

Dr. Kevin Fu, Ph.D.
Beyster Building
2260 Hayward St.
Ann Arbor, MI 48109-2121

May 30, 2018

House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden and Ranking Member Pallone:

Thank you for the opportunity to provide input into the important discussion on legacy medical technologies challenges, opportunities, considerations, and suggestions regarding supported lifetimes. I commend this Committee for bringing focus to and looking for feedback on this critical and pervasive healthcare challenge.

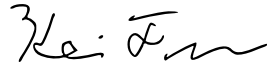
Credentials. I represent the academic cybersecurity community to ensure the next hundred years of trustworthy medical devices, autonomous transportation, and IoT devices. However, the opinions here are my own. Any opinions, findings, and conclusions expressed in this letter are my own and do not necessarily reflect the views of my employers or sponsors. I am founder and director of the Archimedes Center for Medical Device Security at the University of Michigan (secure-medicine.org). I conduct research on computer security and healthcare as part of the National Science Foundation's Trustworthy Health and Wellness (THAW.org) Frontiers project and previously HHS ONC's Strategic Healthcare IT Advanced Research Projects on Security (SHARPS.org). I co-founded the healthcare cybersecurity company Virta Labs. I serve as national chairperson of the Cybersecurity Task Force of the Computing Research Associations Computing Community Consortium (CCC). My participation in the 2008 IEEE paper analyzing the security of a defibrillator led to a wake-up call for medical device manufacturing [11]. I co-chaired the AAMI Working Group on Medical Device Security, which created the first engineering document recognized by the FDA as a medical device security consensus standard. I co-authored the 2012 NIST Information Security and Privacy Advisory Board recommendations [12] to the HHS Secretary on how the federal government must adapt to risks of medical device security. Beginning with my 2006 security seminar at FDA CDRH, my medical device security efforts were recognized with a Fed100 Award, Sloan Research Fellowship, NSF CAREER Award, MIT TR35 Innovator of the Year award, and best paper awards on medical device security by organizations such as IEEE and ACM [14, 9, 13, 8, 6, 3, 4, 1, 2, 10, 7, 5].

The Archimedes Center for Medical Device Security was established to help manufacturers and industry experts navigate the operational hazards of cybersecurity implementation and prepare them for future challenges of FDA requirements. Archimedes is an independent, pioneering center that has produced the most highly cited research on cybersecurity of medical devices. We focus on research, education, and advising industry leaders on methods for improving medical device security. Our members and partners include leading medical device manufacturers, healthcare organizations, regulators including the FDA, standards bodies, and physicians. We offer the following observations and comments about the challenge of security on legacy medical devices based on our research, experience, and our ongoing partnerships with the industry, healthcare, and government.

- A vital first step to reducing legacy device risk for healthcare providers is knowing exactly what devices they have, where they are, and what their current security posture is. Only then can an understanding of the risk be gained and an approach and response plan developed. Until recently, and for a variety of reasons, that has been a nearly impossible challenge for healthcare providers to discover and maintain. However, new software tools and techniques are becoming available to automate the gathering and analysis of this information. Healthcare providers should be encouraged, and government and industry should support, the development of such capabilities across healthcare facilities.
- Device Manufacturers should be highly encouraged or required to provide a software “bill of materials” for all products currently post-market, and for all new devices as they come to market. This provides valuable and actionable information to healthcare providers, regulators, and researchers in assessing the impact of a new vulnerability on their devices and executing a timely response and recovery plan.
- For legacy devices, we have high concern for security incidents affecting the availability of a device. That is, the device or the therapy it delivers is made not operational. These devices are running very old and unsupported operating systems/software without patches applied, which makes them very fragile and brittle to anything unusual, which frequently results in disruption to clinical workflow. The patient safety impact could be high if this happens during a procedure or treatment.
- An agreed set of guidelines or practices could be established to more clearly define the expectations, limitations, timelines, and responsibilities for manufacturers and healthcare providers in their support of secure software in legacy devices. This is an ongoing point of frustration and confusion for stakeholders. Resolving some of these issues would help to reduce the rhetoric and increase progress.
- We must broaden the level and increase the depth of data gathering and information sharing about legacy device vulnerabilities and solutions for all stakeholders. There is a need for a more complete and reliable dataset on legacy devices and their vulnerabilities. And while much progress has been made on vulnerability reporting and response, not enough of the key stakeholders are fully committed.
- The recently released FDA Safety Action Plan could be very helpful in addressing the security issues surrounding legacy devices. The increased rigors of this plan, if implemented, will add some much needed teeth to apply pressure to stakeholders to make meaningful improvement.

Once again, we applaud the Committee on taking up the issue of security of legacy medical devices and truly appreciate the opportunity to provide input and commentary. We look forward to being part of and supporting any next steps taken by the Committee.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Kevin Fu". The signature is fluid and cursive, with the first name "Kevin" and last name "Fu" clearly distinguishable.

Kevin Fu, Ph.D.
Director, Archimedes Center for Medical Device Security
Associate Professor, EECS Department
University of Michigan
archimedes@umich.edu

References

- [1] B. Defend, M. Salajegheh, K. Fu, and S. Inoue. Protecting global medical telemetry infrastructure. Technical report, Institute of Information Infrastructure Protection (I3P), Jan. 2008. https://web.eecs.umich.edu/~kevinfu/papers/whitepaper-protecting_global_medical.pdf.
- [2] K. Fu. Inside risks, reducing the risks of implantable medical devices: A prescription to improve security and privacy of pervasive health care. *Communications of the ACM*, 52(6):25–27, June 2009. <http://www.csl.sri.com/users/neumann/insiderisks08.html#218>.
- [3] K. Fu. Software issues for the medical device approval process, Apr. 2011. Statement to the Special Committee on Aging, United States Senate, Hearing on a delicate balance: FDA and the reform of the medical device approval process, Wednesday, April 13, 2011. <https://spqr.eecs.umich.edu/papers/fu-senate-comm-aging-med-dev-sw-apr-2011.pdf>.
- [4] K. 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*, Washington, DC, July 2011. IOM (Institute of Medicine), National Academies Press. <https://spqr.eecs.umich.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf>.
- [5] K. Fu. On the technical debt of medical device security. Technical report, National Academy of Engineering FOE, Sept. 2015. A version appeared in the National Academy of Engineering’s *The Bridge*, Winter 2016.
- [6] K. Fu. Infrastructure disruption: Internet of things security, Nov. 2016. Testimony to the U.S. House Energy and Commerce Committee, Subcommittee on Communications and Technology & Subcommittee on Commerce, Manufacturing, and Trade joint hearing on Understanding the Role of Connected Devices in Recent Cyber Attacks, Wednesday, November 16, 2016.
- [7] K. Fu and J. Blum. Inside risks: Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, 56(10):21–23, Oct. 2013. <http://www.csl.sri.com/users/neumann/cacm231.pdf>.
- [8] K. Fu, J. Halamka, J. Kufahl, and M. Logan. Commentary: Hospitals need better cybersecurity, not more fear, Sept. 2016. *Modern Healthcare*.
- [9] K. Fu, W. Xu, and C. Yan. How we reverse engineered the Cuban sonic weapon attack. *IEEE Spectrum*, Mar. 2018.
- [10] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, 7(1):30–39, Jan. 2008. <https://spqr.eecs.umich.edu/papers/b1kohFINAL2.pdf>.
- [11] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. 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*, pages 129–142, May 2008. <https://www.secure-medicine.org/public/publications/icd-study.pdf>.
- [12] NIST ISPAB federal advisory committee recommendations on improving medical device cybersecurity, 2012. Sent to OMB Director, HHS Secretary, NSC, DHS, NIST, March 30, 2012. <http://1.usa.gov/1qlnh0X> or http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-ltr-to-omb_med_device.pdf.
- [13] B. Ransford, D. Kramer, D. Foo Kune, J. Auto de Medeiros, C. Yan, W. Xu, T. Crawford, and K. Fu. Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists. *Pacing and Clinical Electrophysiology (PACE)*, 40(8):913–917, July 2017.
- [14] D. J. Slotwiner, F. Deering, K. Fu, A. M. Russo, M. N. Walsh, and G. F. Van Hare. Cybersecurity vulnerabilities of cardiac implantable electronic devices. *Heart Rhythm*, May 2018.