DOI:10.1145/2890488

With the implantation of software-driven devices comes unique privacy and security threats to the human body.

BY A.J. BURNS, M. ERIC JOHNSON, AND PETER HONEYMAN

A Brief Chronology of Medical Device Security

THE CAPABILITIES OF modern medical devices continue to radically transform the treatment of acute conditions as well as the management of chronic long-term disease. As these technologies evolve, so also do the threats to the security and reliability of these devices. Over the past decade, there has been no shortage of headlines warning of pacemaker turned peacemaker, or insulin assassinations. Although these taglines are fictional (but not unimaginable), they capture the tenor of much of the medical device security reportage. While we strongly affirm the necessity of public awareness of these issues, we believe that hyperbole and/or mischaracterizations may lead to panic, desensitization, or perhaps worse, exploitation.

Today, attention is turning to the dangers posed by the omnipresent cyber threat, as signaled with the long-awaited release on Oct. 2, 2014 of Food and Drug Administration (FDA) guidance on the management of cybersecurity in medical devices,[7] and the more recent draft guidance of Postmarket Management of Cybersecurity in Medical Devices.[8] Therefore, as the human body joins the illustrious Internet of Things, it is constructive to take pause and see how we got here. We hope this brief chronology of medical device and health IT security helps provide context for the current state of medical device security.

Though not clearly defined, it appears to us there have been several inflection points in the relatively brief history of medical devices. The first period is essentially a spillover from the broader systems engineering field involving concern over complex systems and accidental disasters. The second period begins with the advent of implantable medical devices, and the third with the threat of unauthorized access to these devices that could cause harm. Finally, the fourth and most recent period is the era of the cyber threat to medical device security. Tying all of these together are the implications of software-controlled systems and the threats to device and system security and consequently, patient health and privacy. We also spot-

» key insights

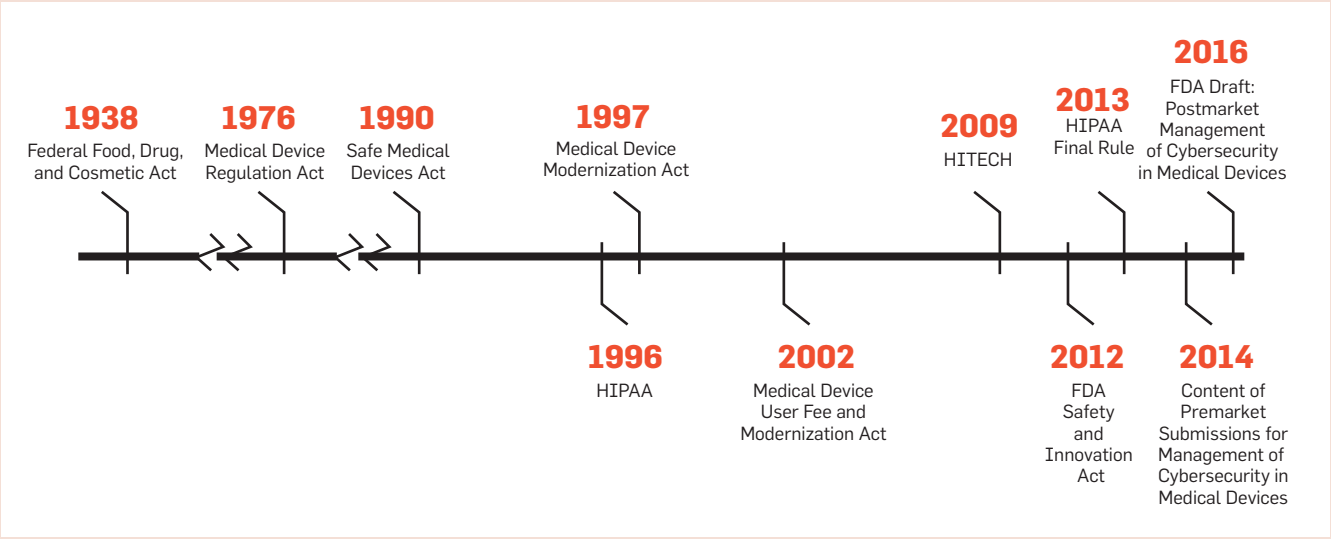
- The achievements of modern engineering and computer science are producing medical technologies that not only extend the lives of many patiences, but also enhance the quality of life for many more managing chronic illness.
- Though medical devices are unique, the cybersecurity threats to medical device security are not unlike those that threaten other software-controlled, network-enabled devices.
- All security-focused decisions involve trade-offs. To fully understand the security trade-offs involved in designing, deploying, and maintaining medical devices, we believe it is critical to pause and take stock of what is at stake.

X-RAY IMAGE BY TEWAN BANDITRUKKANKA

L

UPRIGHT

Timeline of Important Legislation



On Oct. 2, 2014, the FDA released its guidance on the management of cybersecurity in medical devices. This guidance represents the most recent in a long line of federal/legislative initiatives aimed at regulating and/or enhancing security and privacy in the highly sensitive health sector. We outline some of the important federal initiatives below, beginning with the passage of the Federal Food, Drug, and Cosmetic Act of 1938 and ending with the FDA Guidance on medical device cybersecurity in 2014.

1938 Federal Food, Drug, and Cosmetic Act. **In the wake of a medicinal disaster known as Elixir Sulfanilamide in 1937, Congress passed the Federal Food, Drug, and Cosmetic Act of 1938. Today, this act along with its many amendments, has become one of the most influential in the history of U.S. medicine. In addition to extending the purview of the FDA over medical devices and cosmetics, the FD&C Act of 1938 also first mandated the FDA pre-market approval of pharmaceuticals. The overwhelming need for such regulation is expressed by a doctor's regrets over the Elixir Silfanilamide incident:**

"... six human beings, all of them my patients, one of them my best friend, are dead because they took medicine that I prescribed for them innocently, and to realize that that medicine which I had used for years in such cases suddenly had become a deadly poison in its newest and most modern form, as recommended by a great and reputable pharmaceutical firm in Tennessee: well, that realization has given me such days and nights of mental and spiritual agony as I did not believe a human being could undergo and survive. I have known hours when death for me would be a welcome relief from this agony." (Letter by Dr. A.S. Calhoun, Oct. 22, 1937) **[a,b]**

1976 Medical Device Regulation Act **"passed to ensure safety and effectiveness of medical devices, including diagnostic products. The amendments require manufacturers to register with FDA and follow quality control procedures. Some products must have pre-market approval by FDA; others must meet performance standards before marketing."[c]**

1990 Safe Medical Devices Act **"requires nursing homes, hospitals, and other facilities that use medical devices to report to FDA incidents that suggest that a medical device probably caused or contributed to the death, serious illness, or serious injury of a patient. Manufacturers are required to conduct post-market surveillance on permanently implanted devices whose failure might cause serious harm or death, and to establish methods for tracing and locating patients depending on such devices. The act authorizes FDA to order device product recalls and other actions."[d]**

1996 HIPAA. **Regulated by the U.S. Department of Health and Human Services, the Health Information Portability and Accountability Act of 1996 resulted in the establishment of two important patient safeguards, the HIPAA Privacy Rule, and the HIPAA Security Rule. The Privacy Rule established "national standards for the protection of certain health information," and the Security Rule established "a national set of security standards for protecting certain health information that is held or transferred in electronic form."[e]**

[4]1997 FDA Modernization Act. **"Provisions include measures to accelerate review of devices, regulate advertising of unapproved uses of approved drugs and devices, and regulate health claims for foods."[c]**

***2002 Medical Device User Fee and Modernization Act*—"fees are assessed sponsors of medical device applications for evaluation, provisions are established for device establishment inspections by accredited third parties, and new requirements emerge for reprocessed single-use devices."[c]**

2009 HITECH Act. **Enacted under the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act established for the provision of "business associate liability; new limitations on the sale of protected health information, marketing, and fundraising communications; and stronger individual rights to access electronic medical records and restrict the disclosure of certain information." Additionally, new rules were established for breach notifications with penalties applied for failure to notify individuals affected by breaches meeting certain criteria discovered after February 10, 2010.[e]**

2012 FDA Safety and Innovation Act (FDASIA) **"expands FDA authorities to collect user fees from industry to fund reviews of innovator drugs, medical devices, generic**

a http://www.fda.gov/AboutFDA/WhatWeDo/History/Origin/ucm054826.htm

b Ballentine, Carol, "Taste of Raspberries, Taste of Death: The 1937 Elixir Sulfanilamide Incident," FDA Consumer magazine, 1981; Available at www.fda.gov/downloads/AboutFDA/WhatWeDo/History/Origin/ucm125604.doc.

c http://www.fda.gov/AboutFDA/WhatWeDo/History/Origin/ucm054826.htm

d http://www.fda.gov/AboutFDA/WhatWeDo/History/Milestones/ucm128305.htm

e http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

drugs and biosimilar biological products; promotes innovation to speed patient access to safe and effective products; increases stakeholder involvement in FDA processes, and enhances the safety of the drug supply chain."[c]

2013 HIPAA Final Rule. "[A] final rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)."[f]

2014 FDA Guidance on Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Guidance issued by the FDA on the security of medical devices. It recommends that manufacturers "consider cybersecurity risks as part of the design and development of a medical device, and submit documentation to the FDA about the risks identified and controls in place to mitigate those risks. The guidance also recommends that manufacturers submit their plans for providing patches and updates to operating systems and medical software."[g]

2016 FDA Draft Guidance on Post-Market Management of Cybersecurity in Medical Devices. "The draft guidance details the agency's recommendations for monitoring, identifying and addressing cybersecurity vulnerabilities in medical devices once they have entered the market."[h]

f http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/

g http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm416809.htm

h http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm

light the legislative timeline and the evolving threats to information security in healthcare.

Period 1. Complex Systems and Accidental Failures (1980s–Present)

"Welcome to the world of high-risk technologies," begins the introduction to Charles Perrow's treatise on Normal Accidents.[21] From nuclear power plants to avionics to medical technologies, systems engineering feats in the second half of the 20th century forever altered human capabilities and the management of complex processes. However, these advances were accompanied by novel threats to the safety and security of these devices, and constituencies.

1985–1987: Therac-25. From June 1985 to January 1987, six patients received harmful levels of radiation due to defective Therac-25 accelerators. Still studied as a case of complex failure, the Therac-25 disaster was a deadly concoction of user error, faulty software engineering, and insufficient training/support. For example, in one instance, a software glitch caused the device to indicate a malfunction had occurred, causing a radiation therapist to erroneously readminister radiation several times. As it turned out, these glitches had become a part of the daily use of Therac-25, and the manufacturer's support provided little help in the way of troubleshooting or interpreting error codes.[16]

2002: BIDMC network failure. On November 13, 2002, a researcher inadvertently flooded the network of the Beth Israel Deaconess Medical Center (BIDMC) with data, causing harmful delays in access to critical information and information systems. Unfortunately, the network diagnostics were only available through the network itself. When unable to sort out the issues, the hospital pulled the network offline for four days and reverted to paper-based processes. As noted, "[t]he principal point of failure was a software program for directing traffic on the network. The program was overwhelmed by a combination of data volume and network complexity that exceeded the software's specifications."[14]

Period 2. Implantable Medical Devices (2000–Present)

The first decade of the 21st century brought about significant changes in the medical device landscape. By 2001, the number of implantable medical devices (IMDs) in use in the U.S. was greater than 25 million.[22] The advent of IMDs raised the stakes considerably for the security and reliability of medical devices. Previously, the context of device failure was largely constrained to external devices housed in hospitals, clinics, and patient homes. With IMDs, the context of operation expanded symmetrically with the range of activity of the patient. Additionally, the integration of devices into the human body complicated the data communication process between device and physician.

2000s: Implantable Cardiac Defibrillator failure. From 1990 to 2000 the FDA issued recalls affecting 114,645 implantable cardiac defibrillators (ICD).[18] In 2005, the death of a 21-year-old cardiac patient garnered greater attention than many of the previous ICD failures when an ICD short-circuited while initiating what might have been a life-saving electrical shock.[13] In the aftermath of this high-profile tragedy, the health and safety risks associated with ICD malfunctions became a matter of public concern.[19,23]

2005: HCMSS. In June 2005, a workshop on High Confidence Medical Device Software and Systems (HCMSS) was held in Philadelphia, PA. Sponsored by FDA, NIST, NSF, NSA, and NITRD, the workshop had the goal of developing a roadmap for overcoming crucial issues and challenges facing the design, manufacture, certification, and use of medical device software and systems.

Period 3. Unauthorized Parties and Medical Devices (2006–Present)

By 2006, medical device software had reached a tipping point in the U.S. as 50% of the medical devices on the market were either standalone software packages or other device-types with some software-driven functionality.[6,22] The increasing complexity of these devices enabled by software led many researchers and some high-profile patients to begin questioning the vulnerability of medical devices (particularly IMDs) to unauthorized parties. It was during this time that the concept of 'medical device hacking' became a mainstream concern.

2006: Software updates for embed-

ded devices. In 2006, researchers demonstrated the challenges of securely updating the software of embedded devices.[2] Embedded devices lack interfaces that allow a client to acknowledge and install updates. Further, the nature of these devices necessitates that they are both nomadic and, in terms of network connectivity, sporadic. These attributes make embedded devices particularly susceptible to man-in-the-middle attacks.

2008: Implantable Cardiac Defibrillator. In 2008, researchers exposed vulnerabilities in an FDA-approved ICD that allowed modified-off-the-shelf devices to be configured to eavesdrop on information generated by the device and even control the defibrillator's dispensation of electric shock.[12]

2008: *Reigel vs. Medtronic*. In the midst of the revelations of novel security threats posed by implantable devices, the U.S. Supreme Court ruled in a high-profile case limiting liability for medical-device manufacturers for harms caused by devices approved by the FDA.[5]

2011: The year of the insulin pump. In 2011, several high-profile events involving the security of implantable insulin pumps caught the attention of the academics, practitioners, and the public at large. That same year a review of the state of trustworthy medical device software recommended the following to increase the trustworthiness of medical device software: [9]

- regulatory policies that specify outcome measures rather than technology,
- collection of statistics on the role of software in medical devices,
- establishment of open-research platforms for innovation,
- clearer roles and responsibility for the shared burden of software, clarification of the meaning of substantial equivalence for software, and
- an increase in Food and Drug Administration (FDA) access to outside experts in software.

2011: Peer-reviewed insulin pump vulnerability. In 2011, vulnerabilities of insulin pumps to unauthorized parties were disclosed.[17] Using off-the-shelf hardware, successful passive attacks (for example, eavesdropping of the wireless communication) and active attacks (for example, impersonation and control of the medical devices to alter the intended therapy) were achieved.[17] These findings exposed a vulnerability in certain insulin pumps that could allow an unauthorized party to "emulate the full functions of a remote control: wake up the insulin pump, stop/resume the insulin injection, or immediately inject a bolus dose of insulin into the human body."[17]

2011: Peer-reviewed defenses against unauthorized access to IMDs. In response to emerging radio frequency (RF) vulnerabilities, a novel defense against unauthorized access proposed an RF shield to act as a proxy for communications with implantable medical devices (IMD).[10] The shield actively prevents any device other than itself from communicating directly with the IMD by jamming all other communications.

Extending the shield concept, a similar defense emerged that passively monitors an individual's personal health system and interferes in the case of a detected anomaly, eliminating the need for protocol changes to interact with the "shield."[24]

2011: Jerome Radcliffe and Barnaby Jack. On August 4, 2011, Jerome Radcliffe, a diabetic patient, presented a talk at Black Hat 2011 in Las Vegas, NV, in which he announced he had partially reverse engineered the communication protocols for his own insulin pump. His presentation exposed a vulnerability in some insulin pumps allowing unauthorized access and control through the wireless channel.[3] This presentation got the attention of many mainstream media outlets and brought the health and safety risks attributable to unauthorized access and control of medical devices previously identified by researchers and exploited in laboratories into the consciousness of the general public.

In October 2011, in Miami, FL, under the auspices of McAfee (now a division of Intel), famed late hacker Barnaby Jack made a presentation at the Hacker Halted conference exposing security vulnerabilities that allowed an insulin pump to be commandeered remotely via radio frequency.[3]

Period 4. Cybersecurity of Medical Devices (2012–Present)

Most recently, attention has turned to the cybersecurity of medical devices. Harnessing the capabilities of ubiquitous networks, medical device manufacturers are increasingly enabling the connectivity of devices through the Internet or over networks, which also carry the Internet (for example, LANs). There are many advantages to connected devices, including real-time monitoring and software management such as remote installation of software updates. However, medical devices are not immune to the kinds of cybersecurity threats that have become prevalent in this network age. In fact, in terms of the potential consequences, the protection of medical devices is often more critical than that of other device types.

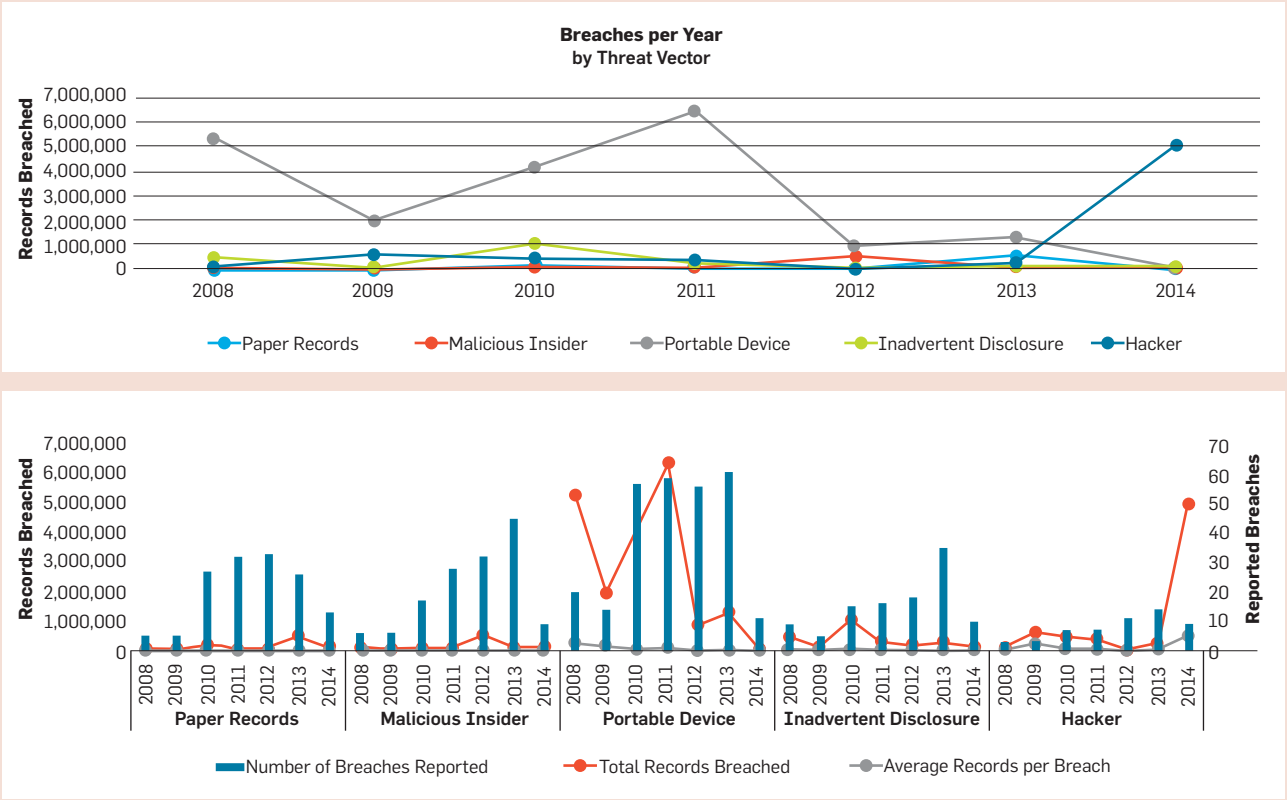
2012: ISPAB Board meeting. In February 2012, the Information Security and Privacy Advisory Board (ISPAB) held its annual board meeting in Washington, D.C. Great concern was expressed regarding emerging issues related to cybersecurity and the associated economic incentives of medical devices to increase medical device cybersecurity, and the coordination of agencies in the regulation of medical device cybersecurity.[4]

Specifically, software-controlled medical devices are increasingly available through and exposed to cybersecurity risks on the Internet. Further complicating this picture, the economics of medical device cybersecurity involves a complex system of payments between multiple stakeholders—including manufacturers, providers, and patients. At the same time, no one agency has primary responsibility from Congress to ensure the cybersecurity of medical devices deployed across this spectrum.[4]

2012: Barnaby Jack pacemaker hack. On October 17, 2012, at the Ruxcon Breakpoint Security Conference in Melbourne, Australia, Barnaby Jack exhibited a video presentation in which he demonstrated the ability to deliver an unwarranted shock through a pacemaker via wireless transmission. Jack found that certain devices could be accessed using a serial and model number. Exposing an important vulnerability, Jack disclosed that the devices would give up these credentials (that is, serial number and model number) when wirelessly contacted with a specific command, giving an unauthorized party the power to control the device.[1]

2013–2014: FDA guidance on medi-

Evolving Threat Vectors of Infosec



On Aug. 18, 2014, Community Health Systems (CHS), one of the largest publicly traded hospital system in the U.S., reported that it had experienced the largest-ever breach of patient health information with the exposure of personal information of 4.5 million individuals. This hacking case, along with other high-profile instances, such as the highly publicized breach of a test server of the new Healthcare.gov site, highlight the evolving cyber-threat to information security in the health sector.

Health IT. **The health industry has long been a laggard in terms of IT adoption. Today, spurred on by legislative initiatives such as HITECH, the rate of electronic health record (EHR) adoption is accelerating in the U.S. Increased opportunities for health information exchange, standardized data collections for use in medical research, and more effective treatment of patients are among the many potential benefits of the aggregation of patient health information into EHR systems. However, centralized EHR systems also create an economic incentive for malicious actors seeking access to the greatest number of records at the lowest cost. Previously, individual patient records were segmented in large part by storing various versions of an individual's record, often in the form of paper records, in separate systems—creating less efficient targets (that is, information silos).**

Breach trends. **The magnitude and nature of the threat vectors to health information security have evolved over just the past few years. Assessing the breach information provided by the Privacy Rights Clearinghouse (privacyrights.org), two inflection points emerge:**

- **The increase in the number of breaches reported in 2010**
- **The emerging impact of cyber-threats in 2014**

We believe the spike in reported breaches in 2010 is likely attributable to the passing of HITECH in 2009 and the accompanying stringent reporting standards and meaningful use requirements. Meanwhile, the cyber-threat to information security in 2014 was amplified by the CHS breach of 4.5 million records. Interestingly, it appears that the industry has improved its ability to limit the exposure of lost or stolen portable devices. In fact, despite a fairly consistent level of breaches reported, the total records breached from stolen or lost portable devices appears to be stabilizing at a lower level.

cal device cybersecurity. In June 2013, the FDA released draft guidance for the management of cybersecurity in medical devices, with the final guidance being released in October 2014.[7] Drawing on much of the experiences and associated research presented here, the FDA guidance places emphasis on the need to consider device security during the design and development stages of medical devices. Specifically the guidance recommends the following:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies; and
- Assessment of residual risk and risk acceptance criteria.

The guidance also identifies "core functions" of cybersecurity activities from the National Institute of Standards and Technology (NIST) cybersecurity framework.[20]

2013–2016: State of medical device

security. Recently, security experts have begun advocating for a more holistic approach to securing increasingly complex and connected medical devices.[25] Noted trust challenges include: hardware failures/software errors, radio attacks, malware and vulnerability exploits, and side-channel attacks.[25]

A 2014 survey of medical device security research found that the majority of the work in security and privacy has been centered on threats to the telemetry interface.[22] That is, much prior research has examined threats to, and defenses of, medical device radio-based communication channels. The survey highlights five important areas of research in wireless telemetry: biometric authentication, distance-bounding authentication, out-of-band authentication, external devices, and anomaly detection.[22]

There are inherent challenges in examining the software threats to medical device security. Not the least of these challenges is the reality that medical devices operate within a "closed source" paradigm, presenting challenges to performing static analyses or obtaining device firmware.[22] Despite these challenges, the importance of ongoing security evaluation is clear, and the FDA's 2016 draft guidance on post-market management of cybersecurity of medical devices seeks to provide recommendations for ensuring cybersecurity in devices that are already in circulation.[8]

The Future of Medical Device Security

The steps we take today will largely define the future of medical device security. Security is a game of trade-offs and the stakes are never higher than in healthcare. However, we must resist the temptation to sensationalize the issues related to cybersecurity in the health sector, and instead apply sober, rational, systematic approaches to understanding and mitigating security risks. Fortunately this approach is taking hold across the industry with the FDA recommending NIST's cybersecurity framework prescribing that firms:

- *Identify*. Identify processes and assets needing protection;
- *Protect*. Define available safeguards;
- *Detect*. Devise incident detection techniques;
- *Respond*. Formulate a response plan; and
- *Recover*. Formalize a recovery plan.[20]

In closing, the threats to the cybersecurity are emergent, and the inevitability of so-called 'zero-day vulnerabilities' must be addressed over the entire useful life of medical devices. This reality is a necessary outworking of innovation and should be embraced by healthcare providers, device manufacturers, software/app developers, security engineers, and even patients.

The medical field has long recognized the fiduciary responsibility of physicians with regard to patients' well-being,[11] and it is safe to say that patients' reluctance to accept medically indicated devices due to concerns about security poses a greater threat to their health than any threat stemming from medical device security. That said, in this world of high-risk medical technologies, it is incumbent on our field to continue to prioritize the security of medical devices as a part of our fiduciary responsibility to act in the interests of those who rely on these life-saving devices.

Acknowledgment

This work was supported by the National Science Foundation (NSF) project on Trustworthy Health and Wellness (THaW.org)–CNS-1329686 and CNS-1330142. The views expressed are those of the authors and should not be interpreted as representing the views, either expressed or implied, of NSF. We also thank Kevin Fu for his guidance. C

References

1. Applegate, S.D. The dawn of kinetic cyber. In *Proceedings of the 5th International Conference on Cyber Conflict*. IEEE, 2013, 1–15.
2. Bellissimo, A. et al. Secure software updates: Disappointments and new challenges. In *Proceedings of the USENIX Summit on Hot Topics in Security*, 2006.
3. Burleson, W. et al. Design challenges for secure implantable medical devices. In *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012, 12–17.
4. Chenok, D.J. ISPAB Letter to U.S. Office of Management and Budget (2012); http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-ltr-to-omb_med_device.pdf.
5. Curfman, G.D. et al. The medical device safety act of 2009. *New Eng.J. Med. 360,* 15 (2009), 1550–1551.
6. Faris, T.H. *Safe and Sound Software: Creating an Efficient and Effective Quality System for Software Medical Device Organizations.* ASQ Quality Press, 2006.
7. Food and Drug Administration. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Guidance for Industry and Food and Drug Administration Staff (2014); http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.
8. Food and Drug Administration. Postmarket Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff (2016); http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.
9. Fu, K. Trustworthy medical device software. *Workshop Report on Public Health Effectiveness of the FDA 510 (k) Clearance Process: Measuring Postmarket Performance and Other Select Topics.* National Academies Press. Washington, D.C. (2011), 102.
10. Gollakota, S. et al. They can hear your heartbeats: Non-invasive security for implantable medical devices. *ACM SIGCOMM Computer Communication Review 41*, 4 (2011), 2–13.
11. Hafemeister, T.L. and Spinos, S. Lean on me: A physician's fiduciary duty to disclose an emergent medical risk to the patient. *Washington University Law Review 86*, 5 (2009).
12. Halperin, D. et al. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of IEEE Symposium on Security and Privacy*. IEEE, 2008, 129–142.
13. Hauser, R.G. and Maron, B.J. Lessons from the failure and recall of an implantable cardioverter-defibrillator. *Circulation 112*, 13 (2005), 2040–2042.
14. Kilbridge, P. Computer crash-lessons from a system failure. *New Eng. J. Medicine 348*, 10 (2003), 881–882.
15. Lee, I. et al. High-confidence medical device software and systems. *Computer 39*, 4 (2006), 33–38.
16. Leveson, N.G. and Turner, C.S. An investigation of the Therac-25 accidents. *Computer 26*, 7 (1993), 18–41.
17. Li, C. et al. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *Proceedings of the 13th IEEE International Conference on e-Health Networking Applications and Services*. IEEE, 2011, 150–156.
18. Maisel, W.H. et al. Recalls and safety alerts involving pacemakers and implantable cardioverter-defibrillator generators. *JAMA 286*, 7 (2001), 793–799.
19. Meier, B. Maker of heart device kept flaw from doctors. *New York Times*, 2005.
20. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity (Ver. 1.0) Feb. 12, 2014; http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
21. Perrow, C. *Normal Accidents: Living with High Risk Technologies.* Princeton University Press, 2011.
22. Rushanan, M. et al. SoK: Security and privacy in implantable medical devices and body area networks. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. IEEE CS, 524–539.
23. Vladeck, D.C. Medical Device Safety Act of 2009: Hearing before the Subcomm. on Health of the Comm. on Energy and Commerce (111th Cong., May 12, 2009); http://scholarship.law.georgetown.edu/cong/45.
24. Zhang, M. et al. MedMon: Securing medical devices through wireless monitoring and anomaly detection. *IEEE Trans. Biomedical Circuits and Systems 7*, 6 (2013), 871-881; DOI 10.1109/TBCAS.2013.2245664.
25. Zhang, M. et al. Towards trustworthy medical devices and body area networks. In *Proceedings of the 50th Annual Design Automation Conference*. ACM, 2013, 1–6.

A.J. Burns (aburns@uttyler.edu) is an assistant professor of computer science at the University of Texas, Tyler.

M. Eric Johnson (Eric.Johnson@owen.vanderbilt.edu) is the Ralph Owen Dean and Bruce D. Henderson Professor of Strategy at Vanderbilt University, Nashville, TN.

Peter Honeyman (honey@umich.edu) is a research professor of computer science and engineering at the University of Michigan, Ann Arbor.

Watch the authors discuss their work in this exclusive *Communications* video. http://cacm.acm.org/videos/a-brief-chronology-of-medical-device-security