Healthcare and Technology: Cybersecurity in Medical Devices

Jennifer Leung

COMP 116: Introduction to Cybersecurity
Ming Chow
Tufts University

Abstract

With every year that passes, we become more and more entrenched in the Internet. On one hand, this signifies leaps and bounds of technological development; at the same time, however, this interconnectedness puts us all at risk to malicious. But it is not just data that can be lost — human lives are at stake too, with the rise of internet-connected medical devices. Devices such as pacemakers or infusion pumps, for example, are in danger of being hacked into stopping or given lethal injections. Ransomware attacks can compromise necessary medical systems, stalling appointments and operations. The cybersecurity of medical devices, which can directly impact life safety, is not nearly as secure as it should be. This paper will discuss the issues concerning the intersection of healthcare and technology, as well as possible action that can be taken to combat them.

Introduction

Cybersecurity is an ever-growing, ever-changing field concerned primarily with the confidentiality, integrity, and availability of information. Unfortunately, few people — or even companies — are aware of safe practices regarding security, and thus leave themselves at risk of attack. This extends to medical devices, with the additional catch of human lives rather than simply data. As defined by the Food and Drug Administration (FDA), a medical device is:

> *"An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory […] intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals […]"* [1]

This definition include items such as pacemakers, X-rays, and medical lasers. It is also important to note that these devices are increasingly connected to the Internet, opening the doors to both advantages and disadvantages. On one hand, connecting these devices leads to ease of use and accessibility. Information about the device or the patient using the device can be quickly transmitted to a database and kept on record. On the other hand, it leaves medical devices vulnerable to all the same dangers of everything else connected to the Internet of Things, and is the subject of this paper.

To the Community

Data, all those bits and bytes of information, is valuable. It can hold any number or combination of things, and the people relying on it can be adversely affected if it is tampered with. But medical devices bring to the table a whole new factor: human life. It draws a divide

between potential fallouts. Technology, as much as it is loved, can be replaced. People, however, cannot. This distinction is why research into medical device security — and anything else that directly affects the human element — is so necessary. There are many tradeoffs often made for technological advancement, but life safety should not be one of them.

Why is it so difficult to manage cybersecurity in medical devices?

Going from an isolated device to a network means that the security of the device is partially reliant to the network. If the network is weak, then every device on it is in danger. Once a device is infected, instead of being contained on that one device, other devices on the network may end up suffering the same fate. This is similar in idea to computer worms, and how they propagate across networks.

Additionally, many medical devices use third party software, and so they cannot control the security of that outside component; they can only pray that it is being maintained properly. Due to the nature of the devices, they are under intense regulation. Although vital, it also means that issuing updates or patches is extremely difficult and slow, leaving devices vulnerable for longer periods of time. [2] Even when passed, the clinical trials that are run tend to be small and not exhaustive. Furthermore, medical devices are expected to be operable in the field for decades at a time, according to security expert Beau Woods — but the software underpinning the devices have a life expectancy of only 2 - 10 years due to the ever-evolving nature of technology. [3]

It’s Not Hypothetical

The dangers imminent to medical devices are not fabricated; many may dismiss such concerns as “it’ll never happen to me,” but such thinking only provides a false sense of security, especially when 94% of healthcare organizations have been the victim of some sort of cyber

attack. [2] Medical devices have been shown to be weak to breaches and attacks in recent years, and thus put life safety at risk. This paper will discuss a few such examples.

Hospira Infusion Pumps

In 2015, the FDA did something for the first time: they advised healthcare providers to stop using a medical device due to cybersecurity concerns. [4] Hospira Inc was a producer of the Symbiq infusion system, responsible for providing patients with medication directly into their bloodstream. Though no attack actually occurred, independent cybersecurity expert Billy Rios demonstrated that it was possible to access the hospital network and direct the delivery system to over- or under- dose the patient; all of this was accomplished remotely by intercepting the wireless connection.

Abbott Pacemakers

MedSec Holdings, a cybersecurity firm, released information detailing the vulnerabilities in Abbott pacemakers that would allow an attacker to modify the devices' battery usage and commands, even being able to deliver a potentially lethal shock to the patient, thus posing a serious threat to the lives of the people using the pacemakers. This was also achieved by intercepting the wireless connection. The FDA issued a warning letter to the company, condemning them for unsafe cybersecurity practices; the company denied the vulnerabilities at first, further endangering the lives of patients. [5] It took several months after that — during which the devices were recalled — for an update to be made available. [6]

WannaCry

The WannaCry ransomware that struck earlier this year took advantage of an exploit termed 'EternalBlue.' [7] A patch had been released prior to the attack that would have protected

against this vulnerability in Windows systems. It was recommended to install the patch — however, the victims of WannaCry, overwhelmingly, did not heed this advice. [8] The National Health Service (NHS) was hit hard by this attack, which could have been easily mitigated if basic security practices had been followed by patching their systems once it was available. The attack encrypted patient data and files, causing NHS bodies to cancel thousands of appointments, and resort to pen and paper for their daily operations. Communications were also affected, causing large-scale confusion. Though NHS claims that no patient harm occurred, there was significant risk to life safety as hospital systems went down and operations had to be cancelled.

Telesurgery

One of technology's strongest points is the innovation that comes with it; the realm of new possibilities for complicated problems. Telesurgery is one such innovation; for areas lacking in trained surgeons, telesurgery makes it possible for a surgeon to remote control a robot to perform surgery. This, of course, would need several security safeguards in place before it can be fully utilized. Tamari Bonaci and co at the University of Washington hacked into telesurgery robot, named Raven II, to show how far the telesurgery community still has to go. The team was able to change or override the commands sent to the robot, take full control of the robot and even shut it down, as well as look into the public video feed. [9] This was all made possible because the connection between the robot and surgeon is made over public networks, using the Interoperable Telesurgery Protocol. Security concerns are raised, as this means that an attacker could shut down the robot, prohibiting surgeries from being performed, or have them performed incorrectly. The video feed also is of concern to the privacy of the patient. One important step to take in regards to telesurgery is the encryption of information sent to the robot.

Action Items

It seems like everywhere we look, we're surrounded by risk; our medical devices are no exception. This does not mean we should abandon our medical devices and sue every company producing them. So what do we do? What steps can be taken to minimize these risks?

The consumer has their own role to play in the grand scheme of things. Consumers should be sure to understand the implications and risks of the things they so easily accept. Doing preliminary research and understanding the fundamentals of cybersecurity goes a long way. Consumers, when buying or using medical devices, should check that the supplier of said device takes security seriously and is transparent about such issues. Additionally, updating frequently and making sure to have the latest version of their devices with the most secure patches is an important way to stay ahead of attackers who may be exploiting older, more vulnerable systems. This does, however, mean greater overhead on the part of consumers. It could also mean that consumers and end users would have to choose between an option that may be cheaper but less secure, or expensive but more secure.

On the other end of the spectrum is the FDA and other government organizations, such as the Department of Homeland Security (DHS). For example, the National Institute of Standards and Technology (NIST) put out the Framework to outline guidelines and goals for cybersecurity, but it is not binding. [10] The FDA has similar guidelines, but these are not currently strictly enforced, allowing companies and other producers to ignore the security recommendations. The regulation needs to be enforced and fast-acting in order to be effective, providing a baseline to look up to. Contingency plans are also necessary to control confusion and risk if something goes wrong. However, stricter regulations are also a double-edged sword; it may continue to make the

process for creating or updating medical devices slow and cumbersome, possibly discouraging manufacturers.

On the part of medical device manufacturers, they must prioritize security in their products and extensively test them. Basic security measures, at the very least, must be implemented: encryption of data, setting minimum permissions, closing unnecessary ports. Updated software and hardware should be used. The tradeoffs here may be the interoperability of the devices. Uplifting security and privacy may be an issue for functionality; many medical devices, such as pacemakers, are small. They don't have the traditional firewalls or antivirus software that other devices have; building that security into them would often require making the devices themselves larger, which hinders their use. [2] Isolating devices to their own network would protect a network-wide attack, but again, deals a blow to how the devices can connect and share information among themselves. More research is needed to determine the best approach to balancing these factors.

Lastly, but perhaps most importantly: education. Hospitals tend to be unaware of these issues, as do general consumers. Better informing all parties empowers them to take proactive steps towards maintaining secure practices. It is difficult to protect against what one does not know is a danger. By ensuring that all parties have a grasp on cybersecurity and why it is important, they are better equipped to make smarter decisions regarding their devices and protect themselves from harm.

Conclusion

Dick Cheney, former Vice President of the United States, had an implantable heart device; he had the Bluetooth turned off in order to thwart attempts at hacking it. [11] He may have

been seen as unnecessarily paranoid at the time, but it becomes an increasingly real threat that we must all remain vigilant of.

Medical device security is not just the responsibility of government organizations, like the FDA or DHS. The burden also rests on the shoulders of the manufacturers, healthcare delivery organizations, and end users. Though there are currently no known instances of hacked medical devices in real patients, the risk is still present. It was revealed that the DHS's Cyber Emergency Response Team is investigating about over 20 cases of cybersecurity flaws in medical devices. [11] The delicate balance between interoperability and security needs to be found, as it is vital to improve the current system surrounding the interwoven fields of healthcare and technology in order to uphold life safety.

References

1. Center for Devices and Radiological Health. “Classify Your Medical Device - Is The Product A Medical Device?” U S Food and Drug Administration Home Page, Center for Devices and Radiological Health, www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm.
2. Williams, Patricia AH, and Andrew J Woodward. “Cybersecurity vulnerabilities in medical devices: a complex environment | MDER.” Medical Devices: Evidence and Research, Dove Press, 20 July 2015, www.dovepress.com/cybersecurity-vulnerabilities-in-medical-devices-a-complex-environment-peer-reviewed-article-MDER.
3. Harris, Dan, et al. “Fears of hackers targeting US hospitals, medical devices for cyber attacks.” ABC News, ABC News Network, 29 June 2017, abcnews.go.com/Health/fears-hackers-targeting-us-hospitals-medical-devices-cyber/story?id=48348384.
4. Clarke, Additional Toni, and Caroline Humer. “FDA warns of security flaw in Hospira infusion pumps.” Reuters, Thomson Reuters, 31 July 2015, www.reuters.com/article/us-hospira-fda-cybersecurity/fda-warns-of-security-flaw-in-hospira-infusion-pumps-idUSKCN0Q52GJ20150731.
5. “2017 - Abbott (St Jude Medical Inc.) 4/12/17.” U S Food and Drug Administration Home Page, www.fda.gov/ICECI/EnforcementActions/WarningLetters/2017/ucm552687.htm.
6. Center for Devices and Radiological Health. “Safety Communications - Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (Formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication.” U S Food and Drug Administration Home Page, Center for Devices and Radiological Health, www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm.
7. GReAT on May 12, 2017. 5:30 pm. “WannaCry ransomware used in widespread attacks all over the world.” Securelist - Information about Viruses, Hackers and Spam, 12 May 2017, securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/.
8. Palmer, Danny. “WannaCry ransomware: Hospitals were warned to patch system to protect against cyber-Attack - but didn't.” ZDNet, ZDNet, 27 Oct. 2017, www.zdnet.com/article/wannacry-ransomware-hospitals-were-warned-to-patch-system-to-protect-against-cyber-attack-but-didnt/.
9. Security Experts Hack Teleoperated Surgical Robot - MIT ... 24 Apr. 2015, www.bing.com/cr?IG=906E988B8ABA434494BB5CB86E2F6822&CID=30EB7E5FF17D6E3213587509F0D26FDC&rd=1&h=q4BrCA_B5buTAtntqLN3AAMpcPhwadgm-VJaNLN9jRQ&v=1&r=https%3a%2f%2fwww.technologyreview.com%2fs%2f537001%2fsecurity-experts-hack-teleoperated-surgical-robot%2f&p=DevEx,5068.1.
10. Framework for Improving Critical Infrastructure Cybersecurity. 2014,

www.bing.com/cr?IG=FE5BA1450D174DA8A1E0947A86259FF4&CID=1673B87F92E060141FE4B329934F614C&rd=1&h=a1m0TiqlAKw_2uInvEJo-rwkRu0yaz2pJayub8A-UR4&v=1&r=https%3a%2f%2fwww.nist.gov%2fsites%2fdefault%2ffiles%2fdocuments%2fcyberframework%2fcybersecurity-framework-021214.pdf&p=DevEx,5067.1.

11. Thomas, Ashley. “Hack Attack: Cybersecurity Vulnerabilities of Medical Devices.” American Bar Association, www.americanbar.org/publications/aba_health_esource/2015-2016/september/hackattack.html.