4-2020

Cyber Security in the Healthcare Industry

Giovanni Ordonez
DePauw University

Cyber Security in the Healthcare Industry

Author: Giovanni Ordonez

DePauw University Honors Scholar Program, Class of 2020, Sponsor: Kevin Moore, Committee members: Khadija Stewart, Chad Byers, Vaughn Selvey

Introduction

During my Junior year, Spring Semester at DePauw University, I took an Honors Course called BioEthics. In this course, we discussed many cases where decision making, in a medical context, is very hard and how using the principles of ethics can make the decision making process a bit easier when dealing with emotion-driven situations/cases. Towards the end of the semester, I wrote a paper about ethics in medical decision making. Since I am a Computer Science major, I began to research if Computer Science had any connection with medicine and if it did then how would ethics be involved? During my research, I learned about medical devices which are any technologies that are used in medicine, but specifically pacemakers. A pacemaker is a device that physicians use to monitor a patient's heartbeat. During that time, my grandmother was admitted into a hospital and I found out that she had a pacemaker installed in order to monitor her heart's beat. However, during my research, I found out that pacemakers were vulnerable to hacking and that a security expert by the name of Barnaby Jack discovered how to hack a pacemaker. He was supposed to make a presentation on the security issues of pacemakers at a Black Hat conference, a well known hacking conference, but passed away days before the conference. After finding out that it is possible to hack into a pacemaker and that there is a possibility that the hacker can send a shock through the pacemaker that is connected to the heart, it terrified me and it only made me more motivated to learn more about this medical device. Through my experience with finding out that my grandmother had a pacemaker and researching about the pacemaker, I realized that I wanted more people to know about these security issues and also be able to help in fixing these vulnerabilities so that patients are not at risk of being hurt or even killed from the same medicals devices that are supposed to aid the patients. It was through my individual interest in pacemakers that led me to learn about the massive dangers of cybersecurity and how it is heavily related to medicine. Not only are there dangers with the use of some medical devices but there are also other vectors by which attackers can do some harm.

There have been many cases of hackers successfully attacking hospitals and it has resulted in millions of dollars in monetary loss. As of 2019, there has been a 25 billion dollar estimated loss in the healthcare industry due to cyberattacks. As well as, on average there are about 113,491 sensitive patient files that are lost from cybersecurity attacks (Sobers, 2020). Given our current times of pursuing technological innovation and heavily relying on technology, the level of danger only increases when companies and innovators create products that are driven by monetary benefit, functionality, and when not much concern is given towards the security of their products.

The purpose of this thesis is to not only bring to light some of the attacks that hackers can perform on medical devices, but also attacks that are present in the context of medicine. By analyzing certain attacks that hackers are capable of doing, I want to bring to attention the lack of security in many hospitals and medical devices so that both the general public and manufacturers are aware of the need for better security. This thesis will first give an overview of the principle of ethics, security flaws of medical devices (Internet of Things devices), flaws in hospital networks, and lastly discuss the weakest link of healthcare security, the human factor.

Ethics

Cybersecurity in healthcare is not a new topic as there are constant articles and news reports made on cases where there has been a hacker who has stolen some information or any other similar case from which a hacker is attempting to get some benefit. Most common attacks are usually ransomware attacks where a hacker steals some information and the hacker asks for money in return for that stolen information. However, the ways from which a hacker is able to cause harm is vast and not all of these forms of attacks are known. For example, attacks on medical devices such as pacemakers. The easiest way to not risk the chance of a cyber attack would be to not use these sorts of devices, but this is not an option that patients who rely on them have. Ironically, it is these same devices that are helping some patients that have the potential to kill them and so the question is whether it is correct to administer such devices when there is always a possibility to harm the patients? Hence I introduce these ethical principles as a guide to discuss if some of these devices are ethically correct to administer to patients. Furthermore not only explore this question but also see if there is a way to add security measures on such devices or other vectors of attacks so that patients can continue to use medical devices and other services with ease in mind that there isn't some other source of harm that can come their way.

The basis for ethics, particularly bioethics in the context of medicine, is to lay down a framework for better decision making on what should be done when taking care of people. Bioethics tackles questions concerning basic human values such as humans' rights to life, the right or wrongs of cases in hospitals, medical technology, medicine, physicians, and about the responsibility that hospitals have for the life and health of their patients (Disabled World, 2019). Within bioethics, there are four principles that form the framework for moral reasoning. In many cases involving healthcare institutions, there can be a lot of situations where moral conflicts can occur and it is hard to decide on a certain action to take. By using these four principles, it is easier to not make emotion-driven decisions that could not be at the best benefit of the patient. One of the main values behind these principles is human life. Meaning that when dealing with decision making, the patient's benefit is the first priority. That is why I suggest having these principles as a common ground in order to address issues within the healthcare industry.

The four principles of bioethics consist of Nonmaleficence, Justice, Beneficence, and Autonomy. Nonmaleficence meaning that physicians should not cause patients harm or at the very least the harm received should not outweigh the patient's benefit from going through a certain procedure. For example, if the patient is in a life or death situation and doing surgery could save their life then that surgery has a greater benefit to the patient than the pain from getting the surgery. Hence under the principle of Nonmaleficence, it is ethically correct for the patient to go through the surgery. Justice meaning that benefits and risks should be fairly distributed. This means that patients who are in similar situations should be treated the same. Beneficence means that physicians should consider the risks and benefits before conducting a procedure as the patient's benefit is the sole purpose of considering a certain procedure. Lastly, Autonomy means that physicians should respect the decision of the patient. Allowing patients to make their own decisions on the consensus that the patients are well informed about their situation. In the case of Autonomy, it is up to the patient to decide what they want to do regardless of what the physician recommends as it is their autonomous right to decide for themselves. By using these principles as a foundation, I will explain why certain systems and devices being used need more secure and suggest some changes that should be made to better manage healthcare issues (Disabled World, 2019).

First, I want to bring to light some of the most concerning case studies in medicine that involve the use of modern technology for the purposes of diagnosis and treatment. There are multiple types of security attacks that can occur in the medical field that fall under Data Security (also known as Information Security), Hardware Security, Network Security, and many more. Data Security consists of a list of practices that are done for the purpose of keeping data secure from unauthorized individuals during both the transmission of data and while data is stored (FruhlInger). Hardware Security, however, focuses on the protection of systems, at the physical layer, from vulnerabilities (Levine and Pipikaite). I would like to first separate the types into two main branches to analyze healthcare vulnerabilities. Data Security and Hardware Security. Data Security in medicine can be described as the field that examines security flaws in the management of patient data. However, it is very possible that hardware security flaws can lead to patient information being leaked but the approaches of these attacks are different. When strictly speaking about Data Security I am referring to the security in the hospital's infrastructure such as the version of the Operating System being used, mal-practices from physicians using certain technology in an insecure manner, or the access privileges given to employees working at hospitals. In comparison to Hardware Security which is concerning the security flaws in Internet of Things devices (IoT devices), devices that interact with networks by sending or receiving data, such as pacemakers, MRI machines which are devices used to develop medical images of a patient’s body, and other types of medical devices. Another important sector in security that I want to discuss is Network Security as it affects both hardware security and data security since they both involve the usage of networks. Network security can be described as techniques used to protect the usability and integrity of networks and data (Cisco, 2020). For example, a medical device such as an MRI (IoT device) machine is connected to the network so that medical images can be sent and stored in some database so that physicians are able to look at the patient records. In order for this process to work, the data transferred has to be connected to some network so that the data can be both stored in the database and also so that physicians are able to get access to this data. However, by dividing Hardware security and Data Security, we can better analyze certain attacks by identifying vulnerabilities found within hardware systems and IoT devices and see how in combination with networks these vulnerabilities can create bigger vectors of attack. Furthermore, I will bring to light this common theme in medical device development where the functionality, user-friendliness, or usability of the product seems to outweigh the number of security features invested to make the medical devices safe.

The Internet of Things is a bit tricky to make more secure as this involves not just the hospitals but also the manufacturing companies that create the devices. In order to be able to make these devices more secure, there needs to be a collaborative effort from both the hospitals and the companies involved in the production of the devices. Ultimately, by analyzing these medical devices I want to bring to attention some of the grave dangers that are present in the use of such medical devices and yet are still being used on patients.

Security of IoT Devices

The three main sources of security errors are with the device's design, software risks/vulnerabilities, and human factors that make the Internet of Things devices less secure (Aram, Rouzbeh, Pasero, and Chouikha, 47). There are many devices that are designed in a way that hinders users from not being able to access certain data from the devices. For example, if devices such as implants were encrypted then doctors would not be able to get quick access to the patient data which is essential in emergency situations. Software risks arise from the architectural designs of the IoT devices and also how engineers create the device. Lastly is the human factor which arises from not handling the devices properly. Therefore the risk of security errors is rather large and in conjunction with the IoT architecture design, there are even more forms of attack that can be performed.

Internet of Things (IoT) devices typically use confidential data. This can be information that is found in factories, businesses, or even health monitoring devices. There are a variety of devices that are used for many different services, but they share some generic architecture for the functionality of the IoT devices. While some devices may implement a variance of this general architecture, they are usually based on the same design model. Therefore, we will look at a general architecture design, analyze the purposes of its different layers, and then explain why there can be some flaws in the way the design was constructed.

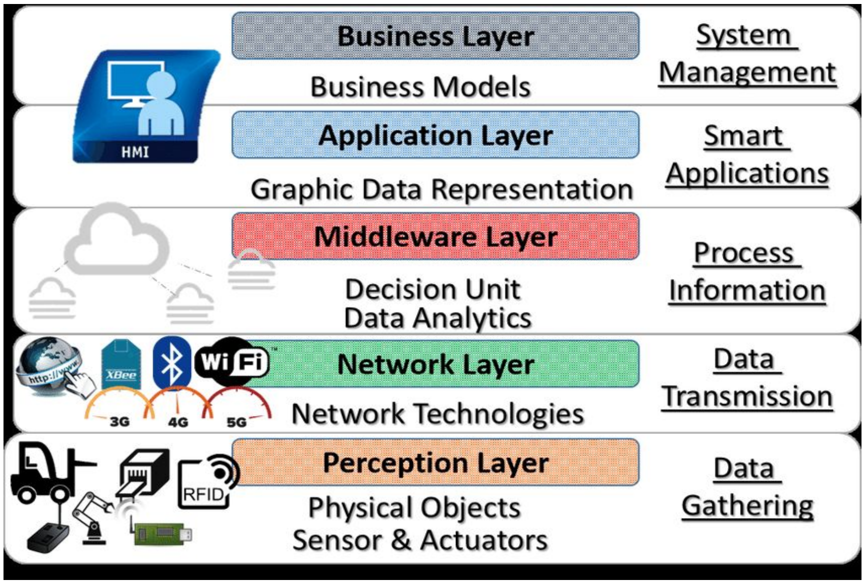


Figure 1: Five Layer IoT Device Architecture (Sethi and Sarangi, 2017)

This generic Internet of Things architecture in Figure 1 is composed of the Application Layer, Network Layer, and the Perception Layer. However, due to the fact that IoT devices are very diverse and heterogeneous, we need to introduce another layer called the Middleware layer which provides extra services such as processing, analyzing, and storing massive amounts of data that is given by the Network Layer (Sethi and Sarangi, 2017). Also, if the IoT device is being used in a business setting or on a bigger scale then there is also the usage of the Business Layer which handles the overall management of a multitude of IoT devices used in a company/organization. However, since the Business layer is concerning the management of a multitude of devices, we will focus on the other layers as they focus on the individual devices' components. In the following sections, we will analyze each of the layers starting from the bottom at the Perception layer up to the Application layer as the upper layers are using the services that are provided by the Perception Later.

Briefly looking at the layers, the Perception Layer/physical devices uses sensors for sensing and obtaining information. The second layer is the Network Layer which is responsible for connecting devices and other servers via some network. It also collects data from the perception layer and transmits it to the upper layers of the architecture. Some of the issues that arise from this layer are information sharing and the transmission of data. The third layer is the Middleware Level and this level is in charge of linking the system to technologies such as databases, the cloud, and performs data processing and storage. Some of the issues that arise from this level are handling security in the database and in the cloud storage. Lastly, the Application Layer, which is responsible for providing services to the user and also used to manage and process data that is given by the middleware layer. Some of the issues that can occur in this level involve the transfer of data and the access to confidential user data (Chen, Zhang, Li, *et al.,* 98-99).

Given that all of these flaws are present, we can begin to see just how dangerous IoT devices can be if the architecture development of the IoT devices is not created with extreme care. Yet how is it that even with these amounts of errors, hospitals still use IoT devices and depend heavily on them for managing patient data? Let's dive deeper into each layer to see all of the components within the layers and see how there is an array of attacks that can be executed to infiltrate the different layers of IoT devices.

Perception Layer

Beginning from the bottom of the architecture, the Perception Layer is vulnerable to attacks that target data transfer and other communications between networks. Within this layer, there are many sensory technologies and identification technologies that are used. These can be devices such as RFID tags which patients would have on their wrist. These RFID tags help physicians by allowing physicians to just scan the tags and be able to look up patient information. One of the attacks that can be directed to these RFID tags is RF Jamming which is when attackers are able to destroy the communication between the tag reader and the tag itself which hinders the physicians' capability of looking up patient records by using the RFID tag. Another attack that RFID tags are vulnerable is tag cloning which allows the attacker to make a replica of a tag. This could be dangerous because if the attacker has an RFID reader it is possible to gain access to user data if the RFID chip is not encrypted properly (Chen, Zhang, Li, *et al.,* 102-103).

The perception layer uses sensor nodes to create communications between technologies. A node is a device or a data point in a large network that serves as a connecting point from some source to some other location. There are a variety of attacks that can take advantage of these sensor nodes to stop communication, but in the context of medicine, one dangerous attack is called Sleep Deprivation Attack. This form of attack is targeted on devices and nodes so that they cannot go into sleep mode. The attack keeps the node busy so that the device cannot go into sleep mode. Meaning that their battery life is drained over time of usage. While this may not sound so threatening, when considering implantable devices that rely heavily on their ability to have a battery life that lasts for at least two years, this can pose a grave danger as devices such as pacemakers will run out of battery and a re-implantation will be needed. In cases where the pacemaker is heavily relied on to monitor the patient's heart, monitoring time will be lost in having to reimplant the patient; Assuming that the patient is in a condition to go through the reimplantation surgery. Similarly with Insulin pumps, which are devices that deliver insulin to the body to manage blood sugar levels, that are implanted. High levels of blood sugar can be life-threatening and insulin pumps are required. Hence in the case where the battery life dies, that immediate insulin release from the pump will not be there and that can be the end of the patient when insulin is needed immediately (Chen, Zhang, Li, *et al.,*102-103).

Network Layer

In the Network Layer, the attacks can vary depending on the protocols that are being used to create network connections/communications. The protocols that are commonly used are Wi-Fi, Bluetooth, and Zigbee. Therefore, this layer can be the most dangerous as there is a bigger array of attacks since each device in the network can be very different from each other. Meaning that it is harder to protect all devices in the same fashion as they all have different vulnerabilities. That being said, one of the most common types of attack are DoS/DDoS (denial of service)attacks which is when an attacker sends multiple requests to a website which causes huge traffic and does not allow users from being able to use a website’s services (Chen, Zhang, Li, *et al.,* 101-102).

For the purpose of this paper, I will look at the most commonly used protocol being Wi-Fi to see what are some approaches to the exploitation of medical devices that use these protocols. Network Security in Wi-Fi networks is achieved through the use of encryption. There are two sectors in Wi-Fi security which are privacy and authentication mechanisms. Privacy is the restriction of access to some network for users who are not authorized. Authentication requires the inputting of credentials from users to get access to the network. In Wi-Fi, encryption is a popular method to ensure privacy. To make it easier to understand, I will use an example to explain how communication is done over a network. When data is sent over a network there are two entities. One sends some data and one receives that data. Let’s say that the sender wants to send some data to the receiver without anyone else being able to see what that data is. This would require some sort of encryption so that the data can be coded in a way that is not readable to others. Once the receiver has gotten the data they need to be able to decrypt it and to do so they would need to know how the encryption algorithm works. Typically what is needed is some key to be able to decrypt the data. Imagine that the data is sent in a box with a lock and in order to see the data you need to open the lock with some key.

The lock represents the encryption added on the data and the need for a key in the algorithm represents the same key needed to open the lock to see the data inside. However in order for both sides to be able to open and decrypt the data the key needs to be known by both the sender and the receiver. This process of exchanging keys is known as a handshake and this key then used for the encryption/decryption process.

One of the most common security tools is Wired Equivalent Privacy (WEP). WEP is a security algorithm for the IEEE 802.11, a standard for information technology telecommunications and information exchange created by the Institute of Electrical and Electronics Engineers (IEEE), wireless networks. IEEE has created many standards by which engineers should follow. IEEE 802.11 was developed in 1999 as one of the earliest wireless security protocols, but it was later found out that its encryption algorithm could be decrypted. As well as other vulnerabilities such as hackers being able to “redirect encrypted data to externally controlled IP (Internet Protocol) addresses which is unique to any computer, laptop, or printer. An IP address can be thought of as a street address which pinpoints to some location in the world except instead of a home being at the address, the IP locates a specific machine. Due to the number of vulnerabilities that are present in WEP, this network protocol is not used anymore but there are still some old routers that still use this as an encryption mechanism to have “privacy” in their Wi-Fi network. This can occur in older companies or businesses who have not updated their technology and if so they are vulnerable to attacks where the data transfer can be easily grabbed and decrypted (Aram, Shirvani, *et al.* 47).

After WEP was found insecure, WAP (Wireless Application Protocol) was created to be more secure than WEP. WAP uses an encryption method called TKIP(temporal key integrity). Essentially the algorithm would use some value, known as a key, which dynamically changes as it is being used and provides better security as there would not be a single key that could be used to access a network. However, there are also some vulnerabilities found. Afterward, WPA2 was created which uses AES (advanced encryption standard) which was thought to be so secure that even the government has adopted this security protocol today. The AES algorithm is a symmetric-key algorithm and that means that the same value key is used for both encrypting and decrypting of data that passes through a network. As well as in 2018, the Wi-Fi Alliance announced the release of WPA3 which replaces the Pre-Shared Key (PSK) exchange, which is how keys are exchanged between two parties before the sending of any data. Instead with Simultaneous Authentication of Equals, a new form of encryption that requires password authentication before a connection can be made over a network. (Burke, 2018)

In 2018, there were some vulnerabilities that were found in WPA2 leading to attack called Key Reinstallation Attack (KRACK). KRACK attacks work by tricking the victim into reusing a currently used key. In terms of the attack, that would mean that it can be possible to decrypt all data that the victim transmits. What this means is that in order to secure or guarantee the WPA2 is for the key to only be used once, but since that is not the case, an attacker can abuse this vulnerability (Mathy and Frank, 2017).

Just last year, 2019, a vulnerability was also found in WPA3 and this brought forth the DragonBlood attack. The WPA3 was said to be so good that it was almost impossible to break the password of the network. However, it was later found that "an attacker within range of some victim, could get access to the password. The flaws in WPA3 fall under two categories. One concerning downgrade attacks on devices that are capable of using WPA3 and the second is concerning weaknesses in the Dragonfly handshake (better known as Simultaneous Authentication of Equals or SAE) of WPA3. The first category was found after discovering that it is possible to create a rogue network and force clients to change from WPA3 to connecting to a rouge WPA2-only network. Therefore, an attacker can then recover network passwords by using techniques such as brute-force, a trial-and-error technique until the password is found. As well as take advantage of any vulnerabilities that were found with WPA2. The second category is a flaw with the Dragonfly handshake which is derived from the algorithm used in order to authenticate the communication between two users. (Mathy and Eyal, 2020)

Dragonfly Algorithm Idea:

```
for (counter = 1; counter < 256; counter++)
    value = hash(pw, counter, add1, add2)
    if value >= p
    p = $value^{(p-1)/q}$
    return p
```

Figure 2: Dragonfly Algorithm

The idea of this algorithm is that you have two addresses or destinations that correspond to the users and then you have a shared password that will be encrypted into a single value. This single value is denoted in Figure 2 as ‘value. Each user is to input a common password and then the algorithm is run to allow communication access. However, based on the information of the password and the two destination addresses, it can affect the size of the encrypted value. If the encrypted value is greater than this ‘p’ value seen in Figure 2, a predefined value that is derived from a crypto group which is a set of values used for encryption purposes, then the algorithm will be executed again. This means that based on the size of the encrypted value, it will determine how many iterations the algorithm must conduct before the connection is made. This can be taken advantage of because depending on the time it takes for the connection, you can analyze it to determine the size of the encrypted value. In combination with a spoofing attack, an attack where communication from an unknown source is disguised as some known source, an attacker could determine a client’s address. Since the encrypted value is a combination of the password, counter, and the address, an attacker would have the values to the counter based on the time it takes for the connection to complete. As well as the addresses because of the spoofing attack. Once they have all of this information then they can conduct a brute-force attack or some other attack to crack passwords and then see if the encrypted values match. If they do then that means that they have the password. This analysis of time and data gained from the implementation of some system is called a side-channel attack or a timing attack for this case (Mathy and Eyal, 2020).

Middleware layer

In the Middleware layer, the attacks typically target the quality of service that is provided and exploit user privacy. Some common attacks are SQL injection and Flooding attack in Cloud. The most common attack is SQL injection which is when an attacker inputs code, called SQL, that is used in the database. This can happen when an attacker inputs code into the search bar of a website. The code is submitted to the server where the code is then sent to the database. If that code works in the database then the attacker can gain access to information that a user should not have access to. This attack is not difficult to conduct but the results of a successful injection can be very devastating. In the context of hospitals, this could mean accessing patients' information. Recently cloud computing has become more common and essentially it is data storage that is available to users via the internet. Microsoft defines cloud computing as the "delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale." An example of cloud computing is dropbox, which allows users to store data. While it does have many benefits, given that this technology is still very new, many of the issues fall on how the developers use this technology. Attacks such as Flood Attacks can occur when a DoS attack is done but onto a cloud service. Meaning that an attacker will send multiple requests to the cloud which can hinder the quality of service (Chen, Zhang, Li, *et al.,*101).

Application Layer

Taking a deeper look at the application layer, the main form of attacks are those that aim at getting access to sensitive data by exploiting vulnerabilities in the application. The application can be in the form of a website on a browser or some app on a device. Common attacks on these applications are code injections, authentication attacks, and authorization attacks. Code injection is when an attacker injects some code into the application such as, for example, inputting a script in the HTML code that makes up a page on a website. This can be used to "steal data, get system control, and to propagate worms." Meaning that if successfully executed it is possible to not only steal user data but also possible to shut down the entire application. Authentication and Authorization issues are a big issue in IoT devices. Authentication is the requirement of credentials from users to get access to a network. There are still many flaws in providing total authentication and this happens because of "over-privileges" that allow the device to have access to information that it should not have access to such as a user's private information. This means that if an attacker gets access to the device they can get access to user information (Chen, Zhang, Li, *et al.,* 99-100).

After considering the many ways that attackers can gain access to private data and devices, it becomes very concerning as to the security of the devices. In the context of medicines, these attacks are not directly life-threatening, but the side-products of such attacks can cause danger ranging from data loss to potential death. Given that this IoT architecture we have discussed is just a general architecture, we need to look deeper at individual IoT devices that are used in hospitals to understand where the architecture plays a role in the specific device and also what are some specific attacks that are concerned with that specific device. I will explain some risks of devices such as insulin pumps, pacemakers, and MRI machines. As well as describe why they have dangerous flaws, provide some suggestions as to how to better protect them, and why manufacturers need to have security in mind when creating medical devices.

Brain Implants

One of the older forms of therapy for depression is known as Electroconvulsive therapy. Doctors have used electricity to jolt brains out of depression for decades. Electroconvulsive therapy was first introduced in the 1930s, but by the 1950s this became a common treatment to fight depression. As this technique further developed, its modern form has been implemented through the use of attaching tiny electrodes, an electrical conductor by which electric current can pass, in the outer layer of the brain to monitor for any seizures that might occur. With these electrodes, physicians are able to shock the patient in the specific location of the brain where a certain seizure might occur and be able to control that seizure. The doctors are also wanting to use this technique for the purpose of inducing certain emotions on patients suffering from depression. This would mean that if a patient is about to enter a depression crisis then with the zap of these electrodes the emotions of sadness are zapped away. The research goal is to be able to create a brain-zapping implant. These implants are small implantable devices that are able to both learn the brain's language and be able to shock the individual when depression begins to set in. (Laura 2019)

The Deep Brain Stimulation system (DBS) is the most common brain implant. It consists of electrodes that are connected to wires running under the skin. The stimulator (also called a pulse generator) has a battery, a processor, and a wireless communication antenna to allow the transfer of data and also so that doctors can program them. Meaning that there needs to be access given to the doctors. That is done via a 'back-door' into the device. A 'back-door' allows doctors to have access to the device in the case of medical emergencies where they need to be in control of the implant. This means that if that 'back-door' exists, then there also exists a vulnerability in the potential access of the implant via this access point. Now, what exactly can occur if someone gets control of the device? Some of the possibilities include the attacker inducing behavioral changes such as hypersexuality or pathological gambling by stimulating parts of the brain involved with rewards learning to make the person act in some manner. (Pycroft, 2016)

There are two different types of attacks that can occur in a cyber threat. Them being blind attacks and a targeted attack. A blind attack is when an attacker requires no specific information in order to perform the attack. In contrast to that of a targeted attack where the attacker needs to know some specific information about an individual. If the attacker is able to get personal data then the forms of attack can change. Potential brain implant attacks that can arise from blind attacks consist of: inducing stimulations, draining implant batteries, inducing tissue damage, and information theft. Compared to the potential brain implant attacks that can arise from targeted attacks which consists of impairment of motor function, alteration of impulse control, modification of emotions, inducing pain, and modification of the reward system. Given all of these approaches to attack it would seem natural to impose security measures in the construction of these implants so that cases like these will never happen, but that is actually not the case. The issue arises that during security implementation on medical devices, it typically results in the doctors having less control over the devices and they need full control in cases of emergencies or being able to monitor their patients thoroughly (Pycroft, Boccard, *et al.*, 455).

There have been some secure implant designs that have been thought of but there is a trade-off to consider. The security over the device and the specific functionalities that are wanted in the device. In the article “Brainjacking: Implant Security Issues in Invasive Neuromodulation”, there are some solutions that are considered with explanations as to why these ideas are difficult to implement and have limitations in the functionality such as the limitations of many IPGs(Implantable Pulse Generators). For example, one of the new improvements that are wanted is for a longer range of wireless communication. The newest IPGs, the portion of the implant that creates the shock stimulations, use wireless communication protocols such as Bluetooth, but in the long run manufacturers are considering using communication over transmission control protocol/internet protocol (TCP/IP) which is another protocol by which network communication can be conducted. The reason is that by doing so it will enable them to have remote control over data passed through the network and also be able to make software updates for IPGs over the Internet. As well as, manufacturers want to change from using machines to program the implants and use proprietary software that is on consumers' devices such as in their tablets and smartphones. Now the issue that arises from proprietary software running on consumer devices is that it is harder for a security analyst to get their hands on that so that means that they cannot help find security flaws (Pycroft, Boccard, *et al.*, 457).

In this same article, there were some security considerations such as the usage of a Cloaker and shield to secure the communication from the implant to the physician. Basically, a Cloaker and shield are external devices that provide an additional layer of security between the implant and any other device that is trying to connect to the implant. While this will increase security, it also requires the use of extra external devices. As well as "require the inconvenience of carrying around additional devices." Just from the word "Inconvenience", there is a clear dominance in the importance of the functionality of a product over the security of the product. This is where we can begin to see what is really important to the companies. Doing business to sell their products in a more cost-efficient way rather than implementing security protocols that need to be implemented so that there are no risks to causing any harm to a patient (Pycroft, Boccard, *et al.*, 458).

When considering the ethical implications of the inconvenience in having to carry more instruments or the inconvenience in the usage of more money during development to provide a secure infrastructure for the device, this is not ethically correct. Going back onto the principle of bioethics we can see how this clearly breaks Nonmaleficence, the idea that physicians should not be causing any harm to the patients. While it may not be the case that physicians are intentionally harming the patients as it can be very well possible that they themselves do not know the dangers. There needs to be a universal mindset change from just creating something that works and ensuring that every aspect of the device is protected. Since cyberspace is still relatively new it is still not an urgent point for companies to consider, but given the number of cases that have already occurred in healthcare systems around the world, there need to be more security measures put in place when creating new products. As we will see later, there are many hacks that have already targeted the healthcare industry and it makes it very questionable why there has not been much action taken to implement better security.

Pacemaker

A pacemaker is a device that is implanted into a patient's chest or abdomen in order to both help monitor a heart's pulse and to control abnormalities in a patient's heartbeat. There are a variety of versions of pacemakers, but they all have similar components. These being a battery, lead wires, and circuitry. The computation and engineering of the pacemaker are built into the circuitry where the microprocessor is able to run many processes based on event-driven situations received from the heart's pulses. In order to better understand the functionality of the pacemaker, I want to explain both the circuitry and the battery components of the pacemaker as those are the main components driving the pacemaker (How Products are Made, 2006).

The battery's primary function is to store enough energy to stimulate the heart with a jolt of electricity. It also provides energy for the sensors and the timing devices. It needs to also be able to generate about five volts of power, which is a little higher than the amount needed to stimulate the heart. The insulated wires are then used to pass the electricity from the battery to the heart and be able to stimulate the heart when needed. However, since internal pacemakers are implanted inside the body, the battery needs to be able to last for a long time so that there is no need to re-implant the pacemaker often. The minimum battery life needed is four years. In addition to that, there needs to be a way to accurately gauge the life-cycle of the battery so that the doctors can know when they will need to change the battery (How Products are Made, 2006).

The circuitry is composed primarily of resistors, capacitors, diodes, and semiconductors. However since microprocessors have become the standard control circuits for pacemakers and other implantable cardioverter-defibrillators (ICDs), we need to look into Processor-Based Implantable Pacemakers. A microprocessor is an integrated circuit. Microprocessors are more advanced than older circuitry and this is mainly because of the low amount of power that they consumed. That meant that the longevity of the battery was now extended. These microprocessors also allow the use of more complex algorithms and have also increased the data storage for the pacemaker. An integrated circuit is a device where all functional blocks such as transistors are fabricated on the same chip so that this small central processor is able to handle the input and output control from the software programming to the hardware circuitry. Basically, this microprocessor is a powerful chip that is able to process all the instructions needed to monitor and handle the responses to abnormalities in a patient's heart (Galla, 46).

These Processor-Based Implantable Pacemakers work in three different operating modes. The first being able to run asynchronously(in real-time) and being able to ignore any unwanted rhythm that can be made from other parts of the body that is not the heart; known as VOO mode. Mode two being 'Inhibited'. In this mode, the pacemaker senses cardiac activity and waits until it senses that there is no further cardiac activity to then deliver a stimulus. The last mode is called 'Triggered'. This is where the pacemaker senses activity and will send a stimulus in a certain desired way. A very popular microprocessor that is being used is the MSP-430F1611 because of the low level of power consumption which is essential for keeping the battery life past the four-year minimum (Chede and Kulat, 49-51).

In terms of the programming involved to make the pacemaker work in the way that it does, it is well designed. However the clear weak point of the pacemakers is if the battery were to die. If an attacker were to successfully conduct an attack such as a Sleep attack, it could deplenish the battery life of the pacemaker if not kill it completely. Not only would it result in the patient's heart not being monitored, but it would result in the patient needing a re-implantation as the pacemaker is needed to keep constant monitoring of their heartbeat in the case of an emergency. However, it is always possible that during that window of time when the pacemaker battery is not working and the reimplantation surgery is being scheduled, the patient could begin to have abnormal heartbeats. Given that the doctor is now able to monitor the heart during this time, that could result in the patient potentially losing their life.

In 2012, an ethical hacker by the name of Barnaby Jack demonstrated that some remotely accessible pacemaker models could be hacked and that it was possible for the delivery of an electric jolt to the person's heart which could kill them (Boyle, 2012). Notoriously, U.S. vice president Dick Cheney had prompted the decision to disable the wireless functionality of the pacemaker for the same reason of the risk of him receiving a lethal jolt (Vaas, 2013). Although this had occurred during 2001-2009, this is still a problem that can happen today. While the capability to be able to track the heartbeat wirelessly is very effective so that patients are monitored, without proper security it would be ethically incorrect to allow patients to use a pacemaker as it would cause them harm. This would break the principle of Nonmaleficence that states that physicians should not cause harm to patients or at the very least the cost of doing something should outweigh any harm that is done.

However, we can see other security flaws when the pacemaker needs to communicate with outside sources via some network. Since pacemakers have an antenna they can send data to physicians remotely so that the physician can monitor the patient. However, this same functionality of transferring data from the pacemaker can also be taken advantage of. Around two years ago, two researchers by the name of Rios and Butts were able to exploit the pacemaker made from the well-known company, Medtronic. What they found was that an attacker could get remote access to the pacemakers and be able to modify patients' pacemaker data. (Newman, 2018). The

Department of Homeland Security had given a statement, after the report of this found breach of the pacemaker, which entailed: “An attacker with adjacent short-range access to an affected product, in situations where the product’s radio is turned on, can inject, replay, modify, and/or intercept data within the telemetry communication,” according to a statement from the DHS (Curley, 2019)

Ultimately, pacemakers have saved the lives of thousands of people by allowing physicians to monitor patients with abnormal heartbeats, but it can also open a window for harm. Determining whether the use of a pacemaker is correct is a hard question because of the possible dangers that are always present. Hence the only way to allow the continuance of pacemakers in a way that is secure would be for manufacturing companies to invest in the making of pacemakers with security features integrated.

MRI & CT Scans

According to the U.S. Food & Drug Association (FDA):

> “Medical imaging refers to several different technologies that are used to view the human body in order to diagnose, monitor, or treat medical conditions. Each type of technology gives different information about the area of the body being studied or treated, related to possible disease, injury, or the effectiveness of medical treatment.”(*U.S. Food & Drug Association, 2018*)

There are a variety of technologies that are able to create medical images, but I will focus on two very commonly used technologies. MRI machines and CT Scans. While both do take medical images, the differences lie in the manner that the images are taken and the visuals that you are able to see in the images. An MRI machine stands for ‘Magnetic Resonance Imaging’ which means that an MRI uses radio waves and magnets in order to create an image of bones, tissues, and organs. In comparison to that of a CT Scan which stands for ‘Computed Tomography’. A CT scan uses x-rays in order to create multiple ‘cross-sections’ of the human body. CT Scans are used to look at bones, tissues, the brain, and other organs in the human body. Some common uses of an MRI are for diagnosing: breast cancer, tumors, joint abnormalities, blood vessel irregularities, and more. While CT scans are used in order to diagnose: circulation problems, abdominal abnormalities, urinary bleeding, lung vessels, and more (Health Images, 2020).

CT and MRI machines are managed through image archiving and are communicated over a system called PACS. PACS stands for ‘Picture Archiving and Communication System’. The main components of PACS are core servers that are responsible for managing the “database, Digital Imaging and Communications in Medicine (DICOM; gateway), Import/export, radiology information system(RID) interfacing, storage systems, Web servers, and other interfaces/image distribution servers” (Heckman and Schultz, 2006). Given that this system is so popular in the healthcare industry it would have been a given that it would be protected, but in reality, there are many flaws with the system implementation of PACS.

Just this past year, 2019, there was a publication of an experimental new attack on 3D Medical Imaging which was created just for the purpose of demonstrating that an attacker can do much more than just hold medical data for ransom. The attack was conducted on a hospital in order to demonstrate how attackers can gain access to the hospital network, alter medical imaging, and gain access to other sensitive hospital data. The attack consisted of a man-in-the-middle attack through the use of a Raspberry Pi 3B, a small computer, which was given a USB to Ethernet adapter and was configured without a network identifier. Basically this attack uses the Raspberry Pi as an intermediary point between a CT Scan and the PACs network to get data before it is sent from the CT Scan to the network. In addition, the Pi was configured so that the attackers could use it as a 'back-door' to get access to the Wi-Fi network.

The Pi was installed after hours when the cleaning staff was working and it was installed in a CT scanner room. The Pi was installed between the CT scanner's workstation and the PACs network. Meaning that "an attacker could either intercept scans directly or perform lateral movement through the PACS to other subsystems and install the malware there" (Mirsky, Mahler, et al., 8) Once they had infiltrated the network it was discovered that data scanned was passed over the network twice. Once over a TCP channel, a protocol for data transfer, to an internal web service and then again to the PACS storage over a TLSv1.2 protocol, a protocol that is designed to provide communication security over a computer network. However, in both passes, the information was being transferred in clear text without any encryption added to the medical images produced by the CT scan. Furthermore, after the attack, the attackers were able to obtain both usernames and passwords for over 27 staff members and doctors because the data being transferred was not encrypted. The reason why the PACS is not encrypted is because it is not a common practice for hospitals to encrypt data that is transferred via the PACs network. Some reasons for this are, that there are compatibility concerns with older technology not being able to handle encrypted data, and because PACs are not connected to the Internet so it is argued that there would be no need to encrypt data as it only stays within the hospital network (8).

Thus far this attack has just breached into the network, but this is only the bare minimum of what the attack is actually able to do. Once the attackers have access to the 3D Medical Images, through the use of machine learning, they are now able to alter the images so well that radiologists are being fooled by the fakes. This attack is based on a neural network called a generative adversarial network, “GAN”. GAN consists of two neural networks, which are algorithms that take some input to “learn” to perform some task, which work against each other: the generator and the discriminator. The generator creates fake samples to try and fool the discriminator while the discriminator learns to differentiate between real and fake imaging samples. As the discriminator differentiates the fakes and the real imaging samples, the generator learns how to make better samples and ultimately create fake imagery that seems authentic. The attack is called CT-GAN and this attack works by using two GANs. One for the removal of cancer and one for the insertion of cancer into the 3D Medical Images. The removal GAN is trained on healthy images, meaning that the patient is healthy and has no cancer, versus the insertion GAN is trained on unhealthy images, meaning that the patient has cancer. For the purpose of this attack, lung cancer was the focus just to test if it would be possible to alter the images so well that even radiologists would not be able to tell a difference between the altered images and the unaltered images. There are other similar attacks but the reason why CT-GAN works better is because of how it takes into consideration the surrounding components of the image so that there is no obvious or unnatural insertion of a cancerous node. Other techniques such as copying and pasting a cancer node create obvious trails of the image being altered. The reason is that the pasted samples ignore the surrounding anatomy of the image which creates inconsistent textures in the image (Mirsky, Mahler, et al., 3-4).

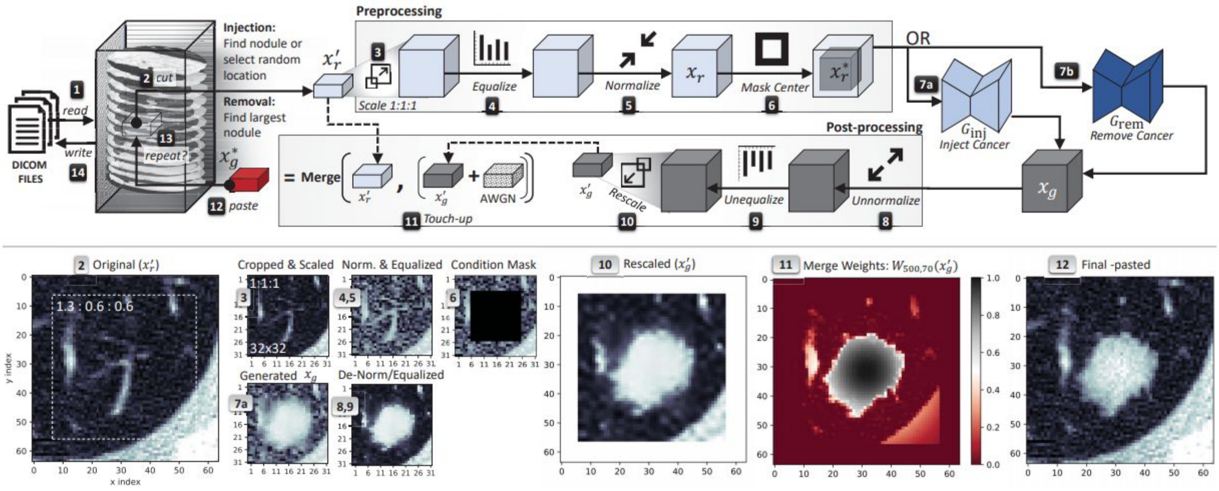


Figure 3: CT-GAN attack process. (Mirsky, Mahler, et al., 10)

Figure 3 illustrates the process that CT-GAN takes in order to insert cancer nodes which is the same process in which the removal of a cancerous node is accomplished. The process is capturing data, choosing a location to either inject a node or remove a node, scaling the image, normalizing the image, masking, injecting/removal of the node, reverse processing, adding some small details, lastly is pasting the node. Once these steps are completed then the image is returned back into the network. The amount of detail that the GAN takes into consideration to make the node seem as original and natural as possible makes it difficult to see if an image has a fabricated node. After the attack was conducted on the test hospital, three radiologists were contacted in order to see if they could be tricked by the CT-GAN Medical Imaging neural network. The attack itself had an average success rate of 99.2% for cancer injection images and 95.8% for cancer removal images. Although this attack was only an experiment, it does bring to light some of the huge dangers in not only the ability to alter medical imaging with machine learning, but also the lack of security that is present in hospital networks due to a lack of encryption. The need for better security is essential as this attack could cause the death of some patients if the radiologists are tricked by an altered image and announce a patient to be healthy when in reality they had cancer. (Mirsky, Mahler, et al., 13).

PACS Vulnerabilities

As of September 16, 2019, the National Cybersecurity Center of Excellence (NCCoE) has released a draft on analysis of the PACS ecosystem by using a risk assessment based on the NIST Cybersecurity Framework and other relevant standards. The NCCoE created an example of how HDOs, healthcare delivery organization environments, can use standards-based commercially available cybersecurity technologies to better protect the PACS system. The challenges when trying to secure the PACS system in a hospital is trying to secure the different kinds of interconnected systems. IoT devices that are used are usually from different vendors and supplies which means that one technique to secure one device will not work on other devices because of how different some IoT devices are from each other. Therefore the range of attacks is very diverse because they can target any IoT devices that are used by hospitals which means that ultimately a hospital only increases their risk by using a wide variety of IoT devices (Cawthra, Hodges, et al., 2).

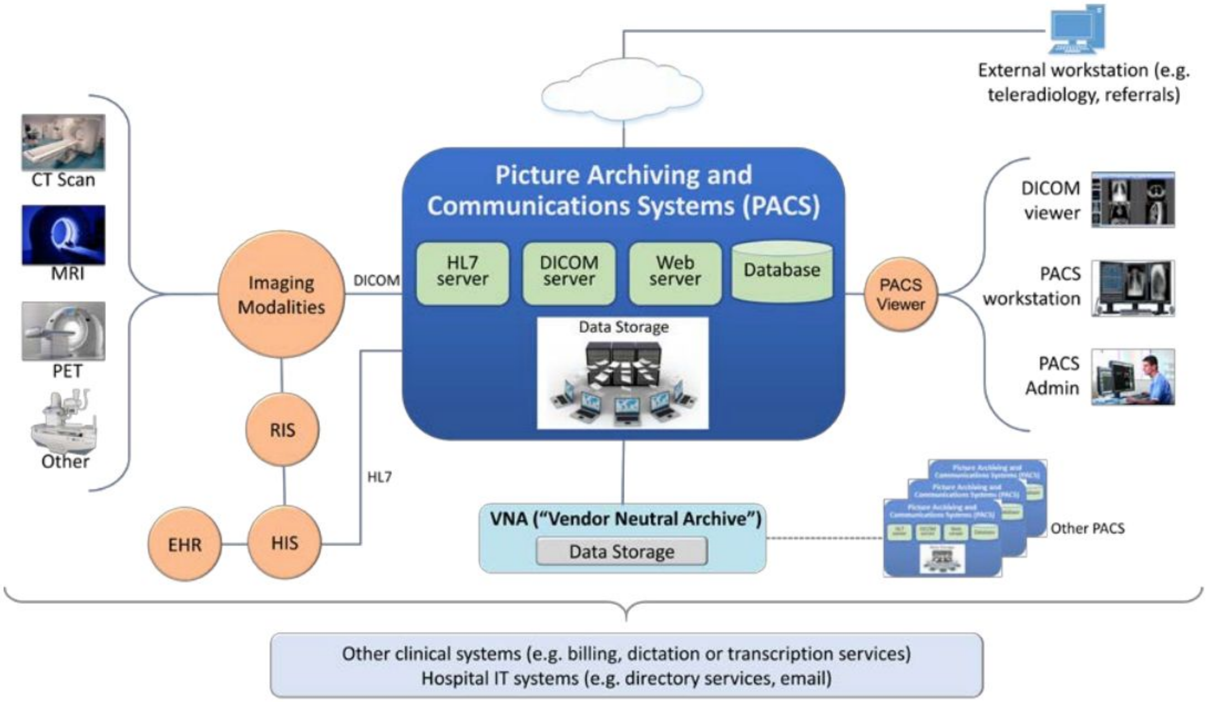

External workstation (e.g. teleradiology, referrals)
CT Scan
MRI
PET
Other
Imaging Modalities
DICOM
Picture Archiving and Communications Systems (PACS)
HL7 server
DICOM server
Web server
Database
Data Storage
PACS Viewer
DICOM viewer
PACS workstation
PACS Admin
RIS
HL7
EHR
HIS
VNA ("Vendor Neutral Archive")
Data Storage
Other PACS
Other clinical systems (e.g. billing, dictation or transcription services)
Hospital IT systems (e.g. directory services, email)

Figure 4: PACS' Medical Imaging Ecosystem

Figure 4 represents the medical imaging ecosystem in a hospital that uses the PACS ecosystem. As previously noted, the PACS system has multiple servers consisting of a database, DICOM, Web servers, and other interfaces/image distribution servers. NCCoE provided a list of threats, vulnerabilities, and risks that are available when using a PACS ecosystem such as the one in the image above. NCCoE assessed the risks of the PACS and medical ecosystem through the use of five scenarios. A sample radiology practice workflow, image data access across the enterprise, accessing-monitoring-auditing, imaging object change management, and remote access. After analyzing each of the scenarios they had created a list of threats that are possible, a list of vulnerabilities, and also a list of risks that are present in these systems. Lastly, NCCoE posed a framework to use in order to solve many of these issues and also a list of technologies that follow security standards such as HIPAA and IEC. Some of the threats listed were actions such as compromising credentials and altering data. This includes threats such as an individual levering privileges for unintended purposes, distortion or alteration of data in transit, or using malicious malware code which affects the servers and workstations (Cawthra, Hodges, et al., 35).

There are also a number of other vulnerabilities that can be present. In accordance with the list of vulnerabilities that were presented by NCCoE, most of the vulnerabilities listed were from lack of awareness or training from the hospital employees and other users. For example, the workforce not being aware or have not received proper training needed to use the PACS system correctly. Security teams not having sufficient training on the proper ways to investigate and write reports on abnormalities found in the system. As well as users who do have access to the networks have more privileges than they should, so the management of authentication and privileges within the hospitals is not strict (Cawthra, Hodges, et al., 19).

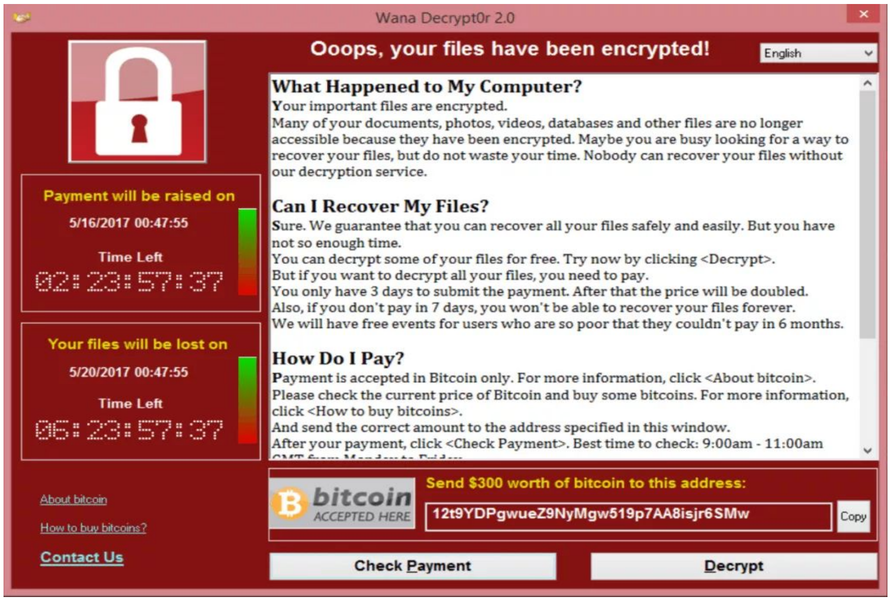
The NCCoE also provided a list of unmitigated risks which can be present in PACS lab environments. The list of risks included attacks such as a patient misdiagnosed because of some changes made to medical data by a user who was not authorized. Such as an attacker performing a CT-GAN attack as presented before. Another risk is the PACS or other systems within the ecosystem being attacked by ransomware which renders the systems and data unavailable (Cawthra, Hodges, et al., 23).

Due to all of these potential risks, the NCCoE mapped out the PACS ecosystem to the NIST cybersecurity framework. The tables describe many functions such as identity and protection which correspond to categories such as data security and information protection processes and procedures. On top of this, the NCCoE also provided a list of products and technologies which can be used in response to all of the risks, vulnerabilities, and threats that are present. For example in regards to the DICOM images, by using products such as Hyland Acuo Vendor Neutral, which provides access to the medical images and stores and retrieves images, or the use of Hyland NilRead Enterprise, which provides medical image viewing and manipulating for PACS, it can make the access of data restricted to only users that are authorized by these technologies. Meaning that if hospitals that implement the PACS environment were to use such products, there would be much safer management of user data (Cawthra, Hodges, et al., 37).

Software Vulnerabilities

One of the most famous hacks in the world is that of the malware attack called WannaCry. This cyberattack hit globally and it threw the United Kingdom's National Health Service into hiatus. What WannaCry actually did was to infect computers which would disallow employees to gain access to files unless some ransom money was paid. If the ransom money was not paid then all of the files on the computer would be deleted. However, in a healthcare setting, this meant that doctors lost access to millions of records which are needed to know what's wrong with patients at hospitals. This attack cost the United Kingdom National Healthcare about ninety-two million pounds because of about twenty thousand appointments having to be canceled due to the data loss (Field, 2018). This attack was effective because there was a security flaw in Microsoft's computers. Computers that used Windows XP, Windows 8, or Windows Server 2003 were vulnerable to this hack due to an unpatched vulnerability (Epstein, 2017).

What WannaCry does is that once it gets access to a host, it will encrypt most or even all of the files on the user's computer and it would ask for ransom money. A red pop screen will appear on the user's screen, just like in this image below:



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

If the user did not pay the money with bitcoin then it would delete all of the user's files that were encrypted and all data will be lost. Now given that this attack managed to affect the healthcare system in the United Kingdom, it does bring to concern just how severe this attack was. Since all data could be lost that would mean that all medical records were lost so basically you have doctors who would have to re-diagnose patients to regain all of the lost data. Now if a patient was in some critical condition then this could potentially have meant severe harm or even death. It was never announced that there was a death caused by this attack but there was a report from the Healthcare Industry Cybersecurity Task Force convened by the US Department of Health and Human Services which noted that health care in the United Kingdom was in critical condition. Experts say that health care lags far behind other industries, like the financial sector, in the level of protection used on their information. However, unlike finance, health care failure can result in injury or even death.” That is why this attack on the healthcare system was a massive blow and it just shows how important it is to have security in healthcare systems (Wetsman, 2019).

The biggest reason why these types of attacks are very successful is due to the fact that many users do not update their computers. This means that if there is a vulnerability available in an older update of a computer and a hacker creates a malware that leverages that vulnerability then they are susceptible to the attack. This is why there are still many malware attacks and why many cybersecurity analysts work to try and defend against these attacks. Although the WannaCry attack was a huge problem, it was an attack that was very obvious once the malware had infected the user’s computer. However, there are attacks that are not as obvious and are very hard to detect as they leave no obvious traces such as the big red screen on your display like the WanaCry attack does. There may be no sign of a breach until a user gets blackmailed for ransom money, some data gets corrupted, or someone discovers the vulnerability; which typically happens way after the infection has occurred. A scenario of this sort is if the attacker has found a back door in a system. Meaning that an attacker found access to a certain area in a system that they were not meant to have access to. If the hacker is good enough then they can make it very difficult to track them and a lot of the times once they have access to some system they move slowly to not catch any attention.

These quieter attacks include cases such as a hospital lab blood gas analyzer attack in Europe. These blood gas analyzers, or also known as an arterial blood gas test, measure the amounts of arterial gases, such as oxygen and carbon dioxide, that are present in a patient’s body. This blood gas analyzer is used in situations where the patient is in critical care. This is needed to determine whether or not the patient’s lungs are able to distribute oxygen throughout the body and be able to excrete out the carbon dioxide properly. However, a company called TrapX had discovered that the attackers were able to move through the networks from a vulnerability found in the blood gas analyzers which allowed them to get backdoor access to the hospital network. This meant that the hackers could tamper with the levels being outputted from the machine which can be very dangerous as wrong numbers could lead to the patient not getting the proper help needed to distribute oxygen to the body. As well as they had access to the hospital network which meant that they could get access to patient data. Ultimately, an attacker does not directly need to attack a hospital network but just find a way to get access to machines that are connected, in some way, to the network itself and just work through that chain of connections. (TrapX Labs, 17)

TrapX had concluded that this attack, known as MEDJACK, had the potential to alter data from the hospital patient data database. There are many other cases of breaches like these. A preventive measure would be to install firewalls in their networks to be more protected, but the reality is that not all hospitals do. In fact, there are some that barely use any security software and are still running very outdated software. It is also the case that some Healthcare IT teams do not have access to the internal software in medical devices and so the only protection that they get is whatever, if any, protection pre-installed onto the device when first acquired. This is very alarming given the fact that if IT is not able to support and have access to the network then it might as well just be as if they were not even there in the first place (Storm, 2015).

The reliance on the software that comes with certain medical devices is not always a smart decision because they can become utterly useless against attacks if they are not consistently being updated and patched against certain vulnerabilities that are discovered in these devices. TrapX had also explained how “medical devices are ‘closed devices, running out-of-date, closed, oftentimes modified and likely insecure operating systems such as Windows 2000, Windows XP” (Storm, 2015). This can become rather serious as technology is always advancing so there will be smarter ways to gain access to data and networks that these attackers should not have access to. This same idea of functionality and user-friendliness over security is becoming more and more apparent as many healthcare institutions simply use what software or hardware they know best as it is more convenient than to change to better secured.

Social Engineering

Thus far we have talked about attackers being able to do a range of things such as accessing hospital networks to being able to manipulate medical imaging. While altering medical images is a very sophisticated and complex attack that requires an attacker to have a tremendous amount of knowledge in not only artificial intelligence but also some medicine to accurately alter medical images that will deceive radiologists. Now we should also consider other less complex strategies or forms of attack that are not just easier to conduct but is also the leading form of attacks. These attacks are under the scope of social engineering. Social Engineering is the psychological manipulation of people into performing certain actions or giving away confidential data. In accordance with the US Department of Justice, social engineering attacks are one of the most dangerous threats in the world. The reason why these attacks are so successful is that the attackers are able to exploit the “natural human tendency to trust.” Humans are more likely to trust other humans than other technology which means that if an attacker is successful in gaining the trust of someone then that would mean that it is more likely for them to get some information/the attack being successful (Fatima and Kaabouch, 1).

Under the scope of social engineering, there are many ways that someone can conduct such an attack. For example, such attacks include phishing, ransomware, online social engineering, and many more. In 2018 there was an attack on a company called Equifax. Equifax is a company that is a credit reporting and monitoring agency that collects data from individuals and businesses to monitor their credit history and to prevent fraud. That being said, Equifax had access to a lot of sensitive user data such as social security numbers, credit card numbers, driver licenses, and other data. There was a phishing email that was sent to Equifax. The email was pretending to be from financial institutions and other big banks such as Bank Of America. Given that the email seemed realistic and passed as an email that they would usually receive, they fell into the trap of the phishing email. This resulted in the loss of about 145.4 million American customers’ sensitive data. Even today there is always news about phishing emails being sent around or robocalls trying to get information from people. Yet, although these attacks are becoming so common, why are people still being tricked? To answer this we should first look into the specifics of these attacks and also look into some other forms of social engineering that are not so common. We can then begin to analyze them as a whole and uncover that within all of these there is a commonality in the way that they are executed. (Fatima and Kaabouch, 2)

The most common social engineering attack is known as a phishing attack. However what is not commonly known is that within phishing attacks there are some classifications of this attack such as spear phishing, whale phishing, vising phishing, interactive voice response phishing, and business email compromise phishing. Beginning with spear phishing, this refers to specific individuals or selected groups using their names to make claims or communication. This requires the collection of info about the victim by using online sources such as looking at the victim's social media to get an idea of what kind of person they are. Whale phishing is spear phishing, but it targets higher ranking people from companies which are called big fishes. Hence the attack was named whale phishing. Vishing attacks are attacks done over the phone in order to manipulate people to give their sensitive info for verification. For example, this could be a call from an insurance company asking for your information to check something with your account. Lastly, there is also business email compromise phishing where attackers will use emails to trick employees, from some company, to click on a link or to download an email attachment to compromise the company's network. While these are a couple of very effective attacks, there are many other forms that also fall under the umbrella of social engineering. However even with just phishing attacks, we can begin to see that there is a common pattern in these attacks. This being that there is some research being done on the target before an attack is done (Fatima and Kaabouch, 5).

Social Engineering attacks are usually composed of the collecting information stage, developing a relationship with some target, exploiting the available info, executing some attack, and lastly exiting without any trace of the attack has occurred. There is certain terminology that some cybersecurity analysts use such as research/reconnaissance, hook, play, and out. However, we can also categorize the attacks into three groups, “social, technical, and physical-based attacks.” Phishing attacks are in the category of social. Other attacks that are also within the context of social attacks are pretexting attacks, phone/email scams, and robocalls. These techniques are grounded on the emotional aspects of humans and also the fact that humans are more likely to make mistakes and trust others. Within the other categories of technical and physical-based attacks, while these attacks are a bit harder to execute, they can be just as affected and in some cases even more effective. (Fatima and Kaabouch, 2)

The technical attacks such as ransomware attacks, pop-up attacks, and baiting attacks, are a bit harder to implement but are definitely doable with the right knowledge and skills. Ransomware attacks are attacks that target both individuals and companies. An affected company can suffer for very long if the ransomware successfully attacks the companies. Ransomware attacks have the power to restrict and block access to data such as files on a victim's computer by encrypting those files. In order to recover the files, the victim is threatened to pay some ransom. Meaning that if the attack is successful, the company has a high probability of losing either their user's information or money from having to pay the ransom. However, the process for developing such an attack is much more complex as the attackers have to be able to create the malicious code that will take all files from a system and then encrypt the files through the use of some encryption algorithm. Baiting attacks lure users to perform some actions such as clicking on some link to get some reward or leaving some USB drive at a coffee shop to lure someone to insert it into their computer. They act like a trojan horse where on the outside there is a clear benefit in doing some action, but in reality, it is a way to take advantage of the user by passing malicious codes onto the user's computer. Pop-up window attacks are attacks when a window appears on the victim's screen informing that the connection to the network has been lost and the user is then prompted to re-enter their credential to regain connection. This pop-up window, of course, being a fake, takes the re-inputted credentials and then sends them to some foreign location where the attackers then have credentials to be able to get access to the network (Fatima and Kaabouch, 7)

When we had previously looked at the other forms of attacks in previous sections such as hacking into pacemakers or altering medical imaging, a lot of the prevention techniques/countermeasures were solely on technological improvements or integrating better systems that provide more security measures. However, for many of the security measures or prevention strategies that are useful for social engineering attacks, they revolve around the human aspect. Meaning that employees need to be trained so that they are not so easily susceptible to these types of attacks. There are many prevention techniques that can be very helpful for both employees and companies as a whole such as encouraging security education and training. By doing so, it can increase the awareness of these social attacks which can keep employees on the lookout when they see some suspicious activity. As well as training on how to manage the company's data so their user’s confidentiality can be ensured. While it may seem that this is such a small change to prevent such destructive attacks, since these attacks rely so heavily on human error, the success rate for these attacks can drop drastically if people are aware of these attacks. Since not many people are aware or not expecting such an attack to happen to them, it is rather hard to be alert and very easy for someone to not realize that they are a victim. Thus by having security awareness classes, it can bring the employees alert level to a point where they can at least prevent some less elaborate social engineering attacks such as downloading a suspicious file from an email attachment (Fatima and Kaabouch, 8).

There are also some mitigation techniques that companies can use to combat a lot of attacks. Human-based mitigation attacks, just like prevention techniques, are very important to mitigate many of the social engineering attacks or at least to lessen the amount of damage that an attacker can do. However, as we have noted, the human component is not the most secure manner of security because this required strong awareness of social engineering attacks and if the human is not able to detect them then there is nothing that the human can do in response to an attack. Hence there are some technological-based mitigation techniques that can improve the accuracy of human-based mitigations against attacks. In accordance with a publication “Social Engineering Attacks: A Survey”, Salahdine and Kaabouch entail that there are four technology-based mitigation techniques which are biometrics, sensors, AI, and social honeypot. A biometric mitigation technique’s purpose is to counteract physical attacks, which are attacks in which the attacker does hands-on work such as sneaking into a company, caused by attackers trying to impersonate a company employee by creating a fake profile. Sensor-based mitigations are used in order to identify individuals. This could be an ID badge that the employee must have in order to get into the premises of their company. AI can be very useful to incorporate into a company because they are able to learn and adapt which means that they can become better defenders for these attacks over time. Lastly, social honeypot is a computer or computer system intended to mimic likely targets of cyberattacks. It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how the cybercriminals operate” (NortonLifeLock, 2020).

One of the hardest attacks to combat is ransomware. As previously stated, these attacks target individuals and companies rather than certain technology which makes it harder to notice them. In the survey, Salahdine and Kaabouch proposed an early warning detection system that is able to alert the employees when there is any suspicious activity on user data. The name of this system is CryptoDrop which analyses many common behavior indicators for ransomware attacks. In addition, they proposed a set of steps to take when mitigating and handling the ransomware attacks. The steps are preparation, detection, containment, eradication, and lastly recovery. In the preparation step, the company's security team must eliminate all the vulnerabilities so that there is no other access point from where an attacker can attack again. In the detection step, with the use of tools integrated into the intrusion detection system (IDS) such as CryptoWall and Locky, a ransomware attack can be detected. In the containment step, the security team is to aim at containing the attack to only a few of the company devices in order to contain the amount of data access that an attacker has. In the eradication step, this involves the cleaning of any damage caused by the ransomware attack. Lastly, in the recovery step, this is the recovery of damaged or lost files that are restored from the company's backups after making sure to dispose of the systems and machines (Fatima and Kaabouch, 11).

Social engineering attacks are by far more successful than other attacks and therefore should be a sector in cybersecurity that needs to be addressed more. This means that there needs to be more teaching about such attacks to the public so that they can be prepared and be less likely to be victims. As the human factor is the most vulnerable aspect for social engineering and hacking in general, training and awareness of both social engineering and cybersecurity should be broadcasted so that the general public can be aware. In the long run, as more individuals are aware and are experienced with these attacks, the vulnerability level for social engineering will lessen and ultimately reduce the number of attacks caused by social engineering.

Discussion & Conclusion

Ultimately there are many techniques that can be used in order to both prevent certain attacks and also to mitigate them once they have attacked. However, the vulnerability level is much higher when users of companies are not aware of the possibilities of hacking occurring. While hacking is known around the world, it is very easy to dismiss the possibilities as the chances of someone becoming a victim is low. However, when looking at the level of severity imposed from being a victim of an attack such as a shock to the heart from a pacemaker, personal information being stolen, and many other vectors of hacking, it is clear that hacking attacks are very dangerous.

Even with the addition of some preventive measures that were introduced in previous sections, that does not guarantee people’s safety if manufacturing companies and hospitals do not begin to implement similar techniques to ensure the security of their services. As addressed before, ethically speaking the use of many of these devices and services is questionable, but the fact is that people rely on such things to live. Therefore preemptive measures need to be taken by imposing better-secured systems, using newer technology, and learning about the risks of such attacks to not only keep systems protected but also keep the general public safe.

Future Enhancements

Given the time frame of this research, there were time constraints and limits to the number of topics that could be covered within the field of cybersecurity. If given a bigger time frame, I would have liked to cover other topics such as the recent creation of spectra devices. This new technology can bring medical imaging to the patient’s home for a low cost of three hundred fifty dollars for a starter set which is much cheaper than the price to get medical imaging done at a hospital; especially for those without any medical insurance to cover some of the costs. While this does seem like an amazing idea to provide such devices so that more of the general public could get their medical images done and be able to report them to their doctors, I do question its security. On the one hand, when looking back at the vulnerability we had seen with the network in hospitals and hacking into medical images, given that these devices are used in remote areas, it would be much harder for an attacker to be able to gain access to a patient's images because it is not certain who would have it or not. However given the fact that this device is going to be accessible to the general public, it would still only be a certain handful of people who would be able to purchase one. Either way, there is no way of knowing if a customer of the spectra devices is a hacker or not. If an attacker does purchase a Spectra, it is possible that the attacker could study the device and learn how medical imaging works and be able to use techniques such as CT-GAN, a technique to alter medical imaging. If they can acquire such a skill then that could cause grave danger to patients if their images were to get altered as described in the *MRI/CT Scans* section of this research paper (Rintoul, 2020).

As well as the attacks that have continued to occur now amidst the COVID-19 pandemic. With the pandemic placing a lot of fear onto the public, criminals have also noticed their fears and have begun to take advantage of it. There have been many social engineering attacks attempting to "impersonate legitimate organizations, such as the Center for Disease Control or the World Health Organization, by offering fake informational updates and even promises of access to vaccines - all for a price, of course!" This statement was from CSO Online which provides the latest information on cybersecurity issues and provides information about best practices to follow. As previously covered in the Social Engineering section, these forms of attacks target the human emotions and by getting the trust of the public they can get information from them. While being in a situation of fear and uncertainty, the human is vulnerable through emotional stress and it can be easier to lure people into giving information for the return of some service. In the case of COVID-19 given that there are many people who are dying, people would want to know that they are safe, and getting access to a vaccine that could save them would be of great interest (Tarun, 2020).

Bibliography

Disabled World. “Bioethics: Basic Definition and Bioethic Principles.” *Disabled World.* 11 Mar. 2019 www.disabled-world.com/definitions/bioethics.php Accessed 23 Apr. 2020.

Fruhllnger, Josh. “What is information security? Definition, principles, and jobs.” *CSO Online.* 17 Jan. 2020 www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html Accessed 23 Apr. 2020

Levine V. Edlyn. Pipikaite Algirde. “Hardware is a cybersecurity risk. Here’s what we need to know” *World Economic Forum.* 19 Dec. 2019 www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/ Accessed 23 Apr. 2020

“What Is Network Security?” *Cisco.* www.cisco.com/c/en/us/products/security/what-is-network-security.html Accessed 23 Apr. 2020

Aram Siamak, Rouzbeh A. Shirvani, Pasero G. Eros, Chouikha F. Mohamd. “Implantable Medical Devices; Networking Security Survey.” *Journal of Internet Services and Information Security (JISIS)* 6.3 (2016): 40-60. Print.

Sethi Pallavi and Sarangi R. Smruti. “Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering (2017): 1-25.* https://doi.org/10.1155/2017/9324035 Accessed 28 Apr. 2020

Chen, K., Zhang, S., Li, Z. et al. “Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice.” *J Hardw Syst Secur* 2, 97–110 (2018). https://doi.org/10.1007/s41635-017-0029-7 Accessed 23 Apr. 2020

Pycroft, Laurie & Boccard, Sandra & Owen, Sarah & Stein, John & FitzGerald, James & Green, Alexander & Pereira, Erlick. “Brainjacking: Implant Security Issues in Invasive Neuromodulation.” World Neurosurgery. 92 (2016): 454-462. Print.

Pycroft Laurie. “Brainjacking – A new cyber-security threat” *University of Oxford.* http://www.ox.ac.uk/research/brainjacking-%E2%80%93-new-cyber-security-threat Accessed 23 Apr. 2020

Sanders Laura. “Brain-zapping implants that fight depression are inching closer to reality” *Science News.* 20 Feb. 2019 www.sciencenews.org/article/brain-electric-implants-treat-depression-closer-reality Accessed 23 Apr. 2020

Curley Bob. “Hackers Can Access Pacemakers, but Don’t Panic Just Yet” *Healthline.* 4 Apr. 2019 www.healthline.com/health-news/are-pacemakers-defibrillators-vulnerable-to-hackers Accessed 23 Apr. 2020

Santosh, Chede & *Kulat, K.D. “*Design Overview Of Processor Based Implantable Pacemaker*.” Journal of Computers. 3.8 (2008): 49-57. Print.*

Wetsman Nicole. “Health Care’s Huge Cybersecurity Problem” *The Verge. 4 Apr. 2019* www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation Accessed 23 Apr. 2020

Epstein Zach. “WannaCry: Everything you need to know about the global ransomware attack.” *BGR.* 15 May 2017 www.bgr.com/2017/05/15/wanna-cry-ransomware-virus-windows-wannacry-explainer/ Accessed 23 Apr. 2020

Field Matthew. “WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled” *The Telegraph.* 11 Oct. 2018 https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ Accessed 23 Apr. 2020

Storm Darlene. “MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks” *Computer World.* 8 Jun. 2015 www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html Accessed 23 Apr. 2020

Vanhoef Mathy and Ronen Eyal. *“Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd”* IEEE Symposium on Security & Privacy (SP). IEEE. May 2020 https://wpa3.mathyvanhoef.com/ Accessed 23 Apr. 2020

Vanhoef Mathy and Piessens Frank. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. *CCS. 3 Nov. 2017* https://www.krackattacks.com/#details-android Accessed 23 Apr. 2020

Cawthra Jennifer, Hodges Bronwyn, et al. “Securing Picture Archiving and Communication System (PACS) Cybersecurity for the Healthcare Sector.” *National Institute of Standards and Technology (NIST) Draft. Sept. 2019*

Salahdine, Fatima, and Naima Kaabouch. “Social Engineering Attacks: A Survey.” *Future Internet* 11.4 (2019): 89. *Print*

Sobers, Rob. “110 Must-Know Cybersecurity Statistics for 2020.” *Varonis.* 15 Apr. 2020 https://www.varonis.com/blog/cybersecurity-statistics/ Accessed 28 Apr. 2020

“Pacemaker.” *How Products are Made.* 2006. http://www.madehow.com/Volume-3/Pacemaker.html Accessed 28 Apr. 2020

Galla Kishore Raghu. “Components of Pacemaker and ICDs - understanding the hardware” *Slide Share.* 12 June 2018. https://www.slideshare.net/raghukishoregalla/components-of-pacemaker-and-icds-understanding-the-hardware Accessed 28 Apr. 2020

Newman Hay Lily. “A New Pacemaker Hack Puts Malware Directly on the Device.” *Wired.* 9 Aug. 2018. https://www.wired.com/story/pacemaker-hack-malware-black-hat/ Accessed 28 Apr. 2020

Burke Stephanie. “Wi-Fi Alliance introduces Wi-Fi CERTIFIED WPA3 security.” *Wi-Fi Alliance.* 25 June 2018. https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security Accessed 28 Apr. 2020

Pycroft Laurie. “Brainjacking - a new cyber-security threath.” *The Conversation.* 23 Aug. 2016. https://theconversation.com/brainjacking-a-new-cyber-security-threat-64315 Accessed 28 Apr. 2020

Boyle Rebecca. “Hackers Could Access Pacemakers From A Distance and Deliver Deadly Shocks.” 17 Oct. 2012. *Popular Science.* *https://www.popsci.com/technology/article/2012-10/hacker-attackers-could-reverse-pacemakers-distance-delivering-deadly-shocks/* Accessed 28 Apr. 2020

Vaas Lisa. “Doctors disable wireless in Dick Cheney’s pacemaker to thwart hacking.” 22 Oct. 2013. https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/ Accessed 28 Apr. 2020

“Medical Imaging.” *U.S. Food & Drug Administration.* 28 Aug. 2018. https://www.fda.gov/radiation-emitting-products/radiation-emitting-products-and-procedures/medical-imaging Accessed 28 Apr. 2020

“MRI vs. CT Scans.” *Health Images.* 2020. https://www.healthimages.com/mri-vs-ct-scan/ Accessed 28 Apr. 2020

Heckman Kenneth and Schultz J. Thomas. “PACS Aechitecture.” *Springer Link.* 2006. https://doi.org/10.1007/0-387-31070-3_13 Accessed 28 Apr. 2020

Mirsky Yisroel, Mahler Tom, et al. “CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning.” *USENIX Security.* 6 June 2019. https://arxiv.org/pdf/1901.03597.p Accessed 28 Apr. 2020

“Anatomy of an Attack.” *TrapX Labs.* 2015. https://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf Accessed 28 Apr. 2020

“What is a honeypot? How it can lure cyberattacks.” *Norton.* 2020. https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html Accessed 28 Apr. 2020

Rintoul Jean. “Spectra.” *Crowd Supply.* 2020 https://www.crowdsupply.com/mindseye-biomedical/spectra#details-top Accessed 28 Apr. 2020

Tarun Renee. “COVID-19 Social Engineering Attacks.” *CSO Online.* 2020. https://www.csoonline.com/article/3533339/covid-19-social-engineering-attacks.html Accessed 28 Apr. 2020