A Matter of Life or Death

Analyzing Vulnerabilities in the Connected Medical Device Industry

Erika Batiz

COMP 116 Final Paper

Professor Ming Chow

Fall 2017

1. Abstract

The medical device industry, though often considered conservative and slow-moving due to regulations, has not been an exception to the technological breakthroughs and disruptions experienced by other industries. Innovative electronic medical devices, along with their promises of improving the quality of patient's lives or even saving them, continue to be brought to market. The global electronic medical device market is expected to reach an estimated $398 billion[1] in 2017, with projections of further growth in the coming years. Yet with the increased adoption and proliferation of these devices, efforts to ensure their security have not kept pace. This paper has two parts: part one examines weaknesses in the market for implanted and otherwise patient-focused devices, utilizing the recent case study of vulnerabilities in Abbott's (formerly St. Jude Medical's) implantable cardiac devices and their wireless transmitter. Part two then discusses industry and regulatory responses thus far, the improvements they have made, and where they have fallen short. It ultimately pulls together the various recommendations and suggestions into one cohesive section on specific actions that can be taken moving forward.

2. Introduction

Connected medical devices are introduced to the public with exciting promises of improving the quality of patients' lives, if not saving them. Some examples of recent radio frequency or wireless consumer devices include neuro stimulators, cardiac devices, continuous glucose monitors, insulin pumps, and internal infusion pumps. There has been a vast increase in networked or cabled devices in clinical settings as well, such as external

[1] Visiongain. "The Global Medical Devices Market Will Reach $398.0bn in 2017 - Press Release - Market Research Reports."

infusion pumps, radiological machines, and monitoring devices.[2] Taking all of this into consideration, it becomes clear that these devices, while having positive effects on patients' lives, are also expanding the threat landscape in the healthcare industry and adding to the number of attack vectors. They are drastically raising the stakes, creating the potential for very serious consequences if the current trajectory is not shifted by prioritizing a focus on their security.

3. To the Community: Importance of Prioritizing Security in Device Development

Breaches and cyberattacks on the ever-expanding web of internet-connected products already occur at a substantial rate. These have historically been problematic for consumer privacy and led to larger-scale issues, such as the creation of botnets. The rise of connected medical devices, however, comes with its own set of security vulnerabilities – only these are now beginning to include the potential for truly life and death consequences. Connected medical devices are creating countless new opportunities for cyberattacks on various facets of the healthcare industry, at a time when there are already existing security weaknesses that are also competing for healthcare providers' attention. Yet there is significant pressure on producers from multiple fronts to continue, or even increase the speed of, the development of these devices.

On one side, governmental agencies and policies are pushing for improved cohesiveness and communication across the industry. This includes increased interoperability between devices and the medical environments into which they are brought[3], as well as further information sharing between healthcare providers. On the

[2] Kube, Nate. "Connected Medical Devices—An Expanding Threat Landscape."
[3] FDA, Center for Devices and Radiological Health. "Digital Health - Medical Device Interoperability."

other side, there is consumer demand for devices that utilize cutting-edge technology and are brought to market quickly, so those who are already facing health problems can hopefully have a chance to benefit from them. Confronted by this pressure, device makers may decide to forgo rigorous security measures as a way to save time and resources. This decision is additionally compounded by deficient regulatory guidance for security measures that must be taken, and the absence of historical precedence for the integration of connected devices – as opposed to other areas of the healthcare industry that are driven by innovation, such as pharmaceuticals.

4. Consequences of Connected Device Vulnerabilities

Concerns about the safety and security of connected medical devices are not new; for example, former Vice President Dick Cheney revealed in an interview that he had his doctors disable the wireless capabilities of his pacemaker when it was implanted in 2007.[4] However, a recent case that began unfolding in the late summer of 2016 and carried on for about a year, provides a robust, fascinating lens through which to examine the complex questions and potential ramifications of security weaknesses in implanted, connected medical devices.

Pacemakers that were produced by St. Jude Medical at that time (the company has since been acquired by Abbott Laboratories) were found to have vulnerabilities that, if successfully exploited, could "allow a nearby attacker to gain unauthorized access to a pacemaker and issue commands, change settings, or otherwise interfere with the intended function of the pacemaker."[5] The US Food and Drug Administration (FDA) became involved

[4] Kloeffler, Dan, and Alexis Shaw. "Former Vice President Dick Cheney Feared Pacemaker Hacking."
[5] ICS-CERT. "Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities."

in the investigation and ultimately in August 2017, a recall was issued for the devices stating that the devices must be given an update to protect them against the grave vulnerabilities. As they were embedded inside of their users, this meant a home visit by a doctor or a trip to the hospital for nearly half a million patients in order to have the firmware patch applied via radio frequency.[6] Once updated, any external device trying to communicate with the pacemaker would require authorization, and it also introduced data encryption and the ability to disable network connectivity.

This single case encompasses some of the most critical questions in security today, including how disclosure should be handled and security design flaws in both hardware and software. There is also the consideration of the potentially disastrous consequences due to the exploitation of a healthcare system that is growing increasingly interconnected through hospital networks, smartphones, the Internet, and medical devices – both implanted as well as their bedside or external components. Furthermore, the problems with Abbott's pacemakers were discovered by an outside group's research; no patients' pacemakers were actually hacked, and to date there have been no known instances of the hacking of an implanted device. Yet the protocol for how such an event would be handled remains to be decided or even vibrantly discussed.

Perhaps the most serious issue of all is that the metrics of success for both interoperability and adoption of innovative, connected devices are directly connected to their scale – meaning that all of the aforementioned problems multiply exponentially when devices are thought of as targets, and their weaknesses, attack vectors, from the perspective of an attacker. For example, potential targets could include implantable cardiac

[6] Arndt, Rachel. "Abbott Recall Signals New Era in Medical-Device Cybersecurity."

devices, machines for CT scans, infusion pumps, and insulin pumps connected with continuous glucose monitoring. Then with each of these devices comes the potential for vulnerabilities similar to those Abbott encountered, in addition to other problems such as failure to account for documented weaknesses when using open source code and software, lack of required authorization or weak passwords, problems in legacy devices, and malware being distributed to devices during firmware updates. Taking all of this into account, it becomes very clear that medical device producers are facing a tough battle in which their attackers only need one attempt to work in order to cause what could be very serious damage – or in the cases of malfunctioning pacemakers or interrupted hospital networks, life-threatening damage.

5. Action Items

As seen in the FDA's involvement in the case of Abbott, there have been some industry and regulatory responses thus far. Much of the regulatory guidance for connected medical devices has fallen to the Center for Devices and Radiological Health (CDRH), which is part of the FDA. Some of the earliest signs of cybersecurity considerations from the FDA date to 2013, but given that they only recently began to really focus on the issue and that products often take years to make it through the regulatory pipeline, "the agency isn't surprised that it's taking some time to see results."[7] For device producers that are overwhelmed by the many potential problems listed above – which is not intended to be exhaustive – the FDA released a guide for premarket cybersecurity[8] in 2014, and a

[7] Hay Newman, Lily. "Medical Devices Are the Next Security Nightmare."
[8] FDA, Center for Devices and Radiological Health. "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."

subsequent guide for postmarket cybersecurity[9] in 2016. These could serve as a helpful starting points; however, more work is needed on providing clear and comprehensive cybersecurity requirements for all companies to adhere to, rather than "nonbinding recommendations." Holding all companies in the industry to a consistent set of policies will even the playing field and ensure a basic level of security for consumers. There is also more work needed on setting industry-wide answers to tough questions such as whether there should be standardized practices for vulnerability disclosure, and what those should be if so, as well as a common scoring metric for the classification of vulnerabilities and their danger to patients.

While regulatory agencies focus on those action items, companies and organizations in the healthcare space must also make cybersecurity a priority, and they can start by requiring usage of basic cyber safety measures. For developers and device makers, this includes an awareness of CVEs in any libraries, open source code, or software that they decide to use, and subsequently making design decisions that address those vulnerabilities. In clinical settings, administrators and IT professionals must be vigilant about installing software and system updates as they are released, creating policies for bring-your-own devices, and establishing protections for their network that take into account all the various networked devices that are connected to it. Further baseline measures that could be taken on both fronts are related to having more personnel dedicated to security – Security Operations Centers (SOCs) are a necessity for the major, large-scale medical device manufacturers, and even the bare minimum of having one person on their IT team focused

[9] FDA, Center for Devices and Radiological Health. "Postmarket Management of Cybersecurity in Medical Devices."

solely on security would be a significant improvement upon current security conditions in many large clinical environments, such as hospitals.

6. Conclusion

Medical devices are just one component of the expansive attack surface of the healthcare industry; however, they pose significant risks as potential attack vectors. On one hand, there are patient-focused devices, in which vulnerabilities could be leveraged to deliver a possibly lethal amount of insulin or fatally modify a person's heartbeat, for instance. On the other hand, there are the multitude of devices that connect to monitors or sensors, which then connect to larger hospital networks, endangering clinical environments' ability to care for patients through dangers such as ransomware, and raising privacy and data breach concerns as well. Though the healthcare industry is currently falling short in prioritizing security for connected medical devices and there are a number of steps that need to be taken by its various actors, one should not feel hopeless looking ahead. Action is certainly needed in order to prevent or even mitigate future cases, but the sooner that basic security considerations are met, the faster the industry can get to work on solving the larger, more complex issues that will arise as these devices increase in adoption and proliferation.

References

1. Visiongain. "The Global Medical Devices Market Will Reach $398.0bn in 2017 - Press Release - Market Research Reports." Accessed October 8, 2017. https://www.visiongain.com/Press_Release/498/The-global-medical-devices-market-will-reach-398-0bn-in-2017.
2. Kube, Nate. "Connected Medical Devices—An Expanding Threat Landscape." Medical Design Technology, December 19, 2012. Accessed October 29, 2017. https://www.mdtmag.com/article/2012/12/connected-medical-devices%E2%80%94-expanding-threat-landscape.
3. FDA, Center for Devices and Radiological Health. "Digital Health - Medical Device Interoperability." WebContent. Accessed October 29, 2017. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm512245.htm.
4. Kloeffler, Dan, and Alexis Shaw. "Former Vice President Dick Cheney Feared Pacemaker Hacking." ABC News, October 19, 2013. Accessed December 10, 2017. http://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434.
5. ICS-CERT. "Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities." Released August 29, 2017. Accessed October 30, 2017. https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01.
6. Arndt, Rachel. "Abbott Recall Signals New Era in Medical-Device Cybersecurity." Modern Healthcare, September 1, 2017. Accessed December 10, 2017. http://www.modernhealthcare.com/article/20170901/NEWS/170909986.
7. Hay Newman, Lily. "Medical Devices Are the Next Security Nightmare." Wired, March 2, 2017. Accessed December 11, 2017. https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.
8. FDA, Center for Devices and Radiological Health. "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." Food and Drug Administration, October 2, 2014. Accessed October 30, 2017. https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf.
9. FDA, Center for Devices and Radiological Health. "Postmarket Management of Cybersecurity in Medical Devices." Food and Drug Administration, December 28, 2016. Accessed October 30, 2017. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.