Security Risk of Wireless Implantable Medical Devices

STEVEN SUGGETT
Lewis University
CAMS Dept.
1 University Parkway Dr., Romeoville, IL
USA

LUCIEN NGALAMOU
Lewis University
CAMS Dept.
1 University Parkway Dr., Romeoville, IL
USA

Abstract: Wireless Security has become increasingly important in recent years. The amount of devices that connect to the internet has skyrocketed with the capability of connecting wirelessly to these devices being recently added. Very few of these devices are equipped with proper security methods. One such device that only recently has been added to the pool of wireless devices is implantable medical devices such as pacemakers. Patients and doctors can connect to these devices to update firmware, view information, and manage the device in other ways; however, the devices still lack the proper cybersecurity and are vulnerable. This paper presents a review of security risk of wireless implantable medical devices, the obstacles and solutions to address security threads that these devices might be exposed to.

Key–Words: Internet of Things, Wireless Security, Encryption, Implantable Medical Devices, Authentication.

Received: November 2, 2019. Revised: May 6, 2020. Accepted: May 18, 2020. Published: May 29, 2020.

1 Introduction

The concern for cyber security has been increasing for many reasons in recent years. Security breaches compromise the information of a system and can happen wirelessly and quietly. A user may have no idea their system has been compromised, but an attacker could have access to view and potentially modify data within the machine. There is no perfect method for security, as any computer connected to the internet, sending data out and taking data in has the ability to be attacked. The closest scenario to a perfectly secure computers are ones that are not hooked up to the internet at all, and even those computers can be compromised if an attacker has physical access to it. In the past, this concern over cyber security was reserved just for computers, as there were not many other devices that could be connected to wirelessly; however, recently there is a growing phenomena where countless devices are connected to the internet. This is known as the Internet of Things, and it includes any printers, DVRs, wireless mice and keyboards, and many different medical devices including pacemakers and implantable cardiac defibrillators. Many of these devices serve very important functions, and this means their security is essential. Even devices that appear to serve no harmful function such as household appliances could be compromised and play a role in other attacks. The security of these devices, especially medical devices, and what can happen once they are compromised must be considered when designing them. There are many different security systems in place and even more on the way, but no matter how sophisticated security methods get there is always the often overlooked security breach through human error, in the form of improperly setting up or ignoring security protocols. Implantable medical devices in particular have been known to contain many security holes, opening the devices up to potential attacks. Many of these devices were designed solely with function in mind, and lack any sort of encryption, authentication, or prevention against attackers gaining access and control over the device [1].

A major cause of this in the past has been the lack of control over the requirement involved in the security of medical devices, and it was not until just recently, around late 2016, that the US Food and Drugs Administration (FDA) has placed more restrictive standards on the security of implantable medical devices [2] . The FDA has made many different recommendations over the years, starting in 2005, when it comes to cyber security for implantable medical devices; however it was not until December 28, 2016 that the FDA turned what used to be non binding recommendations into requirements for medical implant design [2]. In providing these devices with greater security, a variety of known attacks has to be considered and the ways methods to preventing them.

*Corresponding Author

2 Regulation History of Medical Implants

The first medical implant was a pacemaker given to a patient in 1958 [3]. At that time, the primary concern for medical device research has been focused mainly on increasing efficiency and battery life, as there was not a major concern for cyber security. Around this same time, a similar trend was shown where performance was the first major concern, and security did not become an issue until later on. While advances in security for computers has advanced to become very sophisticated since the 1960's, medical devices fell behind in security. Medical devices have relatively recently been given the ability to connect wirelessly to other monitors and devices allowing patients and doctors can view vital information. The methods in which medical devices can connect to outside monitors is through various wireless frequencies, some exclusively used for medical implants while others use more common methods such as Wi-Fi and Bluetooth [3]. There are many known vulnerabilities for these wireless methods if they are not setup properly. Careful setup while using any wireless connection is necessary, and failing to follow proper setup could lead to vulnerable medical devices. For example, leaving Wifi or other passwords as the default or empty makes it extremely easy to break into for attackers. Setting up the security of the devices properly greatly reduces vulnerability of these devices to attacks [3].

3 Potential for Medical Device Attacks

Any message sent wirelessly has the potential to be intercepted, which is why managing proper security protocols for these messages is important. Medical devices have become increasingly dedicated in recent years, having gone from simple mechanical implants that do their job and not much else, to sophisticated mini computers that not only does their job, but also transmits vital information wirelessly to be analyzed by doctors; however, the data transmitted to and from the medical implants, like any other data sent wirelessly, is vulnerable to attackers [4]. The problem has become that while the scope of these medical implants has increased, the necessary security of these devices has yet to be implemented. Two major medical companies, St. Jude Medical and Johnson & Johnson, have even declared that there are unaddressed security risks in current medical implants and other medical devices; however, the risks posed by these security holes are often overblown, and it would often be more dangerous to choose not to accept a medical implant because of the security risks [4].

Deciding not to use a medical device because of the potential for the device to become compromised is much more dangerous. This is because even though medical implants such as pacemakers could be attacked by outsiders, the likelihood of a normal consumer being targeted in a life threatening attack is rather low [4]. Targeting a pacemaker with the intention of compromising it with lethal intent is, at the end of the day, homicide and the chance of becoming the victim of a wireless attacker with intent to kill as rather low. What is perhaps an even more important issue, given how unlikely a fatal attack is using medical implants, is the privacy of information going to and from the device. Sensitive, personal medical information relating to the patient can be compromised by intercepting data going to and from the device, and keeping a patient's private information safe is very important in the medical field. While not many attackers would regularly perform fatal attacks using implants, there are likely many attackers who would be willing to intercept medical data transmitted by these medical implants and sell them to other attackers [4] For this reason it is still very important to ensure the security of medical devices, and of course preventing fatal attacks however unlikely is still from the medical device; however, an attacker is able to listen in on what is being sent, and also send his own commands to the device. Fig. 1. A Doctor is able to freely send

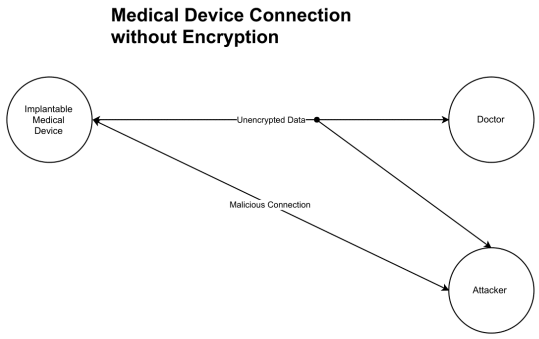

Figure 1: Medical Device Connection without Encryption

and receive information desired, but the obstacles to implementing proper security protocols cannot be ignored. One major obstacle is the cost of implementing security protocols into medical implants. Medical implants are very small, very advanced devices that are constantly evolving. Having to keep security up

to date would delay the release of these medical devices, and increase the cost of future installments and research within them [5]. Implementing security protocols within these medical devices starts at the design level, and researchers and programmers need to keep security in mind even at the very start of medical device related projects. Calls for the government to create security guidelines has been plentiful in the last few years, and more recently some guidelines have started to be made, such as the guidelines created by the FDA. The FDA guidelines require proper implementation of security protocols for the encryption of data, the authentication of its users, and proper use of the privileged user [2]. Research and advancements concerning these devices has typically been focused on making the operating systems within these devices more efficient and faster, and implementing cyber security measures would go against this trend. Because of this many devices still have barebones security, and for the security of patients' privacy and wellbeing it is important that research goes into keeping implantable medical devices secure [5]. To understand some of the requirements recently set by the FDA for secure medical devices, common encryption methods, authentication methods, and the function of a privileged user will be analyzed.

4 Encryption Methods

One of the guidelines that the FDA has required for medical devices is the encryption of data. AES is one of many methods of encryption, and there are various methods that strive to achieve the same goal as it. While the actual encryption method used for encrypting data from these medical devices may vary, AES stands out as an important method because it has been recognized as a very good form of encryption, and has even been formally approved by the government as being recognized as a security standard [4]. AES is currently used to encrypt web traffic, is the major discerning upgrade between WPA and WPA2, two very common security methods used The main goal of encryption is to scramble a message enough to give outside observers the least information possible about the original message. This ensures the privacy of the contents of the message, and is rather important for many devices. The original message that becomes encrypted may either consist of readable words intended to communicate with other people, or the message may also contain commands that are meant to be interpreted by some system. Because the encrypted message should convey the least information possible to an attacker, good encrypted messages should appear completely random. Simply replacing the original message with completely random contents would not be viable though, since the intended receiver of the message must be able to revert the message back to its original form in order to read it [4].

4.1 Diffusion and Confusion in AES Encryption

An effective encryption algorithm needs to be able to take any message, scramble it up enough to appear completely random, provide no statistical data concerning the original message such as how many times a certain letter appears, and be revertable by only the intended receiver. AES was designed from the ground up to do this effectively, and it does this by performing a series of mathematical operations between the data within the original message, and the data contained within a key file, which in its simplest terms is simply a random value applied to the encryption algorithm. The AES algorithm scrambles the original message so effectively, that even changing a single character from the original message will completely transform the outcome of the encrypted message. The message is encrypted using the key, and can be decrypted by anyone who has the same exact key. Anyone without the key will not be able to read or understand the original message, while people with the key can undo the mathematical operations performed from the encryption algorithm and have access to the original message

4.2 Protection Against Brute Force Attacks

Brute Force attacks are when an attacker simply tries every possible key when decrypting a message until they find the original message. It is usually fairly obvious to tell when the original message has been found, because it will be on of the only messages that makes sense and is not just a scramble of random values. For example, if the attacker expects the original message to be in English, then they can try random keys until they decrypt into a message that has English text. In order to ensure the key cannot be randomly guessed the simplest solution has been to make the make the number of possible keys so large that it would take for too long, even for automated computers, to try every possible key. The problem with this is that as time goes on computers are becoming more efficient, and keys that used to be large enough to trusted as safe are not anymore. Thankfully, current encryption methods have attempted to prevent this, at least for a while, by overestimating necessary size for

these keys; however, over time the size of keys will inevitably have to be increased once again. AES, and many other encryption methods, can handle keys that are 256 bits large, or binary numbers that have a length of 256 digits. This means that there are 2$\hat{}$256 possible different keys. Typically, if an encryption algorithm is only vulnerable to Brute force attacks, it is considered secure. The time it would take to randomly guess the correct key as long as the length of the key is sufficient is negligible, especially considering it would be very difficult to prevent attackers from carrying ou Brute Force attacks given the simplistic nature of the attack

4.3 Implementation of AES or Similar Methods

Encryption methods are only effective when implemented properly. There are various quirks with each method that Fig. 2. Doctor is able to send and re-

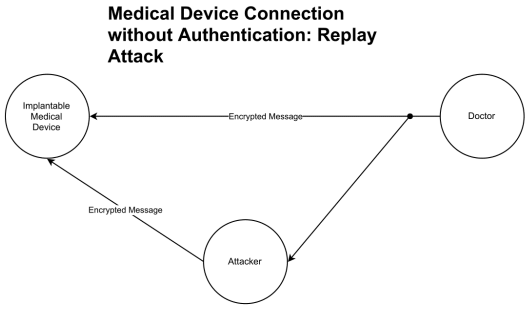

Figure 2: Medical Device Connection without Authentication: Replay Attack.

ceive Encrypted Messages to the device. While the attacker is able to see these messages, because they are encrypted they cannot understand the messages. The attacker is still able to send the same message to the devices, using a replay attack. The device will still understand the attacker's message and perform the operations described in the attacker's copy of the original message. requires proper setup and implementation. In recent years, the biggest cause of security breaches has been human error. Despite having advanced and effective methods of providing security for these devices, people often do not make use of them. Increased security comes at the cost of reduced ease of access and convenience. In the case of medical devices, the security protocols in place may even provide an obstacle in the event of a device failure. For example, if login credentials are required to access the device one of the few people that would know the login credentials of the device, the user, may be in a critical condition, and the paramedics would have trouble accessing it[4].

5 Strong Authentication Methods

The FDA also requires medical devices to Authenticate communication between outside users such as the patient and the doctor, and the medical device itself. Encryption exclusively handles the issue of making sure data cannot be intercepted and read by an outside observer, but by itself is not enough to ensure the total security of medical implants or other devices. While proper encryption methods prevents attackers from learning just about any information within a message, it does not ensure that the message comes from a trustworthy source or has not otherwise been tampered with. For example, in a system secured only with encryption, an attacker could pose as the doctor and send faulty signals to the medical device in an attempt to force it to perform undesired tasks, or send faulty information from the medical device to the doctor or hospital in an attempt to misinform the people managing the device. To prevent this, authentication methods are put into place

5.1 Message Authentication Certificates

Authentication methods aim to prove that any message is from who they claim to be. A very common way to do this is to run various mathematical operations on the original message, similar to encryption, to create a Message Authentication Certificate (MAC) tag. This MAC tag is then attached to the original message, and the two of them are sent together as a single message. When the recipient of the message decrypts the message, they can check the MAC tag to ensure the message has not been tampered with. This works because if the message has been tampered with in any way, after decrypting the tampered message the MAC tag will not be correct after all the scrambling that the encryption and decryption process creates. What this method by itself does not address is the potential for a replay attack, which was a security hole in various medical devices that used only basic encryption protocols but not authentication

5.2 Replay Attacks and Secure Channels

A replay attack is when an attacker intercepts a message, holds onto it, and can then resend that original message as many times as he likes. Even though the first message was sent with good intentions, repeating the message could be harmful. For example, consider if the original message was one that told the de-

vice to restart and the attacker intercepted that message. While the original restart may have been sent in goodwill, the attacker would now be able to tell the device to restart as often as he likes potentially leading to unintended, undesired side-effects. To prevent against this, further authentication methods need to be put into place. One such method is the use of secure channels to send messages. The goal of secure channels is to first prove that a message is from the legitimate sender, and then once the sender has been proven any messages sent between the parties can be trusted to originate from the original sender. Secure channels modify messages over time while the channel is being used. When using a secure channel the values used to encrypt and decrypt modify so that even if the same message in sent exact is sent twice, such as what occurs during a replay attack, the message only properly encrypts and decrypts if it is from someone with the same key that established the channel. Each time a secure channel is established, both parties need to reshare keys to establish a new secure channel. By using a secure channel, replay attacks are prevented; however, in order to establish a connection properly the two parties involved need to somehow share an authorization key between each other. This becomes a bit more complicated when one of the parties is not a person, but rather a medical implant that can only be accessed wirelessly. Because of this, additional steps are necessary in sending authenticated messages to and from medical devices

5.3 Sharing of Keys

channel create a value that attackers cannot pull from intercepted messages. It is possible however, and the Diffie-Hellman protocol shows that property rather simply, even though it is not the main protocol used in authentication. The Diffie-Hellman protocol makes use of performing mathematical operations by using a secret number that only personal party knows with publicly declared numbers that both parties agree on. Diffie-Hellman takes the public number, and raises it to the power of their secret number. The parties then send the numbers resulting from this operation to each other, and then each party then raises the newly received number to the power of their original secret number and both parties should have the same end result. This works because raising numbers to two or more certain powers does not depend on the order that operations were performed, as shown in Equation

Authentication protocols, including Diffie-Hellman itself, makes use of Modular Arithmetic and other methods to further obscure the original numbers. The end result is that both parties are able to send secret information over to each other, despite having to send that information over a public channel. By doing this, the two parties can share values that are then used to create the keys necessary to establish a secure channel. Once a secure channel is made, attackers will be unable to impersonate the senders, and in the case of medical implants, could not send faulty messages to and from the device

6 Privileged User

Another requirement that the FDA has recently made for medical implants is the function of a Privileged user. A Privileged user is a user that has total, administrative access to a device. Privileged users have been used in the past for operating systems such as Linux and Windows, and the function of an administrator has been to restrict potentially harmful commands from regular users. In Linux administrators are often referred to as the “root” user, and has the potential to create, access, and delete any files on the system [6] . Fig. 3. Doctor is able to communicate with the medical device using a secure channel. The Attacker can still see the encrypted messages, they are unable to communicate directly with the device, because the device refuses connections not sent through the secure channel.

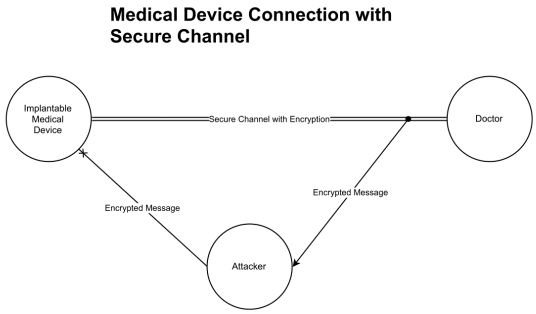

Figure 3: Medical Device Connection sith Secure Channel.

6.1 Role of Privileged Users

Managing system files is often necessary for regular maintenance such as updating the system, adding new users, installing new software, and other tasks. While the system protects itself from potentially harmful actions of regular users such as deleting system files, installing untrusted software, and accessing files with sensitive system information, the system does not protect itself against the privileged user. For this reason, it is not safe to use the privileged user account as a main

account in a system, even for the person in charge of managing the system. Accidently deleting important files or other potential risks of being logged in as the privileged user means that it is often best to only use the privileged user account when immediately necessary, and use a regular account otherwise. The presence of a privileged user is important for keeping the system safe from regular users and managing the system; however, given the control a privileged user has over a system security is essential when implementing one. In Linux systems, connecting to the root account used to be done by logging in directly as the root user, providing both a username and password for the root account. A major risk of this method means giving total access of the system to a single person or multiple people. More recently, Linux has made use of specialized, specific privileges for the system's administrators through use of the "sudo" command [6]. When a user needs to perform maintenance on a system, rather than logging in as the root user and gaining total control over the system, they use the sudo command to gain root level access for only the current command they are attempting to perform. At the time of using the sudo command, a user must provide his own login credentials, and not the root user's credentials. This means that total control is never given to the user, and reduces the likelihood that the system is either accidentally or maliciously tampered with. Furthermore, individual administrative users can be given different permissions for managing the system. For example, some might only be able to install software while other administrative users may be able to mount disks and view system logs. The other advantage of this method is that administrative tasks link back to the person performing them, rather than a singular privileged user account. These actions can all be logged so the actions of the privileged users, which are especially important, can be monitored [6].

6.2 Risks of Full Access

As it stands, there are many medical devices that do not make proper use of the privileged user method, either from allowing full control to anybody that has access including attackers, mismanaging of administrative permissions, or not properly securing current administrator accounts. Even when privileged user systems are set in place, they are not always secure. Many devices that are already in use make use of administrator accounts, but the login credentials for many of these accounts use the default password that anybody with the manual could lookup and use to gain full control of the implantable medical device. When a person gains full access to the device they gain access to all of the information and operations of the device. This would allow attackers to take advantage of lethal tactics such as administering repeated shocks in a pacemaker or altering the settings of the device to be inappropriate for the patient or update the firmware of the device to a version that is more vulnerable to other attacks. In addition to this, an attacker with full control would be able to alter the log files to make it appear as though nothing suspicious has occurred. This is especially important, as the information within the log files could play a major role in investigations relating to device malfunction. Currently, investigators can review the events that previously took place in the case of lethal attacks using implanted medical devices, although by allowing attackers to gain full administrative access to a device it is possible that a smart attacker would be able to cover up or destroy any trace of wrongdoing [6].

7 Other Potential Attacks

Even when using proper encryption, authentication, and privileged user security methods wireless devices of all sorts are still vulnerable to various other types of attacks. Encryption prevents attackers from eavesdropping on data travelling to and from the device, authentication ensures communication is from a reliable source and secure channels prevents replay attacks, and proper restriction of administrative rights prevents attackers from modifying devices and viewing or altering history logs; however, attackers still have the potential to cause the device to malfunction even without gaining direct access to it. One method is to create interference of some sort, blocking any communication made to the device. This jamming could take the form of electromagnetic interference being sent to the device. There is a precedent for electromagnetic interference being possible to cause a device to malfunction, as was shown by research involving the effects of walk through medical detectors on the device. It has been shown that over time, the electromagnetic interference created by the metal detectors were able to cause test devices to malfunction, and attacker's could possibly use similar technology to malfunction a target device [7].

Another method of blocking access to the device involves the use of Dedicated Denial of Service (DDoS) attacks. When attempting to connect to just about any device, including implantable medical devices, the attempted connection needs to be checked if it is from a legitimate source. DDoS attacks are conducted when an attacker makes repeated attempted connections to an individual device that are so plentiful that the device is unable to process all the connections and

becomes inaccessible [8]. In 2016, DDoS reached over 100 Gigabits per second, much greater than a simple medical device would be able to handle [9]. By creating so many illegitimate connection to the device, it is not able to find legitimate connections. In a regular setting this would create a scenario where the device is inaccessible which is already bad for various reasons, but in the case of implantable medical devices DDoS attacks can be much more damaging.

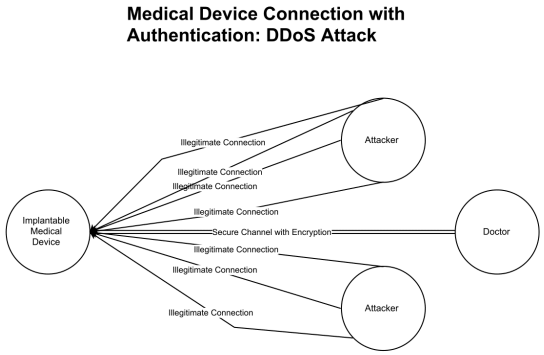

Figure 4: Medical Device Connection with Authentication:DDoS Attack.

Fig. 4. Doctor attempts to make a connection to the device, but the Attacker has made so many Illegitimate connection attempts that the device is unable to find and respond to the doctors connection. The attacker never gains access to the device, but shuts out others from accessing and drains battery from the Implantable Medical Device. This is because with each connection the device requires a certain amount of power to check if the connection is real or if it is an illegitimate attack as part of a DDoS attack. Even if the device turns away all illegitimate connections, it still requires power to filter through them. This means that DDoS attacks, or other repeated connection attacks, against implantable medical devices can quickly drain battery power from the device, causing it to malfunction [10]. Preventing DDoS attacks is rather tricky, as need hardly any information to perform one. All an attacker needs is to find the device or server he wants to connect to, and automate repeated attempts to connect to the device. Current DDoS prevention techniques take the form of redirecting traffic during a DDoS attack to somewhere that can handle the bandwidth traffic such as an internet service provider or the cloud, but implementing these techniques into medical devices seems rather difficult given the restrictions regarding processing power and hardware that have already been an obstacle to cyber security measures being implemented in the devices [10]. In this case, devices would likely have to be given special instructions in handling a DDoS attack, perhaps by temporarily refusing any outside connections to prevent the battery of the device from being forcefully drained. The downside of this approach is that if the device needs to be accessed while it is under attack, it would not be able to connect while it has temporarily set itself to refuse connections.

8 Implementation Obstacles

Properly implementing encryption, authentication, and privileged users would greatly increase the security of implantable medical devices; however, there are a few reasons they have not already been implemented. The medical field is a very divided field with research focused all over the place, and each of these individual sections of the medical field are very small and focused on their designated to optimizing and improving the performance of the devices they are researching. While medical field research is focused on getting these implantable medical devices as small and efficient as possible, researching and implementing cyber security methods would slow this down. Implementing cyber security protocols into a medical device could have a negative impact on the device's performance, and this is often undesirable. Another issue is the cost of cyber security research, as only 3% of funding in the medical field goes to cyber security, where on average other fields allot 11% of funding to cyber security [3]. This means that the cyber security sector of the medical field is extremely small in order to physically be placed inside a person's body. These reasons account for most of the lack of security in implantable medical devices, but another reason could also be part of the issue: the need for security in implantable medical devices is a concern that has only applied for the last few years [3]. Not too long ago, implantable medical devices were secure in the idea that the only way to access them was physically. It is not until recent advances that medical devices such as pacemakers and insulin pumps were able to take advantage of wireless connections to monitor a patient, update firmware, and manage any other functions. Because of this, the security of medical devices still remains in a similar state to the security of computers before cyber security was implemented. During that time, the only security method was hoping that people would either not have access to or be uninterested in compromising information. Recently, the need for cyber security within the medical field and within implantable medical devices has grown to greater focus. While old devices may still be lack-

ing in encryption, authentication, and proper use of the privileged user and other security requirements, but going forward new devices are being required to make use of these security methods by the FDA, FBI, and Department of Homeland Security.

9 Conclusion

While the medical field has been optimizing implantable medical devices in form and function, security has fallen behind. While it is unlikely for a person to be attacked with lethal intent through compromising a medical device, it still has left many people concerned. This is because attacks can often still be traced even when performed through these means. What is more likely to occur is that an attacker will eavesdropping on personal information going to and from the device. Wireless connections have only been a part of medical implants for a very short period of time, so security measures within the medical field has only been in demand for an equally short time. Because of this, many devices lack the encryption, authentication, and access restrictions that are necessary to protect these devices and the information within these devices from outside attackers. Even when proper security measures are put into place, the device has to be setup in a way to take full advantage of the implemented security methods, such as not using default passwords and properly using a secured channel to prevent replay attacks. Designers in the medical field would also be required to become familiar with cyber security methods, as the implementation of many of these methods has to be taken into account from the beginning of the design process. This is because running security methods in these devices takes up resources and memory that used to be dedicated entirely to the performance of the device. The guidelines to follow these security protocols has recently been set by the FDA, so future devices should start using these methods.

References:

[1] Owens B. Stronger rules needed for medical device cybersecurity. The Lancet, Vol. 387, 1384, April 2016.

[2] Aram S, Shirvani R, Pasero E, and Chouikha M. Implantable Medical Devices; Networking Security Survey. Journal of Internet Services and Information Security, Vol. 6, No. 3, August 2016, Pages 40-60. Available: http://isyou.info/jisis/vol6/no3/jisis-2016-vol6-no3-03.pdf

[3] Woods M, Cardiac defibrillators need to have a bulletproof vest: the national security risk posed by the lack of cybersecurity in implantable medical devices. Nova law review, Vol. 41, No. 3, Spring 2017.

[4] Ferguson N, Schneier B, and Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Wiley, March 2010. ISBN: 978-0-470-47424-2.

[5] Brand A, Medical device security: patient safety and cost considerations. Healthcare Financial Management, Feb. 2017, Pages 28-33.

[6] Shackleford D, Keys to the Kingdom: Monitoring Privileged User Actions for Security and Compliance. SANS Institute, May 2010. Available: https://www.sans.org/reading-room/whitepapers/analyst/keys-kingdom-monitoring-privileged-user-actions-security-compliance-34890

[7] Guag J, Addissie B, and Witters D, Personal medical electronic devices and walk-through metal detector security systems: assessing electromagnetic interference effects. Biomedical engineering online, Vol. 16, No. 1, March 2017.

[8] Xie Y and Yu S, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," in IEEE/ACM Transactions on Networking, vol. 17, no. 1, pp. 15-25, Feb. 2009.

[9] Akamai Releases Third Quarter 2016 State of the Internet / Security Report: Q3 report highlights a 138 percent YoY increase in total DDoS attacks greater than 100 Gbps with two record DDoS attacks caused by the Mirai Botnet. PR Newswire Association LLC, November 2016.

[10] Ellouze N, Rekhis S, Allouche M, and Boudriga N Digital Investigation of Security Attacks on Cardiac Implantable Medical Devices. October 2014. Available: https://arxiv.org/pdf/1410.4303v1.pdf