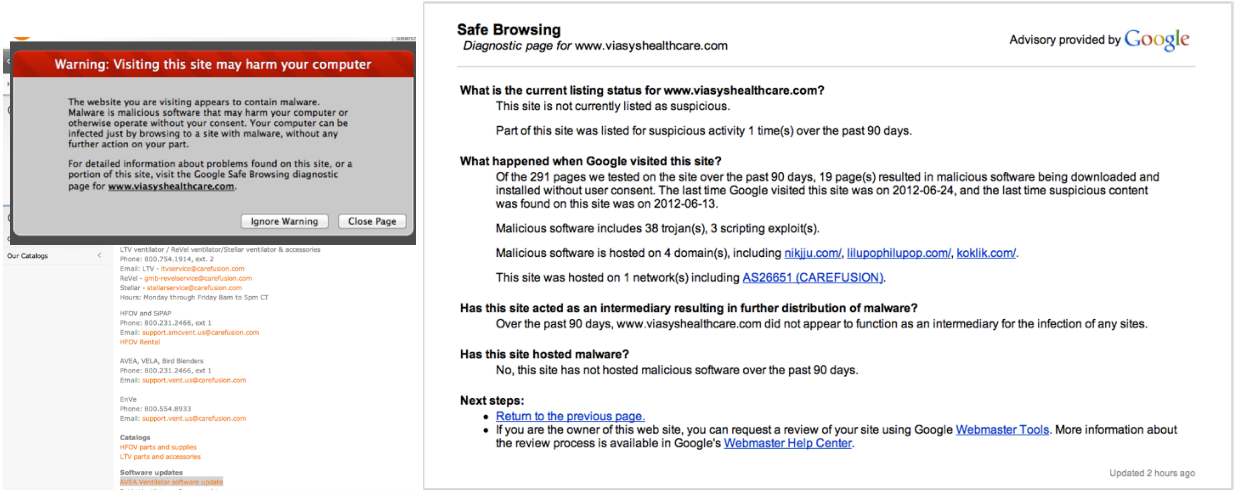


Figure 2: *Barnaby Jack demonstrates to the author a vulnerability in an insulin pump (L). Screenshot copyright Kevin Fu. Hanna et al. demonstrate a proof of concept computer worm that spreads from a safety officer's computer to an Automated External Defibrillator [9] (R). Photo publicly available under open access policy by USENIX.*



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.

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

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

Figure 3: *In June 2012, the author discovered that the website of a ventilator manufacturer was compromised such that unsuspecting hospital technicians downloading a software update received a bonus malware package.*

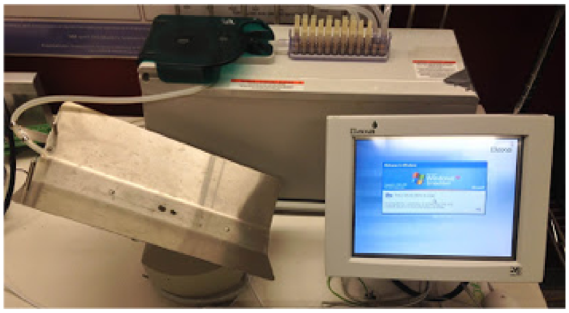


Figure 4: *A drug compounder running Windows XP Embedded was infected with malware according to an FDA MAUDE adverse event report in 2010 [3]. A former engineer from the company later explained that the malware was accidentally spread to other compounders during the repair. Photo copyright Kevin Fu.*

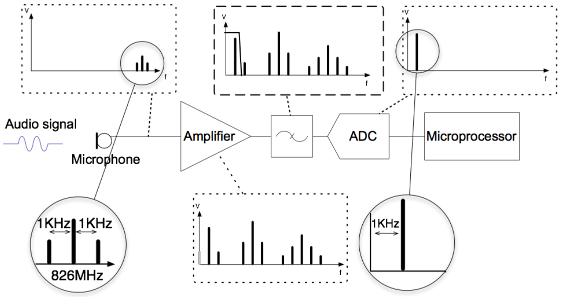


Figure 5: *Exploiting the non-linear components of a sensor front end allows injection of a chosen digital sensor input to a microprocessor [4]. The non-linear component acts as an unintended demodulator for the malicious EMI. Diagram courtesy Denis Foo Kune.*

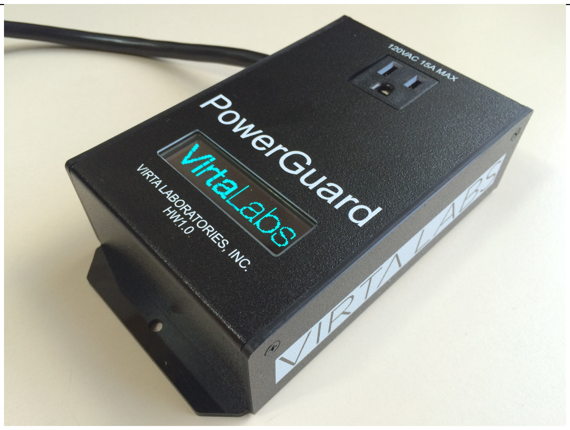


Figure 6: *A smart power outlet designed to detect anomalies and malware via the AC power outlet rather than software. The power outlet uses (among other things) advanced machine learning algorithms and spectral analysis to detect unusual behavior. One can learn about basics of power analysis from an earlier research paper [2]. Photo copyright Virta Labs, Inc. Used with permission.*

Analog Cybersecurity and Cybersecurity Testing Facilities

The author believes that two directions will lead to improvements in medical device security (and security of the Internet of Things in general).

Analog cybersecurity is one of the least understood and least studied area in cybersecurity. Security problems tend to occur in boundary conditions where different abstractions meet. In particular, the analog-digital abstraction poses subtle security weaknesses for cyberphysical systems such as medical devices or the Internet of Things. Researchers have already demonstrated how an adversary can violate widely held computing abstractions as fundamental as the value of a bit. Ionizing radiation and computing faults cause smartcards and processors to divulge cryptographic secrets [1, 12]. Intentional electromagnetic interference causes sensors to deliver incorrect digital values to closed-loop feedback systems such as pacemakers [4]. Acoustic and mechanical vibrations cause drones to fall out of the sky by hitting the resonant frequency of a MEMS gyroscope [13]. The row hammer attack[5] shows how to flip bits in computer memory by rapid activity to adjacent physical rows of memory [10]. The GSMem system [7] shows how to trick computer memory into emitting RF signals in the cellular frequencies. Such analog cybersecurity weaknesses will likely play an increasing role for automated systems such as medical devices.

The notional Bring Your Own Hospital (BYOH) testbed underway at the University of Michigan will enable security testing and experimentation on systems of medical devices to better prepare manufacturers and

[5] http://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

hospitals to cope with the changing threat landscape. The challenge is that manufacturers have difficulty testing beyond the component level because of (1) the diverse array of different configurations and interoperating medical devices, and (2) because of uncertainty of risk to patients during live testing. The BYOH testbed will enable security testing with automated and highly configurable threat simulators. Example uses include control studies to compare effectiveness of different hospital information security policies, and emergency preparedness fire drills to train manufacturers and clinicians on how to respond to cyberattacks and malware infections that affect the timely delivery of care.

Conclusion

Medical devices help patients lead more normal and healthy lives. The device innovation results from a complex interplay of medicine, computer engineering, computer science, human factors, and countless other disciplines. This complexity breeds design-time cybersecurity risks. In order to give patients the confidence to use emerging medical devices, manufacturers need to address the cybersecurity risks during the initial requirements engineering and design time, then continue post-market surveillance thru the product lifecycle.

Acknowledgments

This work is supported in part by by the Archimedes Center for Medical Device Security and the National Science Foundation under the THAW.org project (Award CNS-1330142). Any opinions, findings, and conclusions expressed in this material are those of the author and do not necessarily reflect the views of NSF.

References

[1] Dan Boneh, Richard A. Demillo, and Richard J. Lipton. On the importance of eliminating errors in cryptographic computations. *Journal of Cryptology*, 14:101–119, 2001.

[2] Shane S. Clark, Benjamin Ransford, Amir Rahmati, Shane Guineau, Jacob Sorber, Wenyuan Xu, and Kevin Fu. WattsUpDoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices. In *USENIX Workshop on Health Information Technologies*, August 2013.

[3] MAUDE adverse event report: Baxa corp. exacta-mix 2400, 2010. http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/detail.cfm?mdrfoi__id=1719489.

[4] Denis Foo Kune, John Backes, Shane S. Clark, Daniel B. Kramer, Matthew R. Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In *Proceedings of the 34th Annual IEEE Symposium on Security and Privacy*, May 2013.

[5] Kevin Fu. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*, July 2011. IOM (Institute of Medicine), National Academies Press.

[6] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They can hear your heartbeats: Non-invasive security for implanted medical devices. In *Proceedings of ACM SIGCOMM*, August 2011.

[7] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. GSMem: Data exfiltration from air-gapped computers over GSM frequencies. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 849–864, Washington, D.C., August 2015. USENIX Association.

[8] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the 29th Annual IEEE Symposium on Security and Privacy*, May 2008.

[9] Steve Hanna, Rolf Rolles, Andres Molina-Markham, Pongsin Poosankam, Kevin Fu, and Dawn Song. Take two software updates and see me in the morning: The case for software security evaluations of medical devices. In *Proceedings of 2nd USENIX Workshop on Health Security and Privacy (HealthSec)*, August 2011.

[10] Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, and Onur Mutlu. Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. In *Proceeding of the 41st Annual International Symposium on Computer Architecuture*, ISCA '14, pages 361–372. IEEE Press, 2014.

[11] N Leveson and C Turner. An investigation of the Therac-25 accidents. *IEEE Computer*, 26(7):18 – 41, 1993.

[12] Andrea Pellegrini, Valeria Bertacco, and Todd Austin. Fault-based attack of rsa authentication. In *Proceedings of the Conference on Design, Automation and Test in Europe (DATE)*, pages 855–860, 2010.

[13] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 881–896, August 2015.