PERSPECTIVE

Cybersecurity in Artificial Pancreas Experiments

Derek T. O'Keeffe, MB, BCh, BAO, BEng, MEng, PhD,¹ Spyridoula Maraka, MD,¹
Ananda Basu, MD,¹ Patrick Keith-Hynes, PhD,² and Yogish C. Kudva, MD¹

Abstract

Medical devices have transformed modern health care, and ongoing experimental medical technology trials (such as the artificial pancreas) have the potential to significantly improve the treatment of several chronic conditions, including diabetes mellitus. However, we suggest that, to date, the essential concept of cybersecurity has not been adequately addressed in this field. This article discusses several key issues of cybersecurity in medical devices and proposes some solutions. In addition, it outlines the current requirements and efforts of regulatory agencies to increase awareness of this topic and to improve cybersecurity.

COMMERCIAL MEDICAL TECHNOLOGIES developed from basic medical device experiments have already improved the health of millions of patients, and such research continues to create the next generation of medical devices. As an example, several recent studies have shown the clinical benefit of the artificial (closed-loop/bionic) pancreas (AP) over conventional treatment.¹ These experiments typically involve one or more off-the-shelf continuous glucose monitors, fingerstick blood glucose devices, and insulin pumps controlled by investigational safety and control algorithms running on mobile computing platforms (laptop/tablet/smartphone) and operating over wireless networks under local or remote medical supervision. Because an AP is a safety-critical embedded system that may be the target of security threats ranging from retrieval of personal information to device manipulation, a proactive approach to system security is a prudent strategy. We propose that the security vulnerabilities of medical device technology need to be better addressed by clinical researchers, funding agencies, regulators, and journal editors. To date, there has been insufficient focus on medical device cybersecurity in the academic and clinical literature.

Many experimental AP systems include devices that may not have been designed to work in such configurations, and when they are used in this manner, the clinical research community should be cognizant of the potential security dangers to their subjects. Indeed, in February 2013, President Obama issued an executive order (13636) and a presidential policy directive to reduce cybersecurity risk to critical infrastructure, including medical devices. Regulatory agencies such as the Food and Drug Administration (FDA) have pri-

marily been concerned with safety and efficacy, although with the proliferation of wireless medical device technology, security has rapidly emerged as a regulatory issue. The FDA has produced Investigational Device Exemption guidelines specifically for AP systems. This Investigational Device Exemption document highlights that as part of the communication pathway device description, any wireless security protocols used should be stated.

Although these documents highlight some of the key concepts of cybersecurity (e.g., identify, protect, detect, respond, and recover), they do not, for example, specify a minimum standard of encryption that should be achieved. Furthermore, because these are guidelines, not regulations, the responsibility is often on the clinical research group/company to ensure that best practice is followed while testing novel algorithms/hardware architectures in AP experiments. Nevertheless, they are a welcome and important step forward in highlighting the myriad cybersecurity issues of medical devices.

Cybersecurity concerns can be external (e.g., wireless vulnerability) or internal (e.g., software integrity). It should be noted that all electronic devices, including AP systems, are potentially susceptible to electromagnetic wave interference, and therefore extra caution should be used when operating them in electromagnetic wave interference-rich environments, such as in the vicinity of X-ray computed tomography scanners. Wireless attacks can be passive (eavesdropping [i.e., collecting data and then nefariously using this information] [e.g., a hypoglycemia event]) or active (taking control of the device) and are most likely to occur when vulnerable devices have telemetry enabled for data sharing

¹Division of Endocrinology, Mayo Clinic, Rochester, Minnesota.

²Center for Diabetes Technology, University of Virginia, Charlottesville, Virginia.

TABLE 1. IEEE-11073 STANDARDS FOR PERSONAL HEALTH DEVICES: ARTIFICIAL PANCREAS COMPONENTS

<i>Device</i>	<i>Standard</i>	<i>Status</i>
Glucose meter	IEEE-11073-10417	Approved
CGM	IEEE-11073-10425	Approved
Insulin pump	IEEE-11073-10419	Under development

CGM, continuous glucose monitor.

or wireless control. The goals of a medical device security system are to prevent unauthorized access to devices as well as to reduce the potential negative effects of such intrusions should they occur. Medical device software can be designed to be robust in the face of data corruption, whether accidental or intentional, and medical device networks can use redundant safety layers in order to minimize the impact of an attack on any one element.

Consider the wireless link between a continuous glucose monitor and the microcontroller unit in an AP system; if the link is not encrypted, it may be possible to introduce erroneous data to the target device. Deliberately wrong (high) glucose data sent to an unprotected mobile computing platform may cause the algorithm to deliver excessive insulin, whereas incorrect low glucose values could cause it to deliver too little. Link encryption provides protection against the introduction of false data, whereas intelligent safety algorithms, informed by additional data such as insulin delivery history and located on both the microcontroller unit and the insulin pump, could enable the overall system to detect and reject false data values should they be introduced. Many AP devices communicate using standard wireless technologies such as Bluetooth® (Bluetooth SIG, Kirkland, WA) and Bluetooth low-energy. Some, such as certain insulin pumps, already use data encryption and obscuring to defend against link tampering, but others use simple open networks. It is encouraging that the Artificial Pancreas Standards and Technical Platform Project, funded by the JDRF, is developing interoperability diabetes device communication standards, which will hopefully address wireless security as part of its research effort (Table 1).²

Internal security threats include malware (e.g., viruses, spyware, worms, trojans), which are ubiquitous, even on hospital computers,³ and may be a threat to medical devices.

For example, this malware could collect and transmit personal patient information or, if the computer is controlling a medical device (e.g., magnetic resonance imaging device), may interfere with its correct operation. This threat may be reduced by simple procedures such as restricting the software loaded on microcontroller unit devices to packages that have been prescreened and tested. The global move toward the Internet of Things, which connects disparate devices into a unified mesh of interchangeable information, while offering great promise, must also be tempered with healthy concern. As has been previously reported, vulnerability researchers have already successfully compromised a variety of medical technologies from cardiac devices (e.g., defibrillators) to insulin pumps.³ Medical devices are becoming more networked, but in some cases security procedures are not keeping pace, or users may not be aware of how to use them effectively.

We propose that the current ad hoc approach to reporting the AP technical characteristics and performance needs to become more formalized to focus clinical researchers, regulators, funding agencies, and journal editors on these important issues. We reviewed all (33) of the key AP study articles and supplementary materials (2010–2013) as described by Doyle et al.¹ and found that none of them or subsequent publications documented the wireless security status of their experimental set-up (Supplementary Table S1; Supplementary Data are available online at www.liebertonline.com/dia). The already rich ecosystem of integrated wireless experimental medical devices will no doubt soon expand to include watches, heart rate monitors, and activity monitors—giving rise to additional vulnerabilities, of which clinical researchers should be aware.

We suggest that the technology used in a study should be reported in a manner similar to the statistics section of a journal article in which the mathematical tools and software used are clearly documented. This section would broadly describe the devices, software, and wireless protocols used in the study and state how security concerns were addressed. Understandably, a balance needs to be struck between this technology reporting and providing too much information, which may compromise proprietary knowledge and unintentionally benefit potential hackers with malicious intent. Perhaps authors could simply state that their experimental hardware is in compliance with regulatory agency cybersecurity standards.

TABLE 2. FOOD AND DRUG ADMINISTRATION CYBERSECURITY GUIDELINES

<i>Aspect</i>	<i>Concepts</i>
General principles	Identification of assets, threats, 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 Assessment of residual risk and risk acceptance criteria
Core functions	Identify, protect, detect, respond, and recover
Documentation	Hazard analysis Traceability matrix Software update strategy Software integrity controls Environment use recommendations
Recognized standards	Information technology and medical device security consensus standards

National Cybersecurity Awareness Month (#NCSAM) is observed every October and is designed to engage, educate, and raise awareness about potential cyber threats. On October 2, 2014, cybersecurity guidelines for medical devices were released by the FDA (Table 2) outlining the Administration's expectations for cybersecurity risk management in premarket submissions.⁴

As part of this #NCSAM campaign, the FDA in collaboration with the Department of Homeland Security and the Department of Health and Human Services recently convened a public workshop entitled "Collaborative Approaches for Medical Device and Healthcare Cybersecurity."⁵ This forum brought together the major stakeholders (e.g., medical device companies, clinical researchers, funding agencies, etc.) to highlight, identify, and address the challenges of medical device cybersecurity.

While we acknowledge a balance has to be struck between regulation and innovation, subject privacy and safety are paramount and the main concerns considered by Institutional Review Boards. We believe that implementing basic wireless encryption protocols, restricting the software loaded on mobile computing platform hardware, and, most importantly, documenting the cybersecurity status in the published manuscript will be an important first step.

Acknowledgments

A.B. and Y.C.K. are supported by grant DK85516 from the National Institutes of Health.

Author Disclosure Statement

No competing financial interests exist.

References

1. Doyle FJ, Huyett LM, Bok Lee J, Zisser HC, Dassau E: Closed-loop artificial pancreas systems: engineering the algorithms. *Diabetes Care* 2014;37:1191–1197.
2. Picton PE, Yeung M, Hamming N, Desborough L, Dassau E, Cafazzo JA: Advancement of the artificial pancreas through the development of interoperability standards. *J Diabetes Sci Technol* 2013;7:1066–1070.
3. Maisel WH, Kohno T: Improving the security and privacy of implantable medical devices. *N Engl J Med* 2010;362:1164–1166.
4. Food and Drug Administration: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices—Guidance for Industry and Food and Drug Administration Staff. www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf (accessed March 1, 2015).
5. Public Workshop—Collaborative Approaches for Medical Device and Healthcare Cybersecurity, October 21–22, 2014, Arlington, VA. www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm (accessed March 1, 2015).

Address correspondence to:

Yogish C. Kudva, MD

Division of Endocrinology

Mayo Clinic

200 First Street NW

Rochester, 55905 MN

E-mail: kudva.yogish@mayo.edu