JOURNAL OF THE AMERICAN COLLEGE OF CARDIOLOGY VOL. ■, NO. ■, 2018

PUBLISHED BY ELSEVIER

CARDIOVASCULAR MEDICINE AND SOCIETY

Cybersecurity for Cardiac Implantable Electronic Devices

What Should You Know?

Adrian Baranchuk, MD,[a] Marwan M. Refaat, MD,[b] Kristen K. Patton, MD,[c] Mina K. Chung, MD,[d] Kousik Krishnan, MD,[e] Valentina Kutyifa, MD, PhD,[f] Gaurav Upadhyay, MD,[g] John D. Fisher, MD,[h] Dhanunjaya R. Lakkireddy, MD,[i] from the American College of Cardiology's Electrophysiology Section Leadership

ABSTRACT

Medical devices have been targets of hacking for over a decade, and this cybersecurity issue has affected many types of medical devices. Lately, the potential for hacking of cardiac devices (pacemakers and defibrillators) claimed the attention of the media, patients, and health care providers. This is a burgeoning problem that our newly electronically connected world faces. In this paper from the Electrophysiology Section Council, we briefly discuss various aspects of this relatively new threat in light of recent incidents involving the potential for hacking of cardiac devices. We explore the possible risks for the patients and the effect of device reconfiguration in an attempt to thwart cybersecurity threats. We provide an outline of what can be done to improve cybersecurity from the standpoint of the manufacturer, government, professional societies, physician, and patient. (J Am Coll Cardiol 2018;■:■–■) © 2018 by the American College of Cardiology Foundation.

The Internet of things (IOT) is the connected communication medium in which we all live. IOT brought our professional and personal lives onto a singular platform. The ability to control so many aspects of modern existence with the click of a button on your smart device is efficient and useful, but it comes with a price. IOT security concerns have been a persistent issue, particularly in technologically adept communities, but the explosion of connected devices used in everyday life has markedly increased the risks of inadequate cybersecurity. Hacking is defined as unauthorized access to a computer system to gain information or create problems within the system (1). At present, computer-savvy hackers have intruded into most areas of the IOT space. A Google search of "hacking + [devices such as refrigerators, baby monitors, TVs]" provides multiple interesting and/or concerning results (1,2). This brief perspective from the American College of Cardiology's Electrophysiology Council is intended

The views expressed in this paper by the American College of Cardiology's (ACC's) Electrophysiology Section Leadership Group do not necessarily reflect the views of the *Journal of the American College of Cardiology* or the ACC.

From the [a]Electrophysiology Section, Division of Cardiology, Queen's University, Kingston, Ontario, Canada; [b]Electrophysiology Section, Division of Cardiology, American University of Beirut, Beirut, Lebanon; [c]Electrophysiology Section, Division of Cardiology, University of Washington, Seattle, Washington; [d]Electrophysiology Section, Division of Cardiology, Department of Cardiovascular Medicine, Heart & Vascular Institute, Cleveland Clinic, Cleveland, Ohio; [e]Electrophysiology Section, Division of Cardiology, Rush University Medical Center, Chicago, Illinois; [f]Electrophysiology Section, Division of Cardiology, University of Rochester Medical Center, Rochester, New York; [g]Electrophysiology Section, Division of Cardiology, University of Chicago, Chicago, Illinois; [h]Electrophysiology Section, Division of Cardiology, Albert Einstein College of Medicine, New York, New York; and the [i]Electrophysiology Section, Division of Cardiology, University of Kansas, Kansas City, Kansas. Dr. Chung has received honoraria from UpToDate; has received research support from Zoll; and has served on the EPIC Alliance steering committee for Biotronik (uncompensated). Dr. Krishnan has served as a clinical trial principal investigator for St. Jude Medical. Dr. Kutyifa has received research grants from Boston Scientific and Zoll. Dr. Upadhyay has received research support from Medtronic and Biotronik. Dr. Fisher has served as a consultant to Medtronic; and has received fellowship support from Medtronic, Abbott, and Biotronik. Dr. Lakkireddy has served as a speaker for Janssen, Pfizer, and Biotronik; and has received unrestricted research grants from Bristol-Myers Squibb and Biosense Webster. All other authors have reported that they have no relationships relevant to the contents of this paper to disclose.

Manuscript received October 18, 2017; revised manuscript received December 15, 2017, accepted January 10, 2018.

ISSN 0735-1097/$36.00 https://doi.org/10.1016/j.jacc.2018.01.023

ABBREVIATIONS AND ACRONYMS

CIED = cardiovascular implantable electronic device

FDA = Food and Drug Administration

IOT = Internet of things

to clarify issues that have recently arisen with respect to cybersecurity in cardiovascular implantable electronic devices (CIEDs).

CYBERSECURITY IN MEDICAL DEVICES

A global definition of cybersecurity includes "the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption" (3). In the medical field, cybersecurity refers specifically to the integration of medical devices, computer networks, and software (1). True cybersecurity begins at the point of designing protected software from the outset, and requires the integration of multiple stakeholders, including software experts, security experts, and medical advisors (1–3). Common reasons for hacking and modes of attack are summarized in the **Central Illustration**.

Many different medical devices have been targets of hacking for over a decade. Outside of the CIED world, some of the more notable are:

- Insulin pump hacking: a remote "hacking attack" was publicly demonstrated in both a Medtronic device (4) and a Johnson & Johnson device (5); and
- Drug infusion pumps.

The increasing number of medical devices using software has created a new cybersecurity concern in the medical industry—how can we protect devices from intentional harmful interference in their normal functioning (1)? Advanced wireless communications between health care providers and patients' devices have created the possibility of manipulating the normal interactions, including deactivating features; delaying, interfering, or interrupting communications; and altering programming. This poses a potential risk to clinical care, as patients could be harmed by the action of a malignant or inadvertent deleterious change in programming by the "hackers" (2).

CYBERSECURITY ISSUES IN CIEDs. In August of 2016, Muddy Waters Research LLC released a short-sell report maintaining that CIEDs manufactured by St. Jude Medical (now Abbott) were at high risk for medical device hacking (6). The report, written in collaboration with MedSec (Miami, Florida), a cybersecurity research firm focused on health care, details 2 types of cybersecurity breach, using screenshots as evidence: a "crash attack" leading to high rate pacing, and a battery drain attack (6). A major claim was that radiofrequency telemetry with the Merlin@home remote monitoring system (St. Jude Medical, now Abbott, St. Paul, Minnesota) was rendered incapable of communication after bombardment with radio traffic. An attempt to reproduce the "Muddy Waters" conditions by a group of researchers failed to produce any clinical harm; although telemetry could be inhibited, presumably to protect battery, there was no effect on essential device function (7). The motivation for the study and release of information does not appear to have been focused on patient safety, based on the public release of information without informing either the Food and Drug Administration (FDA) or the manufacturer prior to releasing the report (7). However, a warning letter was issued by the FDA (8) to Abbott urging the firm to increase cybersecurity based on the Muddy Waters report and the detection of areas of vulnerability in their remote monitoring system. Although the weaknesses in the integrity of cybersecurity for medical devices is obvious, its perceived effect on patients' safety by all "key players" (device industry, software designers, security researchers, agencies, and clinical health care providers) has not been the same.

POTENTIAL CLINICAL CONSEQUENCES OF PACEMAKER HACKING. Patient safety issues with respect to pacemakers are largely confined to those resulting from oversensing or the potential of sudden battery depletion (**Table 1**). As happens with other causes of electromagnetic interference (radiation therapy, electrocautery, and welding) the detection of signals of noncardiac origin may inhibit pacing, inducing prolonged periods of asystole with the consequent risk of syncope or sudden death. Sudden battery depletion is also most clinically relevant in a pacing-dependent patient.

POTENTIAL CLINICAL CONSEQUENCES OF IMPLANTABLE CARDIOVERTER-DEFIBRILLATOR HACKING. Security vulnerabilities exist in all software. The same areas of vulnerability in pacemakers also apply to implantable cardioverter-defibrillators. Interrupting wireless communications (remote monitoring) would be possible for a hacker operating in the same radiofrequency as the medical device, and interruption of communication would inhibit the value of telemonitoring and allow any clinically relevant events to go undetected by the system. In a pacing-dependent patient with an implantable cardioverter-defibrillator, oversensing may inhibit pacing. In addition, oversensing may result in inappropriate and even life-threatening shocks. If reprogramming was performed, disabling therapies (antitachycardia pacing and shocks) would result in no response from the device upon clinical life-threatening ventricular tachycardias. Inducing