Journal of Diabetes Science and Technology
2015, Vol. 9(5) 1143–1147
© 2015 Diabetes Technology Society
Reprints and permissions:
sagepub.com/journalsPermissions.nav
DOI: 10.1177/1932296815583334
dst.sagepub.com
SAGE

Cybersecurity for Connected Diabetes Devices

David C. Klonoff, MD, FACP, FRCP (Edin), Fellow AIMBE[1]

Abstract

Diabetes devices are increasingly connected wirelessly to each other and to data-displaying reader devices. Threats to the accurate flow of information and commands may compromise the function of these devices and put their users at risk of health complications. Sound cybersecurity of connected diabetes devices is necessary to maintain confidentiality, integrity, and availability of the data and commands. Diabetes devices can be hacked by unauthorized agents and also by patients themselves to extract data that are not automatically provided by product software. Unauthorized access to connected diabetes devices has been simulated and could happen in reality. A cybersecurity standard designed specifically for connected diabetes devices will improve the safety of these products and increase confidence of users that the products will be secure.

Keywords

cybersecurity, diabetes, device, connected, security, hack, data

Patients with diabetes have an extremely high need for secure information flow to display glucose information and deliver insulin dosing commands when sensor and actuator information is transmitted wirelessly through connected medical devices. Therefore sound cybersecurity is needed for connected diabetes devices to maintain confidentiality, integrity, and availability of the data and commands.

Cybersecurity

Diabetes devices contain streams of personal patient information and can permit remote commands of data delivery, treatment instructions, and insulin administration. This personal information as well as the software that implements the capability of sending a remote command, and the software that accepts a remote command are all assets. Threats to these assets may degrade their function and cause the user of the diabetes device to have a health risk. Such threats can come in the form of unauthorized (1) disclosure, (2) modification, or (3) loss of function. Security is the concept of protecting assets. Cybersecurity is the concept of protecting digital assets. For medical devices cybersecurity means protection of data and command information that are transmitted wirelessly between connected medical devices. These devices include blood glucose monitors, continuous glucose monitors (CGMs), insulin pumps, other wearable sensors, cloud computer systems, and readers, such as desktop computers, laptops, pads, smartphones, and watches. Cybersecurity refers to protecting information that is being wirelessly transmitted (also known as "data in motion") as well as information that is being stored (also known as "data at rest"). The purpose of cybersecurity for connected diabetes devices is to protect these products from unauthorized disclosure, modification, and loss of function. Avoiding such disclosure preserves confidentiality, avoiding modification preserves integrity, and avoiding loss of function preserves availability.

The CIA Triad for Information Security

A principle at the core of information security for the safe utilization, flow, and storage of information is the CIA triad. CIA stands for *c*onfidentiality, *i*ntegrity, and *a*vailability. These three properties of data are the main objectives of information security.[1]

The aim of data confidentiality is to ensure that information is available only to people who are authorized to access it. To view this information, authorized users must authenticate in some way before access is granted. The method of ensuring data confidentiality is cryptography, which consists of encryption (changing the data located in files into an obfuscated form) and decryption (decoding obfuscated data back to their original form with a key or password). If the encryption and protocols are implemented correctly, then

[1]Diabetes Research Institute, Mills-Peninsula Health Services, San Mateo, CA, USA

Corresponding Author:
David C. Klonoff, MD, FACP, FRCP (Edin), Fellow AIMBE, Diabetes Research Institute, Mills-Peninsula Health Services, 100 S San Mateo Dr, San Mateo, CA 94401, USA.
Email: dklonoff@diabetestechnology.org

there is no threat to the data being decrypted without the key. In some cases, however, the software that implements the cryptography or the network protocols can introduce vulnerabilities. In reality, poorly protected data transmitted wirelessly can sometimes be illicitly captured with a sniffer tool that monitors network traffic. Also, stored data on a phone, tablet, computer, or watch can be stolen and accessed.

The aim of data integrity is to ensure that data are recorded and presented exactly as intended and in the case of a glucose monitor or insulin dosing record the data stored must be the same as what was measured. Later, upon retrieval and retrieval, the data must be exactly the same as when they were initially recorded and not altered in any way. Data integrity also includes rules defining the relations a piece of data can have to other pieces of data, such as when a time stamp is linked to a glucose value, a glucose value is linked to an insulin bolus dose, or a premeal stamp is linked to a glucose value or an insulin dose. Any unintended change to data as the result of a transmission, storage, editing, or retrieval operation is a breakdown in data integrity. One way to ensure integrity is with hashing. A hash value (or simply hash), also called a message digest, is a number generated from a string of text, which serves as a digital signature. It is affixed to a file or string of data prior to encryption. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. The hash functions in a one-way direction to create an output that cannot be inverted to identify the input. A detection system compares the hashes of the data at input and output. If the data have not changed, then the hashes will be the same, and if the hashes are different, then there has been a breach of integrity.[2]

The aim of data availability is for data to be immediately accessed. The term is sometimes also defined as the percentage of time that a system can be used for productive work. A common method of assuring availability is to build redundant systems. The relative amount of continuous glucose sensor data availability might be defined as the number of data points delivered over the anticipated lifetime of the sensor divided by the number of data points that would have been delivered over this lifetime if there had been no data dropout. As an example, if a CGM that functions from the first day though the last day of intended use is subject to data dropout on various occasions, then it will be unavailable on those occasions.[3] The manufacturer might claim that the device delivered data each day it was worn and claim 100% uptime. By the proposed definition, however, the availability was less than 100%. Furthermore, on some occasions a sensor might stop functioning hours or days before the end of its projected lifespan. The manufacturer might again claim that the device delivered data continuously until it stopped functioning at which point it was removed and that it therefore provided 100% availability. Again, by the proposed definition above, however, the availability was less than 100%. Both scenarios represent states of reduced data availability. Any time a presentation of a remotely transmitted data from a BGM or CGM is denied by an adversary, then that action is said to result in compromised availability.

Cyber Threats to Connected Medical Devices

The US Department of Homeland Security (DHS) is now looking into at least two dozen cases of possible cybersecurity flaws in medical devices.[4] The products are under review by the agency's Industrial Control Systems Cyber Emergency Response Team. DHS is concerned that an episode, like the one in the television drama *Homeland*, where the fictional vice president of the United States was killed by a cyber attack on his pacemaker,[5] could occur in real life. The agency is working with manufacturers to identify and repair software coding bugs and other vulnerabilities that hackers can potentially use to expose confidential data or attack hospital equipment. DHS said the probe was based in part on research by Barnaby Jack, a hacker who died in July 2013. Jack had said he could hack into wireless communications systems that link implanted pacemakers and defibrillators with bedside monitors.[4] Former Vice President Dick Cheney has revealed that he once feared that terrorists could use the implanted defibrillator implanted near his heart to kill him and had his doctor disable the wireless device.[6] In 2007, he asked his doctor to remove the device and replace it with one with the wireless control component removed, fearing that terrorists might gain control of it and deliver a fatal electric jolt.[7]

National security experts view cybersecurity flaws of medical devices as a credible threat. For example, to address the cybersecurity challenges of wireless infusion pumps, the National Cybersecurity Center of Excellence at the National Institute of Standards and Technology and the University of Minnesota are now collaborating on a project to secure those devices from vulnerabilities due to malware or hacking and access control.[8]

Cyber Threats to Connected Diabetes Devices

There are no known incidents of patients being harmed from hacking attacks against their medical devices. Given the unfortunate abundance of so-called softer and more catastrophic targets that are also currently poorly protected, it is unknown whether there is a terrorist threat associated with poor cybersecurity of diabetes devices. Several reports in the past few years about insulin pumps with wireless control having potential vulnerabilities have increased interest in the cybersecurity capabilities of these devices.

In August 2011 at a security conference in Las Vegas, security researcher analyst Jay Radcliffe hacked an insulin pump 150 feet away to either disable the device or cause delivery of an overdose of insulin. His demonstration required special hardware and a program that he wrote to communicate with the device. He also required knowledge of the pump's six-digit identification (ID) number, although he stated that this number could potentially be obtained by software designed for brute-force guessing or through social engineering.[9]

At security conferences in October 2011 in Las Vegas[10] and in Miami,[11] a research architect, Barnaby Jack, demonstrated that he could hack an insulin pump wirelessly to deliver a potential fatal bolus dose of insulin without first knowing the device's ID number. The wireless link had no encryption and no authentication. He developed a scanner with a high-gain antenna to boost its range and then scanned the company-designated frequency for a pump, retrieved the target pump's ID, and gained control. Jack instructed the target pump to deliver its maximum dose of 25 units into a test bench, but first substituted dye for insulin. At a security conference in February 2012 in San Francisco,[12] Jack again wirelessly hacked into an insulin pump that was placed in a see-through mannequin, this time from 300 feet away. His software stole the pump's security credentials and had it empty all its contents into the mannequin. It is not known whether these types of incidents have been corroborated by other independent researchers.

Do-It-Yourself Hacking

Diabetes devices can be hacked not only by unauthorized agents but by patients themselves to extract data that are not automatically provided by products' software. The current do-it-yourself movement by patients and caregivers intends to deliver improved access to (1) diabetes data for constructive purposes, such as obtaining integrated data across devices from multiple manufacturers, and (2) better or even simply different tools for data visualization. There is an essential conflict between the desire to have greater access to data and the need to protect such data from unauthorized access for malicious purposes. The Nightscout project is an effort of patients to hack their own Dexcom CGMs. Nightscout is an open source, do-it-yourself project that provides real-time access to a Dexcom CGM from web browsers through smartphones, computers, tablets, and the Pebble smartwatch. The goal of the project is to allow remote monitoring of glucose levels of diabetes patients with existing monitoring devices.[13] This movement may have been launched to access Dexcom data and create a product similar to the Medtronic MySentry. Initially, a father used the USB interface of his CGM to obtain real-time remote readings of his child's glucose levels uploaded to the cloud. Eventually other software engineers joined in and shared source code to have CGM data transmitted to wearable devices.[14] The group, eventually known as Nightscout, estimates that over 1000 copies of homemade source code for this process have been downloaded.[15] These developers claim that this code is being regularly improved through an open-source development model. This system is not cleared by the FDA. Although this patient-driven project is part of an emerging do-it-yourself movement of patient empowerment, CGM-using patients are at risk if the hacked data should lack proper confidentiality, integrity, or availability, or if the software is subject to lack of safety for any other reason. CGM-wearing diabetes patients might be at risk of acute complications if their hacking software should have any safety issues. Do-it-yourself medical software like Nightscout (compared to FDA-regulated medical software) in some cases might be unsafe if it does not (1) provide support in case of problems; (2) undergo adequate testing, repair, and redistribution of updates to users if a flaw is discovered; (3) contain sufficient confidentiality features to preserve privacy; or (4) designate a responsible party to manage the response to a problem. At least two do-it-yourself movements are now working on closed-loop systems, which are potentially even more risky because they manage both CGM data as well as insulin dosing commands. These movements include DIYPS[16] and the #OpenAPS project.[17] The dangers posed to patients from the do-it-yourself artificial pancreas may not be from individuals with malice, but rather from users with an excess of enthusiasm and a shortage of knowledge and experience.

Responding to Cyber Threats to Connected Diabetes Devices

Many types of cyber threats have been in the news recently.[18] On February 10, 2015, the Obama administration announced formation of a new agency that will integrate intelligence about cyber threats, provide analyses to policy makers and enhance the work of existing federal cybersecurity centers and others in response to the rising frequency, scale, sophistication and severity of cyber attacks. The new Cyber Threat Intelligence Integration Center, which will be under the Director of National Intelligence, will be modeled after the National Counterterrorism Center.[19]

Medical cybersecurity is also becoming an important issue for FDA and DHS, which are working together to prevent medical systems and implanted devise from being hacked.[20] On June 13, 2013, the FDA issued a statement on the topic: "We recommend that manufacturers review their cyber-security practices and policies to assure that appropriate safeguards are in place to prevent unauthorized access or modification to their devices."[21]

It is important for cybersecurity regulators to carefully consider the potential risks and benefits of proposed solutions to cybersecurity risks for patients with diabetes. These devices that collect and manage diabetes data are increasingly becoming connected with cloud storage, personalized website for offline review and downloading, real-time transmission to various wearable or portable readers through the use of mobile medical applications, and real-time decision support software. A challenge for diabetes device developers is that although data must be protected, in many cases data are now intended to be made available to not only patients, but also relatives, health care providers, and hospitals. Patients with diabetes have a special need for impeccable data fidelity when they access their current glucose levels, glucose trend data, predictive data, insulin dosing records, hypoglycemia alerts, hyperglycemia alerts, blood pressure records, calorie information exercise records, and various reminders and timely notifications. Everything about the importance of robust cybersecurity that is true for medical devices in general is particularly true for diabetes devices.

To address the aspect of the security of insulin pump systems, in 2011 Kohno, Paul, and I reviewed the security of these devices. We recommended five features that would lead to robust cybersecurity for these devices. These include (1) constant availability of access to systems; (2) confidentiality of information; (3) integrity without alteration of data; (4) authentication for privileged access; and (5) authorization of identity before execution of commands.[22]

Cybersecurity Standard for Connected Diabetes Devices

On October 2, 2014, the FDA released an important cybersecurity guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."[23] This guidance clearly described guiding principles for sound cybersecurity practices and how to work with FDA to get products cleared when they contain cybersecurity features. The document, which covers all medical devices, was not intended to be the final word for diabetes devices. Based on the special needs for real-time data confidentiality, integrity, and availability, there is now a need for a cybersecurity standard for connected diabetes devices. This standard will need to address how to identify threats, how to mitigate threats, and how to deal with threats after they have been identified for the types of connected devices used by people with diabetes. A Cybersecurity Standard for Connected Diabetes Devices Program is needed. Such a program would bring together leading experts in diabetes and cybersecurity from the academic, government, and private sectors. The goal would be to develop a standard to harmonize technical specifications, rules, methods, and definitions of diabetes devices related to cybersecurity and to reassure patients that these products are safe. Regarding safety interventions, it is usually better to act too early than too late.

Assurance—The Next Frontier After Standards

No matter how much safety is built into a standard, cleared products on the market do not always meet standards for which they were approved. Despite rigorous premarket evaluation against a standard, what really counts is how well a medical device works when it is actually used.[24] This is why postmarket surveillance is important to assure high quality of cleared devices. The best way to assure cybersecurity of diabetes devices is to both: (1) mandate a level of performance at the front end such that failure to attain this performance would lead to adverse regulatory or economic consequences; and (2) test the product in a postmarket surveillance program at the back end to ensure that the device is continuing to maintain its initial level of performance. Since 2012 FDA has been moving toward development of a medical device postmarket surveillance system. On February 23, 2015 the Engelberg Center for Health Care Reform at the Brookings Institution (under a cooperative agreement with FDA) published a report recommending a pathway to achieving such a system.[25] The new Cybersecurity Standard for Connected Diabetes Devices will provide maximal value if it can link with a surveillance program to provide assurance that the performance of a connected device is demonstrably compliant with that standard.

Abbreviations

CIA, confidentiality, integrity, availability; CGM, continuous glucose monitor; DHS, US Department of Homeland Security; FDA, US Food and Drug Administration; ID, identification.

Declaration of Conflicting Interests

The author declared the following potential conflicts of interest with respect to the research, authorship, and/or publication of this article: DCK is a consultant for Google, Insuline, Lifecare, Novartis, Roche, Sanofi, Tempramed, and Voluntis. He is also a stockholder in Tempramed.

Funding

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

References

1. Perrin C. The CIA triad. June 30, 2008. Available at: http://www.techrepublic.com/blog/it-security/the-cia-triad/. Accessed March 30, 2015.
2. Gibson D. Understanding the security triad (confidentiality, integrity, and availability). May 27, 2011. Available at: http://www.pearsonitcertification.com/articles/article.aspx?p=1708668. Accessed March 30, 2015.
3. Baysal N, Cameron F, Buckingham BA, et al. A novel method to detect pressure-induced sensor attenuations (PISA) in an artificial pancreas. *J Diabetes Sci Technol*. 2014;8(6):1091-1096.
4. Finkle J. U.S. government probes medical devices for possible cyber flaws. October 22, 2014. Available at: http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022. Accessed March 30, 2015.
5. Churnin N. "Homeland" followup: can your pacemaker be hacked? December 3, 2012. Available at: http://healthblog.dallasnews.com/2012/12/homeland-follow-up-can-your-pacemaker-be-hacked.html/. Accessed March 30, 2015.

6. Daily Mail Reporter. Dick Cheney reveals he feared terrorists would kill him by staging Homeland-style attack on his pacemaker. October 18, 2013. Available at: http://www.dailymail.co.uk/news/article-2466951/Dick-Cheney-reveals-feared-terrorists-kill-staging-Homeland-style-attack-pacemaker.htm.
7. Porter T. Dick Cheney had heart device replaced over fears of homeland style terrorist attack. October 19, 2013. Available at: http://www.ibtimes.co.uk/dick-cheney-heart-attack-terrorist-homeland-pacemaker-515159. Accessed March 30, 2015.
8. National Institute of Standards and Technology. Cybersecurity center invites feedback on securing medical devices. December 22, 2014. Available at: http://www.nist.gov/itl/pumps-122214.cfm. Accessed March 30, 2015.
9. Kaplan D. Black hat: insulin pumps can be hacked. August 4, 2011. Available at: http://www.scmagazine.com/black-hat-insulin-pumps-can-be-hacked/article/209106/. Accessed March 30, 2015.
10. Stilgherrian (CSO Online). Lethal medical device hack taken to next level: attacker sniffs insulin pump ID, delivers fatal dose. October 21, 2011. Available at: http://www.cso.com.au/article/404909/lethal_medical_device_hack_taken_next_level/. Accessed March 30, 2015.
11. Goodin D. Insulin pump hack delivers fatal dosage over the air: sugar blues, James Bond style. October 27, 2011. Available at: http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/. Accessed March 30, 2015.
12. Parmar A. Hacker shows off vulnerabilities of wireless insulin pumps. March 1, 2012. Available at: http://medcitynews.com/2012/03/hacker-shows-off-vulnerabilities-of-wireless-insulin-pumps. Accessed March 30, 2015.
13. Nightscout #WeAreNotWaiting. Available at: http://www.nightscout.info/. Accessed March 30, 2015.
14. Hurley D. Diabetes patients are hacking their way to a bionic pancreas. December 24, 2014. Available at: http://www.wired.com/2014/12/diabetes-patients-hacking-together-diy-bionic-pancreases/. Accessed March 30, 2015.
15. DIYPS.org. With #DIYPS, #WeAreNotWaiting to make the world a better place. March 26, 2015. Available at: http://diyps.org/. Accessed March 30, 2015.
16. Ramirez E. Do it yourself diabetes. February 17, 2015. Available at: http://quantifiedself.com/2015/02/diy-diabetes/. Accessed March 30, 2015.
17. Lewis D. Introducing the #OpenAPS project. February 4, 2015. Available at: http://openaps.org/introducing-the-openaps-project/. Accessed March 30, 2015.
18. Perakslis ED. Cybersecurity in health care. *N Engl J Med*. 2014;371(5):395-397.
19. Sarkar D. Obama administration to form new agency to help fight cyber threats, attacks. February 10, 2015. Available at: http://www.fiercegovernmentit.com/story/obama-administration-form-new-agency-help-fight-cyber-threats-attacks/2015-02-10. Accessed March 30, 2015.
20. Horowitz BT. FDA, DHS warn medical device makers, hospitals on cyber-threats. June 15, 2013. Available at: http://www.eweek.com/security/fda-dhs-warn-medical-device-makers-hospitals-on-cyber-threats. Accessed March 30, 2015.
21. US Food and Drug Administration. Cybersecurity for medical devices and hospital networks: FDA safety communication. June 13, 2013. Available at: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm. Accessed March 30, 2015.
22. Paul N, Kohno T, Klonoff DC. A review of the security of insulin pump infusion systems. *J Diabetes Sci Technol*. 2011;5(6):1557-1562.
23. 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. October 2, 2014. Available at: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf. Accessed March 30, 2015.
24. Shuren J, Gross TP. Moving toward a national medical device postmarket surveillance system. February 23, 2015. Available at: http://blogs.fda.gov/fdavoice/index.php/2015/02/moving-toward-a-national-medical-device-postmarket-surveillance-system/?source=govdelivery&utm_medium=email&u=email&utmtm_source=govdelivery. Accessed March 30, 2015.
25. Brookings Institution. Strengthening patient care: building a national postmarket medical device surveillance system. February 2015. Available at: http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM435112.pdf. Accessed March 30, 2015.