ASEE IL-IN Section Conference

Cybersecurity Threats Targeting Networked Critical Medical Devices

Emily Gaukstern
Wentworth Institute of Technology

Shankar Krishnan
Wentworth Institute of Technology

Cybersecurity Threats Targeting Networked Critical Medical Devices

Emily Gaukstern, Shankar Krishnan, Ph.D.

Biomedical Engineering Department
Wentworth Institute of Technology
Boston, Massachusetts 02115

Introduction

Cybersecurity is infectiously becoming a cause of growing societal concern amidst numerous allegations in the defense, intelligence, finance and healthcare domains. As the population has seen cybersecurity vulnerabilities exploited by anonymous subjects residing at multiple locations around the globe, concern is increasing and attention is being brought to a new type of crime that is committed through networked computer systems. The field is rapidly growing with cybercriminals capitalizing on the victims' unpreparedness with the associated technologies and infrastructure. It is reported that organized cybercrime activities have expanded to exceed illegal drug trafficking [1]. The ways in which the cyber threats are infiltrating networked systems are becoming very intricate, newer threats seem to be evolving once the threats are detected and addressed as evidenced in different fields including healthcare. Rapid advances of technological applications in the healthcare field are designed to diagnose, cure disease conditions, provide therapy and rehabilitation to patients. It is to be noted that Electronic Health Records (EHR) contain private information of patients and are stored in networked systems. Healthcare has become a prime target for cyberattacks and it has been reported that over 90% of healthcare organizations have been the victims of cyberattacks. These events include attacks on medical devices and hospital information systems (HIS) [2]. Addressing the cybersecurity issues with medical devices is a complex problem of vital importance especially due to potential serious consequences.

The objective of this paper is to review and analyze the cybersecurity issues pertaining to implantable and programmable medical devices in selected cases and make suggestions to improve observed security challenges.

Background

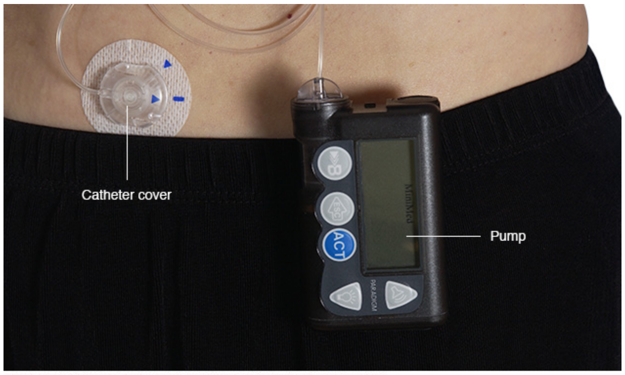
Cybercrime within the medical field has grown widely for its ability to specifically target individuals as well as the monetary value linked with their EHR. In May of 2017, the White House Director of National Intelligence stated, "The medical sector was firmly in the sights of the cyber criminals [3]." According to experts, the value of stolen personal health information is ten to twenty times greater than the value of a stolen credit card number [4]. On the dark web, medical records are sold for a bitcoin equivalent of $60 a piece, credit card numbers are individually sold for only $1-$3. This large difference in value is due to the amount of personal information found in a patient's medical record. Once bought, medical records are used for a wide variety of purposes from opening a line of credit to charging a major surgery, or medication. Often as a byproduct of the theft, many medical records can be altered or changed without notice, such as an allergy to a prescription. This error in a patient's medical records can lead to accidental death if unnoticed and unattended by medical professionals. IBM research stated over 100 million medical records were compromised globally in 2015 alone, an equivalent of about a third of the United States population had their medical records compromised in 2015. The data breaches and cyber threats have increased dramatically in frequency and have had staggering financial impacts while continuing to put patient information at risk. It has been reported that nearly 90% of healthcare organizations have suffered a breach of their data since 2015. It has been estimated that the annual cost of dealing with the security breaches is $6.2 billion [5]. A report by the GAO reported that, "Criminals are aware that obtaining complete health records are often more useful than isolated financial information, such as credit information...Electronic health records often contain extensive amounts of information about an individual" [6]. Due to the importance of health care information, it was declared part of the nation's critical infrastructure, meaning the destruction of such information would have debilitating results on the nation's health, safety and/or security.

Case Histories of Cyber Attacks on Implantable and Programmable Medical Devices

The significance, severity and the consequences are better understood and appreciated by reviewing multiple case histories. In the following sections, case histories of cyberattacks on implantable and programmable medical devices, insulin pumps and pacemakers, are described.

Insulin Pumps

An insulin pump provides continuous and as-needed dose delivery of the protein insulin to diabetic patients. Insulin pumps deliver insulin by continuous infusion through a single subcutaneous site which is replaced, on average, every three days. The insulin pump alleviates the need for a diabetic patient to have multiple injections and also improves the blood sugar level counts. The continuous delivery of small doses of insulin is administered in order to maintain the basal rate, predetermined by the attending physician. The basal rate combined with the individual bolusing to match activity and calorie intake create the total insulin needed for an insulin dependent patient. The pump in size is relatively small and worn on the outside of the body. The insulin is delivered to the body through a catheter connected to a thin cannula and placed into the subcutaneous layer, as shown in Figure 1.



© MAYO FOUNDATION FOR MEDICAL EDUCATION AND RESEARCH. ALL RIGHTS RESERVED.

Figure 1: Insulin Pump Connected to a Diabetic Patient

The wireless connectivity of the device creates a susceptible environment for the hacker to infiltrate. The cybercriminal can gain access to the device through a tiny radio transmitter that permits adjustment to any settings functions [7]. A block diagram configuration of potential pathways of infiltration are shown in Figure 2.

The hacker has the ability to not only access the EHR of the victim but also adjust settings on the infusion pump to release large doses of insulin into the patient without their knowledge or consent. This could have serious impacts on the individuals targeted causing severe hypoglycemia [8]. The rapid increase of insulin within the patient's body causes the cells to absorb more glucose from the blood causing the liver to release less glucose, due to glycogenesis. The body attempts to correct the decrease of glucose in the blood by increasing glucagon, a hormone released by the pancreas, and epinephrine secretion. If the hypoglycemia is severe and prolonged, it can lead to functional brain damage, including impairment of cognitive function, motor control and consciousness, or even death.

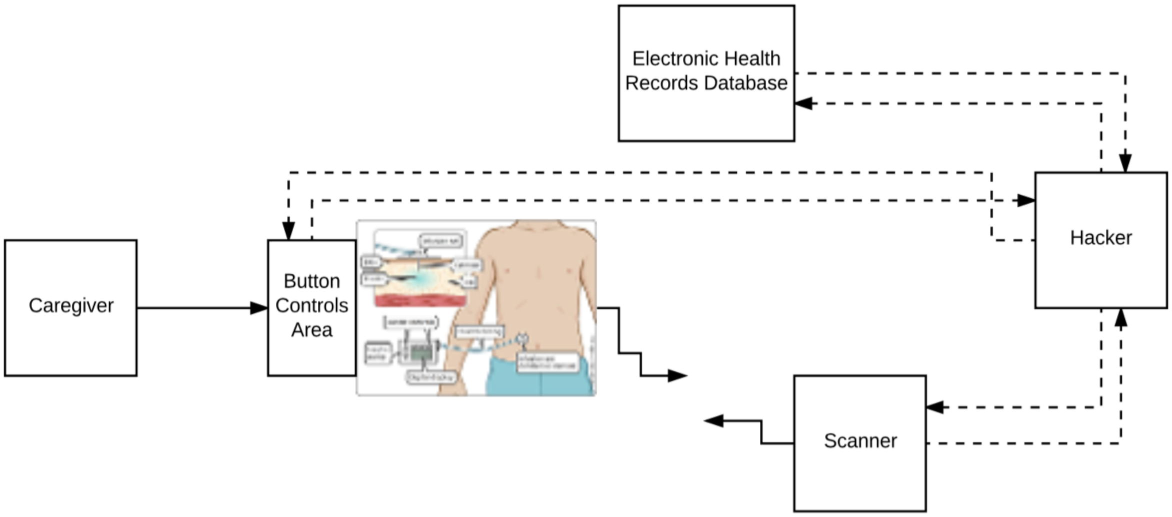


Figure 2: Infiltrated Insulin Pump System

Cardiac Pacemakers

Pacemakers are prescribed for implementation to patients with cardiac arrhythmia. Usually a candidate patient for a pacemaker has issues with the electrical activity due to malfunctions or complications with the SA node. A surgeon would implant a pacemaker under the skin close to either the right or left collarbone of the patient. A cardiac pacemaker consists of electronic circuits that provide stimulation to myocardium thus triggering this electrical activity needed for proper mechanical functioning of the heart. The pacemaker has electrodes at the end of the wires connecting to different chambers of the heart, as shown in Figure 3a; a commercial cardiac pacemaker is shown in Figure 3b. A demand pacemaker is designed to sense when the heart needs assistance by measuring each heartbeat and providing a stimulus on demand. Rate-responsive pacemakers adjust heart rates depending on the patient's level of activity. They measure the SA node rate but also breathing, blood temperature and other factors. Today's permanent pacemakers last about 10 years, depending on how frequently the device has to work [9].

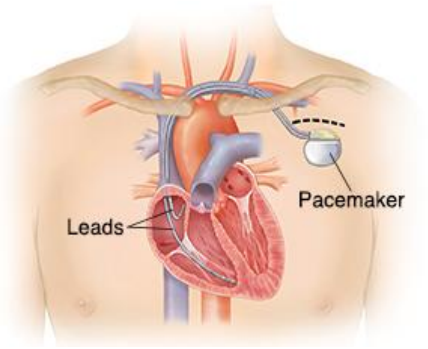


Figure 3a: Cardiac Pacemaker

Figure 3b: Commercial Cardiac Pacemaker [10]

Based on the patient conditions, the attending physician may need to adjust the settings on the pacemaker through external programming. While this programming function provides an essential function for appropriate patient care, this is also a weak link for possible access by unauthorized persons. This is one major area that is vulnerable to cybersecurity threats with the pacemaker leading to potential harm to the patient. The pathway that is responsible for programming any required information into the pacemaker is a possible entry port for criminals to gain access to the pacemaker device. The pacemaker is linked with the hospital network for programming and monitoring, which is a major cybersecurity concern for the care providers [9]. A scenario of infiltration applicable to a medical device in general is displayed in Figure 4.

Hackers may obtain access to the hospital network by unauthorized means, and from the hospital network communicate with the interface connected to the medical device originally intended for patient care purposes. Thus the hackers may be able to access the adjustment settings on a medical device implanted in a patient and the settings may be reset to lethal values [11].

Specifically in the pacemaker, the settings could be reconfigured to slow the heart rate down, or speed the heart rate up by variable shocking to the myocardium. The patient would enter severe bradycardia when the pacemaker is not sending an electrical current to the heart at a required fast rate and the heart is unable to pump adequate amounts blood to meet the body's needs. When the heart rate is rapidly increased by the pacemaker, the patient experiences severe tachycardia sending the heart into atrial flutter or ventricular fibrillation, during which the chaotic electrical pulses cause the ventricles to quiver and stop pumping blood.

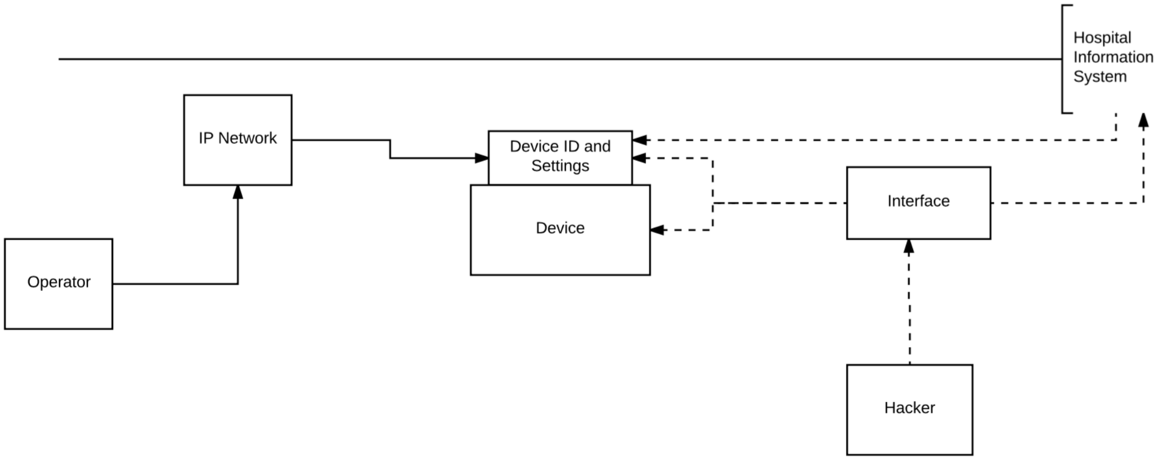


Figure 4: Basic Block Diagram Depicting Infiltration of a Medical Device through a Hospital Network

Results and Discussion

In the following sections some of the adverse events reported in clinical situations pertaining to insulin pumps and cardiac pacemakers are described so the negative impacts of the reported cyber attacks are analyzed.

Hacking Insulin Pumps

In October of 2016, Johnson and Johnson issued a warning regarding possible security issues with the Animas OneTouch Ping Insulin Infusion pump, as shown in Figure 6. A cybersecurity firm discovered possible areas of infiltration allowing for full control of the pump through its unencrypted radio frequency communication system. After gaining control, the hacker would be able to dose the patient with possible lethal amounts of insulin from up to 25 feet away [12] [8].

Figure 6: Animas OneTouch Ping Insulin Infusion Pump [13]

In our research, we could not find a published instance of the pump having been hacked by any cyber criminals to date. The feasibility of cyber attacks on insulin pumps was demonstrated at two security conferences in Las Vegas and Miami. In 2011, at a cybersecurity conference in Miami a cyber attack on a Medtronic insulin pump was demonstrated by McAfee researcher, Barnaby Jack. The first hacking of the insulin pump was by a scanner with high-gain antenna to boost its range. The scanner was used 150 feet away from the target to scan the company-designated frequency for a pump which helped to retrieve the target pump's ID and ultimately gain access to the insulin pump controls. Also in 2011, the second infiltration of the pump was demonstrated wirelessly from 300 feet away at the Black Hat conference in Las Vegas. The hacker used a Medtronic Minimed Paradigm pump, as shown in Figure 7. The software extracted the pump's security credentials and had the pump empty all of its contents of insulin into the simulated victim [12] [8].

Figure 7: Medtronic Minimed Insulin Pump [13]

Hacking Cardiac Pacemakers

The cardiac pacemaker system was found by the FDA in 2017 to have an area of cybersecurity vulnerability. The St. Jude Pacemaker works with an at home radio frequency system, Merlin@home, designed for communication over the Merlin.net Patient Care Network, as shown in Figure 8.

Figure 8: Merlin@home Transmitter [5]

A safety alert in January 2017 by the FDA stated that the device, "contain configurable embedded computer systems that can be vulnerable to cybersecurity intrusions and exploits. As medical devices become increasingly interconnected via the Internet, hospital networks, other medical devices, and smartphones, there is an increased risk of exploitation of cybersecurity vulnerabilities, some of which could affect how a medical device operates." [9] The Merlin@home transmitter is designed to communicate with any St. Jude cardiac device because there is a lack of strong authentication [11]. Cyber attackers are able to reverse engineer the communication process and access the cardiac devices.

Recommendations to Address Cybersecurity Threats

The medical devices described, with active cyber threats and areas of infiltration, we recommend should include the described premarket and post market adaptations to the systems. A safeguarded administrative interface requiring users to complete multi-factor authentication before enabling the viewing, sharing or modification of information on medical devices would reduce the risk of intrusion by providing better forms of identification [14]. Verifying who the user claims to be reduces the risk of infiltration significantly. The medical devices within the hospital network are left vulnerable to a variety of threats due to the network connectivity. Eliminating this problem by firewalling the devices off from the hospital network would provide safer patient care. Because of the necessity to protect the data being imported and exported from the medical devices, strong encryption is needed when the information is being stored as well as when in transit [14]. The manufacturers and providers need to both have detailed incident response plans to ensure the most appropriate and effective response in the case of an infiltration to a medical device. Intermittent security sweeps of the networked systems would need to be conducted to ensure the system is running at proper capacity too many security measures have been implementing rendering the system counterproductive.

Future Work

Many advancements and future applications of the technology and procedures associated with cybersecurity of critical medical devices can be made. Previously existing manufacturers of medical technologies, specifically high risk medical devices, need to enforce policies and procedures for providing essential protection from possible infiltration and cyber-attacks. Emerging medical technologies need to be conscious of cyber threats and specific areas of each device that have susceptibility to infiltration from the initial moments of the design stage. Medical technology companies are required to stay advancing as increasing amounts of medical technology are transitioning to mobile functioning and telehealth technology. Healthcare and medical professionals are doing work from smartphones and mobile devices. The surge in attention to mobile and telehealth is leaving patients susceptible to risks. A mobile or home network has a dramatically less amount of safeguarding and security leaving patient information vulnerable to an infiltrator accessing unauthorized information.

Conclusion

Cybersecurity vulnerabilities are exploited by hackers in networked medical device systems abusing the rapid advancement of medical technologies and the associated value of the patients' health records. Improving the cybersecurity issues pertaining to implantable and programmable medical devices through protective multi-level authentication, providing firewalls from medical device systems to the hospital networks, encryption when storing patient information and using the data in transit, and extensive incident response plans from both the manufacturers and providers will result in reduced amounts of cyberattacks on medical devices and a more accepting patient community because of increased care and decreased risk.

References

1. Axel Wirth. "Cybercrimes Pose Growing Threat to Medical Devices." *AAMI* Application of Risk Management for IT Networks Incorporating Medical Devices (2011): 26–34. Print.
2. Kevin Fu, and James Blum. "Controlling for Cybersecurity Risks of Medical Device Software." *AAMI* Managing Risk. Horizons (2014): 38–41. Print.
3. "Worldwide Threat Assessment - The Director of National Intelligence's View." IDG Communications. *CSO*. N.p., 11 May 2017. Web. <https://www.csoonline.com/article/3195742/security/worldwide-threat-assessment-the-director-national-intelligences-view.html>.
4. Christina Farr. "On the Dark Web, Medical Records Are a Hot Commodity." *Fast Company*. N.p., 7 July 2016. Web. < https://www.fastcompany.com/>.
5. HIPPA Journal. "Largest Healthcare Data Breaches of 2016." *HIPPA Journal*. N.p., 4 Jan. 2017. Web. < http://www.hipaajournal.com>.

6. Joe Davidson. “Cyberattacks on Personal Health Records Growing ‘Exponentially.’” *The Washington Post*. N.p., 28 Sept. 2016. Web. < https://www.washingtonpost.com/>.
7. John P Mello Jr. “Insulin Pump Susceptible to Hacking.” *Tech News World*. N.p., 7 Oct. 2016. Web. < http://www.technewsworld.com/story/83969.html>.
8. Jim Finkle. “J&J Warns Diabetic Patients: Insulin Pumps Vulnerable to Hacking.” *Reuters*. N.p., 4 Oct. 2016. Web. < http://www.reuters.com/article>.
9. Carson C Block. Muddy Waters Research: Muddy Waters Capital LLC, 2016. Web. < http://www.muddywatersresearch.com>.
10. “St. Jude Medical Announces First Implant of Next Generation Quadripolar Pacemaker in India.” *The Enterprise of Healthcare*. N.p., 23 Sept. 2013. Web. <http://ehealth.eletsonline.com/2013/09/st-jude-medical-announces-first-implant-of-next-generation-quadripolar-pacemaker-in-india/>.
11. Michael Mezher. “FDA, DHS Find Cybersecurity Vulnerabilities in St. Jude Heart Devices.” *Regulatory Affairs Professionals Society*. N.p., 11 Jan. 2017. Web. <http://www.raps.org>.
12. Dan Goodin. “Insulin Pump Hack Delivers Fatal Dosage over the Air.” *The Register*. N.p., 27 Oct. 2011. Web. <http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/>.
13. “OneTouch Ping.” *Animas*. N.p., 2017. Web. <https://www.animas.com/diabetes-insulin-pump-and-bloog-glucose-meter/onetouch-ping-blood-glucose-monitor>.
14. “9 Important Steps in Securing Medical Devices.” *Health Data Management*. N.p., 18 Apr. 2017. Web. <https://www.healthdatamanagement.com>.
15. Ashley Thomas. “Hack Attack: Cybersecurity Vulnerabilities of Medical Devices.” *American Bar Association Health Bar Section*. N.p., Sept. 2015. Web. <http://www.americanbar.org>.
16. Brooke H. McAdams. “An Overview of Insulin Pumps and Glucose Sensors for the Generalist.” *Journal of Clinical Medicine* 5.1 (2016): n. pag. Web. <https://www.ncbi.nlm.nih.gov>.
17. David C Klonoff. “Cybersecurity for Connected Diabetes Devices.” *Journal of Diabetes Science and Technology* 9.5 (2015): 1143–1147. Print.
18. Jerzy W Rozenblit et al. “Security Challenges for Medical Devices.” *Communications of the ACM* 58.4 (2015): 74–82. Print.
19. Marianne Kolbasuk McGee. “Ramping Up Medical Device Cybersecurity.” *Gov Info Security*. N.p., 26 Sept. 2014. Web. <http://govinfosecurity.com>.
20. Michael Rushanan. “SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks.” *IEEE Symposium on Security and Privacy* (2014): 524–539. Print.
21. Patricia AH Williams, and Andrew J Woodward. “Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem.” *Medical Devices: Evidence and Research* 8 (2015): 305–316. Print.

22. "TrapX Labs Discovers New Medical Hijack Attacks Targeting Hospital Devices." *TrapX Research Labs*, 2016. Print.
23. TrapX Security. *Anatomy of Attack*. TrapX Research Labs, 2016. Web.