Journal of Diabetes Science and Technology
2018, Vol. 12(4) 743–746

DOI: 10.1177/1932296818763634
journals.sagepub.com/home/dst
SAGE

Standards for Medical Device Cybersecurity in 2018

Sean Yuan[1], Anura Fernando, MS[2], and David C. Klonoff, MD, FACP, FRCPE, Fellow AIMBE[3]

Keywords
cybersecurity, diabetes, digital health, device, medical device, mobile phone, standards

Diabetes Device Cybersecurity

Medical devices are increasingly connected wirelessly to each other and to data-management devices. Threats to the accurate flow of information and commands may compromise the safe function of these devices and put users' health at risk. These devices can be on-body wearable or implantable systems that monitor and transmit data from a person and send it to a hub (such as a handheld controller/monitor, another device, a smartphone, a pad, or the cloud) for analysis, presentation, aggregation with other data streams, and storage. Such devices might also receive data or commands to be relayed to the patient. These devices can also be large nonportable devices for diagnosis (eg, MRI, CT, PET, or ultrasound imaging equipment and ICU monitors) or for treatment (eg, infusion pumps, ventilators, and medical lasers located in health care facilities).

Sound cybersecurity of medical devices can be achieved by maintaining (1) confidentiality by protecting these devices from unauthorized disclosure, (2) integrity by protecting these products from unauthorized modification, and (3) availability of data by protecting these products from loss of function.[1] A medical data breach, which is the release of secure or private/confidential information to an untrusted environment, can represent a security risk, a safety risk, or both. Five steps for a hospital or medical organization to improve medical device cybersecurity include (1) establishing a risk management plan, (2) building a protection framework, (3) following basic security hygiene, (4) including security in contracts, and (5) building a zero trust network. Hospitals that act to improve medical device cybersecurity will decrease the risk of privacy breaches, financial ransom, and harm to patients.

Recent Developments in Standards

Recent hacks of hospitals and health insurance companies around the world have put medical device cybersecurity in the public spotlight. NIST published a cybersecurity framework in 2014[2] and an update to this document in 2017. Public comment for the update ended in January 2018.[3] In addition, The FDA has published two guidance documents related to the management of cybersecurity in medical devices: a 2014 document specifying the content of premarket submissions,[4] and a 2016 draft guidance for postmarket management of cybersecurity.[5] The first FDA guidance recommends that manufacturers integrate risk management into the development of medical devices and provide the FDA with certain documents when they submit for approval. The second FDA guidance recommends manufacturers continually monitor cybersecurity for products already on the market to account for new threats and vulnerabilities.

The FDA's guidance documents are advisory and not enforced by law.[6] However, not complying with the recommendations can result in a delayed approval process and penalties for unsafe products. In addition, these guidance documents are limited in scope. They do not evaluate the risk assessment process used by manufacturers to appraise the cyberthreats their products face, nor do they provide criteria for manufacturers to test the efficacy of the measures designed to combat those cyberthreats. To fill these gaps, private organizations have developed and published detailed consensus standards for the management of medical device cybersecurity. Three of the most prominent efforts have been TIR57, the UL 2900 series, and DTSec. The first two of these standards address risk assessment and development lifecycle processes, but do not specify a performance assessment of the actual product for adequate cybersecurity protection. DTSec, a standard intended only for diabetes devices, requires not only that manufacturers declare that they have met performance requirements including architecture that incorporates sound risk assessment and lifecycle processes, but that products be assessed for their performance.

[1]Diabetes Technology Society, Burlingame, CA, USA
[2]UL, Northbrook, IL, USA
[3]Mills-Peninsula Medical Center, San Mateo, CA, USA

Corresponding Author:
David C. Klonoff, MD, FACP, FRCPE, Fellow AIMBE, Diabetes Research Institute, Mills-Peninsula Medical Center, 100 S San Mateo Dr, Rm 5147, San Mateo, CA 94401, USA.
Email: dklonoff@diabetestechnology.org

AAMI TIR 57

Technical Information Report 57 (TIR57), "Principles for Medical Device Security—Risk Management," published by the Association for the Advancement of Medical Instrumentation (AAMI),[7] provides guidance to help medical device engineers integrate cybersecurity risk management into the overall development of the device so they can preemptively identify and stop potential threats before the device goes to market. Specifically, it provides a list of steps for how to identify and evaluate threats and vulnerabilities, control security risks, and monitor the efficacy of these controls. TIR57 builds off the principles presented in ANSI/AAMI/ISO 14971, "Medical Devices—Application of Risk Management to Medical Devices," a standard familiar to and already implemented by medical device manufacturers. ANSI/AAMI/ISO 14971 covers all risks to medical devices, whereas TIR57 highly focuses on cyber risks. Unusually, the FDA added TIR57 to its list of recognized standards less than a month after AAMI approved it internally, reflecting the need for protection of medical devices in an increasingly digitized world. A press release from AAMI states that the addition of TIR57 to the FDA's list of approved standards means that manufacturers who implement it can expect to have all the information expected by the FDA in premarket submissions.[8]

UL 2900 Series

The UL 2900 series of standards is three related documents titled Software Cybersecurity for Network-Connectable Products.[9] UL describes its 2900 series as a testing framework for manufacturers to objectively demonstrate their compliance with FDA expectations for medical device cybersecurity. It provides repeatable, reproducible, testing-oriented criteria to assess a device's cyber vulnerabilities, fight malware, and test the security measures. From a product testing perspective, UL 2900 requires all interfaces of the product and its communication channels be defined, and that security risk controls be applied in a manner consistent with product risk management principles (including those in TIR57). UL 2900 references a number of previously established product and process standards. It was built around the NIST Cybersecurity Framework and also leverages the principles of Common Criteria, which helps make it compatible for use with standards such as DTSec. UL 2900 also requires that products be evaluated for all known vulnerabilities in accordance with the National Vulnerability Database (NVD) and International Telecommunications Union (ITU) CYBEX Standards. UL 2900-1: General Requirements was adopted by the American National Standards Institute (ANSI) as a national consensus standard and added to the FDA's list of recognized consensus standards in 2017 and published in the US Federal Register.

DTSec

In 2016, Diabetes Technology Society (DTS) completed the first broad consensus cybersecurity standard with performance requirements for any medical device. Named DTSec (DTS Cybersecurity Standard for Connected Diabetes Devices),[10] the standard contains both performance requirements and assurance requirements. The goal of DTSec is to raise confidence in the security of network-connected medical devices through independent expert security evaluation. Although originally intended only for diabetes devices, DTSec can inherently be used in any medical product contributing to the protection of high value assets. Expansion of this standard to cover all medical devices will be specified in the next phase of its development. In 2017, IEEE and UL signed a Joint Standard Development agreement to develop a consensus-based standard for wireless diabetes device security based on DTSec.[11] Diabetes Technology Society turned over DTSec to these two organizations for this purpose. It will be the first standard ever co-managed by these two established standards development organizations. The goal of these two organizations is to co-manage this standard as a national document, expand it to cover all medical devices, and then elevate it to the international level.

DTMoSt

In 2017, DTS began work on its second cybersecurity standard called DTMoSt (the Diabetes Technology Society Mobile Platform Controlling a Diabetes Device Security and Safety Standard). The Steering Committee includes representatives from (1) the US government, including FDA, NIST, DHS, FBI, NIH, NASA, and DoD; (2) the Australian government; (3) professional organizations, including ADA, the Endocrine Society, and AADE; (4) Standards Development Organizations, including IEEE and UL; (5) industry, including mobile phone manufacturers, hardware and software manufacturers, medical device manufacturers, and medical device testing labs; (6) academicians from medicine, diabetes education, information technology, engineering, mathematics, and law; and (7) patients. A draft version of the standard was posted in early 2018 for public comment.

DTMoSt takes the principles of DTSec and applies them specifically to the use of mobile phones to control actions by wearable or implantable diabetes devices. The involvement of mobile phones requires special considerations because of the need for resource availability. A phone platform has other purposes than medical applications, some of which may overutilize processing power or battery. The ability to deliver real-time control of rapidly changing physiological processes can put heavy strain on a phone's operating system, leading to loss of function with severe consequences for diabetes patients. Stakeholders affected by connected medical devices will increasingly demand assurance of safe cybersecurity from health care professionals who are prescribing and overseeing

use of these products.[12] DTMoSt aims to provide assurance that off-the-shelf consumer mobile phones can safely control diabetes devices.

Comparisons/How Do They Interact?

Simplified, TIR57 is primarily a risk management document implemented during the development process, while UL 2900 is primarily a product-testing document that can be applied at all stages of a device's life cycle. The temporal scope of the former is more limited than that of the latter. For example, UL 2900 can be used not only for demonstrating that security controls have been implemented as a device nears FDA review, but also that the controls are effective and under surveillance years or even decades down the line. The emphasis on different stages of product development means that the two standards complement each other. A manufacturer could hypothetically apply TIR57 during the development cycle of a medical device and then use UL 2900 to ensure compliance with recognized cybersecurity criteria.

DTSec contains elements of both early-stage risk management and late-stage monitoring of products on the market. The first section of DTSec helps developers identify and document threats applicable to medical devices, similarly to how TIR57 provides a list of steps for how to evaluate vulnerabilities. The cornerstone of DTSec, however, is its emphasis on practical assessment of products through its Assurance Program. Rather than addressing common vulnerabilities using common testing techniques, DTSec focuses on understanding the specific threat model for a product (or similar products within a product family) and then deriving the specific security requirements the product needs to combat those threats. DTSec publicizes a list of independent, accredited labs that perform vulnerability testing consistent with ISO requirements. The goal of this testing is to ensure the product faithfully upholds its defined security requirements. Products that pass assessment receive public certification that they meet DTSec Security Targets.

The format of DTSec is unique from TIR57 and UL 2900 in that it follows a multi-stakeholder process for identifying the appropriate security requirements for specific products and then offering a program to gain assurance in those products (and those requirements) through assessment. DTSec does not prescribe the specific testing methodology used to gain assurance in the security requirements for a product. This is left flexible for the developer and the lab. DTSec is complementary to the current UL 2900 series in that UL 2900 testing can provide testing assurance artifacts that a DTSec lab can use the accelerate product evaluation. Overall, the emphasis of DTSec on cybersecurity assessment mirrors the goal of the UL 2900 series.

FDA recognition of both TIR57 and UL 2900 means that manufacturers who adhere to the guidelines can expect to have addressed all the information expected by the FDA in products submitted for approval. In this way, both documents are a link between the broad outline set by the FDA in its premarket and postmarket guidance documents and the technical, engineering details of device security. Manufacturers who elect only to use the FDA's guidance documents might have more freedom in designing and implementing cybersecurity solutions, but also face the risk that the FDA will delay or reject the approval of their product.

Finally, all three organizations (AAMI, UL, and DTS) promote their respective standards as consensus efforts. The committee of TIR57 includes almost forty representatives from industry, academia, and government agencies. UL 2900 was developed under the ANSI canvass process, establishing a national consensus body comprised of manufacturers, users, supply chain stakeholders, regulators, academia, and many others. DTSec was created by a committee of 58 representatives from academia, government agencies, industry, hospitals, and nonprofit organizations.

The Future

Recent controversies have arisen about the security of medical devices that cannot be evaluated by the public. This uncertainty can erode trust in the wireless medical device industry. Accusations of inadequacy[13] and claims of adequacy[14] regarding medical device security have been made. Often, there is no clear right or wrong answer. In this environment, independent assessment of the security of specific medical devices is necessary. DTSec, which is intended to provide such assurance, will receive an IEEE number designation and will be closely linked to the UL 2900 series. Attention to proper risk management in the architecture of medical devices per TIR 57 and the UL 2900 series, along with documentation of sound security per the principles of Common Criteria (and as applied to medical devices by DTSec) will improve the security of medical devices and will bolster the confidence of users of these products that these products meet a cybersecurity safety standard.

Abbreviations

AADE, American Association of Diabetes Educators; AAMI, Association for the Advancement of Medical Instrumentation; ADA, American Diabetes Association; ANSI, American National Standards Institute; CT, computed tomography; DHS, Department of Homeland Security; DoD, Department of Defense; DTMoSt, Diabetes Technology Society Mobile Platform Controlling a Diabetes Device Security and Safety Standard; DTSec, Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices; FBI, Federal Bureau of Investigation; FDA, Food and Drug Administration; ICU, intensive care unit; IEEE, Institute of Electrical and Electronics Engineers; ISO, International Organization for Standardization; ITU, International Telecommunications Union; MRI, magnetic resonance imaging; NASA, National Aeronautics and Space Administration; NIH, National Institutes of Health; NIST, National Institute of Standards and Technology; NVD, National Vulnerability Database; PET, positron emission tomography; TIR, Technical Information Report.

Acknowledgments

The authors thank David Kleidermacher for his helpful comments and Annamarie Sucher for her expert editorial assistance.

Declaration of Conflicting Interests

The author(s) declared the following potential conflicts of interest with respect to the research, authorship, and/or publication of this article: AF is an employee of UL. DCK is a consultant to Ascensia, EOFlow, Intarcia, Lifecare, Novo Nordisk, AstraZeneca, and Voluntis.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

1. Metivier B. Fundamental objectives of information security: the CIA triad. 2017. Available at: https://www.sagedatasecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad. Accessed February 6, 2018.
2. Sedgewick A. Framework for improving critical infrastructure cybersecurity. Version 1.0. 2014. National Institute of Standards and Technology. Available at: http://nist.gov/cyberframework/. Accessed February 19, 2017.
3. National Institute of Standards and Technology. Update to cybersecurity framework. 2017. Available at: https://www.nist.gov/news-events/news/2017/12/update-cybersecurity-framework. Accessed February 6, 2018.
4. US 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. Available at: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf. Accessed February 6, 2018.
5. US Food and Drug Administration. Postmarket management of cybersecurity in medical devices: guidance for industry and food and drug administration staff. 2016. Available at: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. Accessed February 6, 2018.
6. US Food and Drug Administration. CFR—code of federal regulations title 21. 2017. Available at: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=10.115. Accessed February 6, 2018.
7. Association for the Advancement of Medical Instrumentation. AAMI TIR57: principles for medical device security—risk management. 2015. Available at: http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729. Accessed February 6, 2018.
8. Advancing Safety in Health Technology. FDA points manufacturers to AAMI cybersecurity recommendations. 2016. Available at: http://www.aami.org/newsviews/newsdetail.aspx?ItemNumber=3719. Accessed February 6, 2018.
9. UL 2900 Standard. New standard for software cybersecurity for network-connectable products. 2017. Available at: https://industries.ul.com/blog/new-standard-for-software-cybersecurity-for-network-connectable-products. Accessed February 6, 2018.
10. Diabetes Technology Society. DTS cybersecurity standard for connected diabetes devices. 2016. Available at: https://www.diabetestechnology.org/dtsec.shtml. Accessed February 6, 2018.
11. UL Global Standards. IEEE and UL to develop a standard for wireless diabetes device security provided by DTS. 2017. Available at: https://www.ul.com/newsroom/pressreleases/ieee-and-ul-to-develop-a-standard-for-wireless-diabetes-device-security-provided-by-dts/. Accessed February 6, 2018.
12. Klonoff DC, Kerr D, Kleidermacher D. Now is the time for a security and safety standard for consumer smartphones controlling diabetes devices. *J Diabetes Sci Technol*. 2017;1(5):870-873.
13. Huntley A. St. Jude medical accused of having 'stunning' cybersecurity risk in cardiac devices. 2016. Available at: https://www.fiercebiotech.com/medical-devices/st-jude-medical-accused-stunning-cyber-security-risk-cardiac-devices. Accessed February 6, 2018.
14. McCarthy J. St. Jude fires back at muddy waters, MedSec: our medical devices are secure. 2016. Available at: http://www.healthcareitnews.com/news/st-jude-fires-back-muddy-waters-medsec-our-medical-devices-are-secure. Accessed February 6, 2018.