Journal of Diabetes Science and Technology
2016, Vol. 10(2) 435–438

DOI: 10.1177/1932296815602100
dst.sagepub.com
SAGE

Cybersecurity Regulation of Wireless Devices for Performance and Assurance in the Age of "Medjacking"

David G. Armstrong, DPM, MD, PhD[1], David N. Kleidermacher, BS[2], David C. Klonoff, MD[3], and Marvin J. Slepian, MD[4,5,6]

Abstract

We are rapidly reaching a point where, as connected devices for monitoring and treating diabetes and other diseases become more pervasive and powerful, the likelihood of malicious medical device hacking (known as "medjacking") is growing. While government could increase regulation, we have all been witness in recent times to the limitations and issues surrounding exclusive reliance on government. Herein we outline a preliminary framework for establishing security for wireless health devices based on international common criteria. Creation of an independent medical device cybersecurity body is suggested. The goal is to allow for continued growth and innovation while simultaneously fostering security, public trust, and confidence.

Keywords

cybersecurity, diabetes, medical devices, medjacking

We have recently witnessed explosive growth in our modes of social interaction as well as in our technologies of interaction. These developments have begun to impact health monitoring and delivery. Notably we have seen the rise of health-related wearable and implantable sensors, monitors and devices with wireless remote communication capabilities.[1,2] This trend toward enhanced communication and connectivity, while creating the potential for enormous health benefit, also has created the possibility for adverse outcomes. These include (1) loss of privacy, (2) identity and information theft, and (3) major security concerns. Therefore, we feel that the time is right to consider an addendum to the social contract—namely a cybercontract amendment. We propose here a new security paradigm for wireless health devices that will allow for growth and innovation, while at the same time fostering public trust and confidence.

Patients with diabetes and other diseases are adopting electronic devices for monitoring and treatment, and increasingly these devices possess wireless communication capabilities. The functions built into all medical devices must meet a high level of safety and must provide security assurance that they are free of vulnerability. Security introduces assurance challenges that extend beyond safety. A safety-critical system must prevent accidental failures, while a security-critical system must protect against attempts to inflict damage on purpose. If an electronic system has thousands of software flaws, as most do, it may be that none of these result in a *safety* failure; however any one of these flaws may be exploited by a determined attacker to breach *security*. Indeed, medical device manufacturers need to improve their security approaches to match their current safety capabilities. Assurance of cybersecurity is a process of evaluating a product according to a rigorous protocol at a level of confidence that the product performs according to its claims for its target use environment. If a product does not perform according to its cybersecurity claims, then it is risky for security breaches, and if a product is not tested with high assurance then there will not be a high degree of confidence that it provides adequate cybersecurity. Given the many recent high-profile lapses in cybersecurity reported in the media, it appears that many companies and institutions

[1]Department of Surgery, Southern Arizona Limb Salvage Alliance (SALSA), University of Arizona College of Medicine, Tucson, AZ, USA
[2]BlackBerry Limited, Pleasanton, CA, USA
[3]Diabetes Research Institute, Mills-Peninsula Health Services, San Mateo, CA, USA
[4]Departments of Medicine and Biomedical Engineering, University of Arizona, USA
[5]Arizona Center for Accelerated Biomedical Innovation (ACABI), Arizona, USA
[6]Sarver Heart Center, Arizona, USA

Corresponding Author:
David G. Armstrong, DPM, MD, PhD, Southern Arizona Limb Salvage Alliance (SALSA), University of Arizona College of Medicine, 1501 N Campbell, Tucson, AZ 85724, USA.
Email: armstrong@usa.net

cannot provide assurance that their systems are secure from cyberthreats. Therefore, robust security features (as described by a manufacturer) and a high level of assurance that these claimed features perform adequately (as certified by an impartial body) are both needed to foster confidence in the capability of a product to perform its function.

Current Governmental Regulation

Contemporary government legislation and regulations for security, such as the US Health Insurance Portability and Accountability Act (HIPAA) for health care, the Payment Card Industry security standard (PCI) for financials, and most recently the US Federal Trade Commission (FTC) guidance on the Internet of things (IoT),[3] while well-intentioned, have not yet increased the quality of security assurance. Furthermore, these basic initiatives may provide a false sense of security to consumers and developers as to prevention of major attacks. Technology companies are still able to advertise their wares as being safe in "government computing environments that demand the strictest security," while in fact they may have major vulnerabilities identified only days later.[4] In commerce and medicine, department store chain Target (PCI) and insurance company Anthem (HIPAA) are but two examples of major recent breaches in financial and health information, respectively.[5,6] Based on these real threats, the US Federal Trade Commission proposed the following recommendations:

> Companies developing IoT products should implement reasonable security
> Companies should consider how to minimize the data they collect and retain
> Companies should test their security measures before launching their products
> Companies should consider implementing reasonable access control measures
> Companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities
> Congress should enact general data security legislation[7]

Such guidance points developers in the right direction but fails to address the core challenge of *defining* the security protections required by specific medical systems and then enabling stakeholders to obtain a high level of assurance of these protections by *evaluating and certifying* them. To move us further toward effective security, we must have a common language and evaluation criteria for these activities.

The International Common Criteria and Evaluated Assurance Levels

A consortium of national governments came together in the mid 1990s to create a framework for specifying security requirements—for any electronics product, software component, or system, and for evaluating vendor claims of conformance to the requirements. The framework that the consortium developed is ISO/IEC 15408, known informally as the Common Criteria (CC),[8] which remains the only internationally accepted, generally applicable product security framework. CC has been utilized to specify a wide variety of security functionality over almost two decades. Requirements are specified in two dimensions: functional requirements cover security features of a system, while assurance requirements provide the confidence those features actually do what they claim. The selection of assurance requirements may direct the assignment of an evaluated assurance level (EAL) for the system. EALs range from 1 to 7 in increasing levels of assurance. The high EALs represent a level appropriate for protecting high value resources against sophisticated and determined attackers; EAL 4 and lower are intended to protect against nonsophisticated or inadvertent attacks against security.[9] EALs 5 and above must be designed into the system and cannot be added on later. EAL 7 assurance requirements include formal design and implementation methods and extremely rigorous testing, including vulnerability assessment at the source code level.

Government Application of ISO 15408

In 2012, after more than a decade of attempted implementation with the vast majority of evaluations performed at the lower EALs, the US government decided to do away with EALs and started publishing what can be considered EAL 0 security specifications that aim only to define security functionality, not ensure it.[10] The problem of assurance has therefore been left as an exercise for vendors, users, and system owners.[11]

In part because of the above difficulties in implementation of effective and robust security initiatives, directives and guidance by government agencies, the overall track record has contributed to a widespread perception that high assurance is prohibitively expensive, both for developers and evaluators.

Recent Medical Device Security Standards Initiatives

Security for medical devices has recently received substantial attention from government and nonprofit standards bodies. For example, in December 2014, the NIST National Cybersecurity Center of Excellence issued the "Wireless Medical Infusion Pumps" use case document in December 2014, with the goal "to help healthcare providers secure their medical devices on an enterprise network, with a specific focus on wireless infusion pumps."[12] This document provides an excellent review of the threat environment and associated security functional requirements needed for infusion pumps, but does not delve into assurance requirements nor their use

in aiding the evaluation and assessment of products claiming conformance to the security functional guidance. The need for independent assurance by evaluation is made even more apparent in light of recent documented successful hacks of medical implants termed "medjacking."[13-15]

In May 2015, IEEE issued the "Building Code for Medical Device Software Security," with the goal of "reducing the risk that software used to operate medical devices is vulnerable to malicious attacks."[16] This document discusses security functional requirements, such as software/firmware integrity and authenticity validation via digital signatures, as well as assurance requirements such as secure coding standards and the use of rigorous vulnerability analysis and testing techniques. The document does not offer an approach to independent evaluation and certification of medical devices and the requirements they claim to meet. The document's authors, however, acknowledge the importance of this problem: "For this work to have real effect, it must be carried forward by those with responsibilities for building and evaluating medical devices." This, we believe, offers a way forward.

The Diabetes Technology Society has announced a plan to develop a consensus cybersecurity standard for connected diabetes devices. We expect that both security features and assurance will be addressed. Furthermore, we believe that some of the recommended security features for diabetes-specific devices such as blood glucose monitor systems, continuous glucose monitors, insulin pumps, and closed loop systems will also apply to medical devices used for monitoring and treating other diseases.

The Way Forward

We propose that a freestanding process organized by one or more *independent, nonprofit organizations* be dedicated to developing requirements standards and testing programs for medical device cybersecurity. A parallel to this structure may be seen in the area of medical device regulation, contrasting the United States with its sole reliance on the FDA, versus Europe with its European Commission Directives and freestanding Notified Bodies.[17] Such a process would establish the metrics and standards for evaluations that then may be performed by contract third-party entities—these being subject to periodic audit for quality assurance. The organization would then certify the results of these evaluations. Another parallel model example is the creation of a sort of Underwriters' Laboratories or American Society for Testing of Materials (ASTEM)—both independent, objective organizations dedicated to unbiased analysis and recommendation and standard development.[18,19]

A freestanding cybersecurity agency would thus be best organized and governed by medical, industry, academic, and other independent subject matter experts, but without centralized control from any of these groups. Furthermore, international participation, in terms of leadership manpower and recognition of specific country issues and concerns, would bolster effectiveness. This organization would adopt a policy of continuous improvement, acknowledging the fact that assurance methods are always evolving. This organization would likely use the CC to govern specification and evaluation of security requirements. We propose an organizational focus on the standard's predefined assurance packages EAL 5 and higher or alternative assurance packages that may fit specific medical device market constraints better but still offer a similarly high assurance of protection against sophisticated attack threats. Furthermore, this organization must promote, through training, education, and evaluation methodology, the use of assurance-efficient techniques, such as automated and semiautomated formal verification, automated testing, automated vulnerability analysis, and proven-in-use measurements to ensure evaluations can be performed economically, from the perspectives of both time and money. The organization must strive for openness and transparency through public disclosure of its operations, specifications, and evaluation methodologies and results. Finally, while we have emphasized independence, still we suggest that this agency have a strong, effective liaison and relationship to government, allowing for synergistic efforts, while maintaining its value as an independent body.

This influence and reputation of this organization and process will be based on the quality of its work and adoption by users, vendors, and enterprises as the de facto standard for meaningful electronic system security. As such, assurance may be provided in the form of an independent "seal of approval."

Core tenets for such a process would be as follows:

1. Security specifications and evaluation methodologies framed by Common Criteria (ISO/IEC 15408)
2. Evaluations that target high assurance (EAL 5 and higher or similar custom assurance packages)
3. Independent, unbiased leadership with high security assurance expertise
4. International participation
5. Continuous process improvement
6. Evaluation efficiency (cost and time)
7. Openness

The proposed focus on higher assurance levels and associated evaluation is commensurate with the protection of value of resources (human life) against sophisticated, well-resourced attackers we must assume will try to circumvent those protections.

In conclusion, the rapid growth of digital technologies has both advanced medicine and society, but has also introduced new risks. Compromise of device security and the associated risk to life-critical function, intellectual property, and privacy are emerging concerns. Government efforts should continue to adapt to the rapidly emerging risk issues and concerns. However, reflection suggests that a more agile means is needed to augment efforts. An opportunity

exists for a free standing agency or agencies to be created that is independent of government administration while allowing for government influence and oversight. Creation of such a body will go far to establish and restore consumer and end user confidence, limit cyber villain efficacy, and foster innovation without fear.

Abbreviations

ASTEM, American Society for Testing of Materials; CC, international Common Criteria; EAL, evaluated assurance level; FDA, US Food and Drug Administration; FTC, US Federal Trade Commission; HIPAA, US Health Insurance Portability and Accountability Act; IEC, International Electrotechnical Commission; IEEE, Institute of Electrical and Electronics Engineers; IoT, Internet of things; ISO, International Organization for Standardization; PCI, Payment Card Industry security standard.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

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

References

1. Lee N. The Lancet technology. *Lancet*. 2015;385(9966):408.
2. Topol EJ, Steinhubl SR, Torkamani A. Digital medical tools and sensors. *JAMA*. 2015;313(4):353-354.
3. Federal Trade Commission. *Internet of things—Privacy and security in a connected world*. Washington, DC: Federal Trade Commission.
4. VMware infrastructure earns security certification for stringent government standards. United States. Available at: http://www.vmware.com/company/news/releases/common_criteria.html. Accessed February 4, 2015.
5. Riley M, Elgin B, Lawrence D, Matlack C. Missed alarms and 40 million stolen credit card numbers: how Target blew it. *Bloomberg Businessweek Technology*. 2014.
6. Reed Abelson and millions of Anthem customers targeted in cyberattack. *New York Times*. February 5, 2015. Available at: http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html
7. Federal Trade Commission status report. Privacy & security in a connected world. November 2013. Available at: http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
8. Recognition of common criteria certificates in the field of information technology security. Available at: https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf.
9. Revision V 3 1. Part 3: security assurance components. Available at: https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf.
10. FAQs28Mar_v6.pdf. Available at: https://www.niap-ccevs.org/NIAP_Evolution/faqs/niap_evolution/FAQs28Mar_v6.pdf.
11. Microsoft Word. Attachment2-SKPPSunsetFAQ _3_.DOC. Available at: http://www.niap-ccevs.org/announcements/SKPP%20Sunset%20Q&A.pdf.
12. NCCOE_HIT-Medical-Device-Use-Case.pdf. Available at: https://nccoe.nist.gov/sites/default/files/nccoe/NCCOE_HIT-Medical-Device-Use-Case.pdf.
13. The medical device hijack story you need to hear. Medical Device and Diagnostic Industry news products and suppliers. Available at: http://www.mddionline.com/blog/devicetalk/medical-device-hijack-story-you-need-know-06-09-15?cid=nl.mddi01.20150611. Accessed June 16, 2015.
14. Zetter K. Lawmakers call for probe of medical devices after researcher hacks insulin pump. *Wired*. August 19, 2011. Available at: http://www.wired.com/2011/08/medical-device-security/.
15. Klonoff DC. Cybersecurity for connected diabetes devices [published online ahead of print April 16, 2015]. *J Diabetes Sci Technol*. Available at: http://dx.doi.org/10.1177/1932296815583334.
16. Haigh T, Landwehr C. Building code for medical device software security. cybersecurity.ieee.org. Available at: http://cybersecurity.ieee.org/images/files/images/pdf/building-code-for-medica-device-software-security.pdf.
17. Regulatory framework—European Commission. Available at: http://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework/index_en.htm. Accessed February 23, 2015.
18. ASTM International Standards. Available at: https://global.ihs.com/PPC/astm.html?RID=Z56&MID=PPCT&gclid=Cj0KEQjwy7qrBRC4lp7_hM3dgIoBEiQA72pCnvwRduZjAvm-TPHw6jZP0beTumsi8OTQAx8VFotdZYw8aAhpQ8P8HAQ. Accessed June 3, 2015.
19. Underwriters Laboratories. Available at: http://ul.com/. Accessed June 3, 2015.