ON AWARENESS OF CYBERSECURITY OF WIRELESS IMPLANTABLE MEDICAL DEVICES

by

John R. Santa Cruz JR

Submitted in partial fulfillment of the
requirements for Departmental Honors in
the Department of Criminal Justice
Texas Christian University
Fort Worth, Texas

May 2, 2016

ON AWARENESS OF CYBERSECURITY OF WIRELESS IMPLANTABLE MEDICAL DEVICES

Project Approved:

Supervising Professor: Michael Bachmann, Ph.D.

Department of Criminal Justice

Adam Shniderman, Ph. D.

Department of Criminal Justice

Matt Chumchal, Ph. D.

Department of Biology

ABSTRACT

Implantable medical devices (IMDs) have become widely utilized medical care options for people with chronic illnesses such as type I diabetes and heart arrhythmias since they provide convenient, personalized treatment at relatively low costs. As technology advances at an exponential rate, manufacturers incorporate more features such as wireless telemetry to enhance the ease and specificity of treatment (Park, 2014). Though these technological innovations bolster the functionality of IMDs, they also leave these devices open to cyber attacks that can steal personal information or cause fatal malfunctions, and the public awareness of this security risk is very much lacking outside of the small sphere of those conducting research on the matter (Ankarali et al., 2014). This paper discusses the basics behind what IMDs are, what they are used for, and how their wireless capabilities are both a benefit and a security risk for the patients using them. We review examples of previous experiments highlighting the vulnerabilities to IMDs and provide multiple examples of different types of proposed malicious attacks that a hacker could elicit as well as some methods of protection against them. Additionally, we assess the level of awareness of potential cyber attacks against IMDs among a pool of college pre-health professions students. Finally, we predict what future vulnerabilities will emerge based on current risks to healthcare security and discuss ways to decrease risk by increasing awareness and training of medical laypeople, students of higher education, and healthcare professionals.

Keywords: implantable medical device, telemetry, security, privacy, risk, awareness, cyber attack

I. Introduction

Implantable medical devices (IMDs), such as pacemakers, implantable cardioverter defibrillators, and insulin pumps, have greatly improved the convenience and specificity of treatment for patients with chronic illnesses such as type I diabetes, fatal heart arrhythmias, and many more all over the world. It is estimated that more than one million pacemakers and two hundred thousand implantable cardioverter defibrillators are surgically implanted worldwide each year (Alexandria, 2015); additionally, an estimated one million insulin pumps are currently in use, with that number continually increasing (Scrase, 2015). As technology continues to develop at an exponential rate, the quality of treatment that IMDs provide improves. Many of these devices now possess wireless telemetry capabilities so that doctors and patients can view medical data and adjust treatment without the need for additional surgery (Park, 2014). Wireless IMDs have become increasingly necessary for treatment of many chronic disorders, not only from a medical standpoint, but also from a socioeconomic view due to their upkeep cost and level of convenience. Having devices that provide constant monitoring and treatment of chronic diseases while going about normal day to day activities reduces the number of doctor visits and greatly decreases the troubles and annoyances accompanied with managing such diseases. In comparison to other forms of treatment, wireless IMDs are usually a better option because of their ability to fine-tune appropriate disease management, record and transmit specific medical data, and provide a relatively inexpensive way to live with ailments without much hassle (Hei & Du, 2013).

However, as these devices depend more heavily on wireless communication, the risk of a cyber attack for the theft of personal information or causing intentional malfunction becomes all the more real, and the lack of security measures against such attacks only makes

them more likely to occur (Ankarali et al., 2014). Even though the use of wireless IMDs is widespread throughout the world and there is a plethora of research devoted to how and why people hack into pacemakers and insulin pumps, the awareness of the existing security risks is minimal in the public sphere. Since there have been no documented cyber attacks on patients through their wireless IMDs thus far, coverage in the media has been almost non-existent, and since most people do minimal research outside of their daily news provider, much of the public is unaware of the topic altogether.

II. Overview of Pacemakers and Implantable Cardioverter Defibrillators

Pacemakers and implantable cardioverter defibrillators (ICDs) are necessary for people living with certain heart conditions by correcting arrhythmias. Cardiac muscle, like skeletal and smooth muscle, contracts in response to electrical stimuli that gets propagated from cell to cell through the opening and closing of ion channels until the whole heart contracts. Contraction only occurs when an electrical gradient threshold has been reached, which occurs automatically in the heart due to leaky ion channels in specialized cardiomyocytes known as pacemaker cells. These cells, many of which are located in the sinoatrial (SA) node of the heart in the right atrium, constantly produce electrical impulses, or action potentials, that travel along the heart's electrical conduction system to produce coordinated contractions of the four chambers of the heart to effectively pump blood at a steady rate. The rate at which these electrical impulses fire depends on certain stimuli from various homeostatic mechanisms, but under normal conditions, this will occur 60 to 100 times per minute in adults. For people living with arrhythmias, or abnormal heart rhythms, there is a disruption somewhere in this electrical circuit due to a number of different reasons and can

lead to heart attack, stroke, or heart failure; thus, arrhythmias need to be monitored and corrected to prevent life threatening complications. (Hei & Du, 2013)

Different IMDs for the heart are designed to correct different types of the most severe forms of arrhythmia. Pacemakers are used to treat people with bradycardia (slow heart rate) and blocked electrical pathways by detecting slow contractions and providing small electrical signals over a period of time to regulate the heart to beat at a normal pace. On the other hand, ICDs serve to correct tachycardia (or fast heart rate) or a heart experiencing fibrillation (quivering instead of beating) by sending a single large electrical pulse to shock the heart (defibrillation), effectively stopping all contraction, and let the pacemaker cells re-establish normal rhythm. Recently, ICDs have been given secondary pacemaker functions to ensure normal rhythm after shocking the heart during a tachycardic event. Pacemakers and ICDs, which will be referred to as cardiac IMDs, are typically surgically implanted in the chest below the collarbone. Each contains a pulse generator that receives electrical signals from the heart and produces electrical stimuli in response, one or more leads connecting the pulse generator to one or more chambers of the heart to conduct the electrical signals, and electrodes found at the end of each lead. Cardiac information, such as electrocardiograms, gets logged on the IMD, which can be read wirelessly by a physician in close proximity who can then adjust treatment accordingly with a device called a programmer. They have a lifespan of, on average, roughly seven years, until they need to be surgically replaced since wireless charging is difficult due to the thermal stresses it would place on the surrounding body tissues. Even with the repeated surgeries, cardiac IMDs provide an extremely convenient method for treating severe heart arrhythmias and allow people suffering from such heart conditions to live comfortable lives without many complications. (Hei & Du, 2013)

III. Overview of Insulin Pumps and Associated Devices

Another type of IMD prominent in the population is the continuous subcutaneous insulin infusion pump. For people with type I diabetes, proper insulin administration is absolutely crucial. In not-diabetics, the pancreas, particularly the pancreatic beta cells, produces and secretes insulin into the bloodstream in response to increased blood glucose levels, typically after eating foods rich in carbohydrates. During digestion, carbohydrates are broken down into glucose that gets absorbed into the bloodstream. The pancreas then responds by secreting insulin, a protein hormone, which is necessary for cells throughout the body to utilize glucose in the blood as a source of energy by binding to receptors on the cell membrane and initiating a signal cascade that leads to glucose absorption by the cell. Insulin also serves to store excess glucose in the form of glycogen in the liver and muscles to be used as a convenient energy reserve. Both of these insulin functions results in decreases of blood glucose levels. Opposing these effects, glucagon, another protein hormone secreted by the alpha cells of the pancreas, raises glucose levels in the blood when it is low, typically when it has been a few hours since digestion has taken place, by converting the stored glycogen back into glucose and putting it into the blood. The balancing act between insulin and glucagon is vital for keeping people within a normal blood glucose range. In type 1 diabetics, however, autoimmune cells gradually destroy the pancreatic beta cells responsible for producing insulin; thus, these people must track their own blood glucose levels at all times and require appropriate insulin administration through either needle injections or insulin pumps. Since diabetics must consciously monitor and maintain their own blood glucose levels, they are highly prone to hyper- and hypoglycemia. Hyperglycemia, or high blood glucose, occurs from

having too little insulin to compensate for a large increase in blood sugar, which can lead to a diabetic coma from cells being deprived of glucose and can even result in the destruction of small blood vessels in the eyes, kidneys, heart, and nervous system. In contrast, hypoglycemia, or low blood glucose, results from receiving too much insulin and can cause the brain, which relies heavily on glucose availability, to shut down, leading to coma and possible neurological damage. (Nichols, 2015) (Medtronic)

Insulin infusion pumps and their associated devices offer type I diabetics the ability to manage their condition in a more specific, effortless way that does not impose on daily life as much as manual injections. Controlling type I diabetes through insulin injections requires the person to monitor their blood glucose levels periodically throughout the day, typically by pricking their finger to get a blood sample for a glucose meter, and then manually calculate and inject a bolus dose of however much insulin is needed to restore normal blood sugar. This type of treatment is highly susceptible to human error, such as not checking blood glucose frequently enough or injecting too much or too little insulin, and also is not very specific in terms of continuously managing blood sugar throughout the day. In contrast, insulin pumps are worn outside of the body, typically around the waist, and delivers insulin through a subcutaneous tube in response to high blood glucose readings from an attached continuous blood glucose meter inserted under the skin that typically transmits wirelessly to the insulin pump. Together, the insulin pump and the continuous blood glucose meter allow for specific bolus treatment at mealtime as well as basal rate treatment that delivers small doses throughout the day for random spikes in blood sugar, logging this treatment information for the doctor to review. These devices can also calculate how much insulin the person needs to reach normal levels. Some pumps have extra features, such as having a touch screen or being

waterproof, having alarms for out of range levels, missed measurements, and blockages, and even connecting to smart phones and smart watches to display readings and give alerts, in order to make them even more convenient for both patients and doctors in providing treatments (Whitney, 2015) (Zawoad & Hasan, 2015). Thus, for type I diabetics, insulin infusion pumps and their associated devices are arguably the best alternative to having a functioning pancreas. (Aleppo, 2015)

IV. Overview of Generalized Wireless IMD Characteristics

When designing an IMD, there are many restrictions that must be taken into consideration. Certain materials must be used to ensure prevention of allergic reaction or corroding of the implant (Meng & Sheybani, 2014). Additionally, due to the need for a compact device, the resources that an IMD is able to contain is very much minimalized; energy supply, processing power, memory space, transmission range, and functionality are all limited by the requirement for size reduction, though battery life is the main priority for most. Typical IMDs utilize a non-rechargeable power source that may require surgery to replace since, as previously stated, external electromagnetic charging causes body tissues to experience thermal effects (Hei & Du, 2013).

There exist many components and properties that are common across the majority of wireless IMDs. First, there is a data acquisition component, such as sensors to measure heart rhythms or blood glucose levels, in order to gauge what is happening in the body. Secondly, there is the telemetry component that allows the IMD to wirelessly communicate with external devices for a number of reasons, including transmitting or receiving measurements, treatment logs, patient information, commands, and so on. The control component, which

gives the IMD its treatment parameters and program logic, takes advantage of the telemetry component and allows the patient or healthcare professional to adjust treatments as needed through the use of a device called a programmer. The action, or the therapy delivery, component elicits a response when the body measurements fall outside of these set parameters, such as secreting insulin when blood glucose levels rise above normal range or eliciting a shock when tachycardic. All of the data gathered from each of these parts is kept in the data storage component, which contains sensor measurements, treatment history, patient records, and other sensitive healthcare information. Finally, each IMD has some internal battery source that powers all of these tasks, the size and capacity of which depends on the device's function and physical accessibility. This relatively simplistic design, though slightly different depending on which wireless IMD is being considered, works well for proper functionality and treatment adjustments (Slobbe, 2013).

V. Experimental Wireless IMD Attacks

Remote monitoring of medical events and complications by wireless IMDs decreases the regularity of clinical visits and reduces the overall cost of treatment; thus, the trend is currently and is expected to continue going towards implementing wireless telemetry in devices such as cardiac IMDs and insulin pumps (Meng & Sheybani, 2014). However, the utilization of technological advances in the medical field also allows for potential cyber attacks to occur, especially since the trend for cybercrime is on an uphill slope. Introducing wireless communications to IMDs thus opens up a window of opportunity for information theft and malicious tampering.

There has been a copious amount of research devoted to the possibility of hacking implantable and wearable medical devices that contain wireless communication capabilities. One vulnerability that has been very well documented and explored is the exploitation of the telemetry between IMDs and their programmers. A programmer is a device, typically operated by the overseeing physician, that has complete control over everything its IMD does; it can store patient data onto and retrieve it from the IMD, program therapy parameters depending on the necessary treatment, collect patient biometrics that the IMD has recorded, and a variety of other functions through close-proximity radio frequency commands. The problem lies in the fact that the IMD trusts the programmer's signals completely with little to no authentication required, and attackers can mimic them to take control of the IMD and bypass the programmer.

In one experiment, researchers Halperin et al. (2008) were able to relatively easily extract sensitive information and elicit responses to one model of an implantable cardioverter defibrillator through several software radio-based attacks. They used an oscilloscope and a universal software radio peripheral (USRP), which can intercept radio communications within a frequency band as well as generate wireless signals with varying configurations of data, frequency, modulation, and power (Li, Raghunathan, & Jha, 2011). Their equipment was able to eavesdrop on the transmissions between their ICD and the programmer on the short-distance 175kHz frequency; they then decoded and reverse-engineered the transmissions, allowing them to overhear sensitive information passed between them and also giving them the ability to create their own transmissions identical to that of the programmer. Utilizing replay attacks, or the sending of a certain packet of data containing a command over and over again to elicit a response, they were able to pose their USRP as the programmer and control

the ICD. Thus, they were able to extract and change stored information such as the patient name, date, time, and diagnosis. Even more concerning was their ability to disable all therapies on the ICD and have it produce a 1J command shock, which would induce fibrillation. When using the ICD properly, the command shock is used during an electrophysiological (EP) study to induce fibrillation and the automatic therapies on the ICD would immediately detect and treat the fibrillation, thereby testing to see if the device is working properly. However, turning off the therapies and then eliciting a shock, as Halperin et al. has demonstrated, could result in serious harm or death to the patient. (Halperin et al., 2008)

Another experiment involving the vulnerabilities of IMD telemetry was done by Li et al. (2011) in which they were able to control a popular market insulin pump by, again, bypassing the programmer. As in the Halperin experiment, they were able to reverse-engineer the communication protocol between the insulin pump and the programmer through passive eavesdropping, but on the longer-distance 915MHz frequency. They easily extracted the PIN associated with the pump that is required to communicate with it and, thus, could stop and start insulin injection as well as inject a bolus dose that could dangerously decrease a patient's blood sugar from over 20 meters away (Li, Raghunathan, & Jha, 2011). Furthered findings and demonstrations were giving by Jay Radcliffe and Barnaby Jack (Klonoff, 2015). Radcliffe hacked his own insulin pump at a security conference in 2011 by reverse-engineering the transmissions sent from his wireless programmer in order to program a small, inexpensive, easily obtainable radio frequency transmitter to control his pump. He was thus able to tell the pump to administer doses of insulin on command and cause the pump to become inactive from 150 feet away, though he needed the pump's serial ID number

beforehand. Shortly following in 2012, Jack developed a scanner with a high-gain antenna, for boosted range, and scanned the company-designated insulin pump frequency to find a nearby pump, retrieved the pump's serial ID number, and instructed it to deliver its maximum dose from over 300 feet away (Klonoff, 2015).

Though these instances were not malicious in nature and were only used to show that IMDs can be hacked, there will most likely come the day when someone chooses to exploit the existing vulnerabilities for personal gain at the expense of the patient. And the extent of these attacks, as shown, could be much more harmful than learning a few basic details about the patients or their heart rhythms.

VI. Possible Methods of Attack and Exploitations

Based on the experimental findings mentioned above as well as from other instances not previously discussed, there are a number of different attacks that exploit the telemetry interface of IMDs that have been determined to be valid and extremely possible in a real-life setting. One such type of attack involves the interception and interference of the communications between the IMD and the programmer. Passive eavesdropping, as discussed previously, is the collection of transmissions between the two devices. As the communication channel is highly unsecure, it is relatively easy for someone with a technological background to listen in on the operating radio frequency to decode the programmer-IMD transmissions in order to gather information such as the patient name, diagnosis, overseeing physician, device serial number, biometrics, treatment programming, and any command the programmer sends to the IMD. Taking it a step beyond simple collection, active eavesdropping interferes with the wireless communications by altering the transmissions while they are being exchanged;

outcomes that can result from this include jamming the signal to block the communications, called a denial of service attack (Slobbe, 2013), or changing the messages sent to elicit inappropriate readings or responses. (Halperin et al., 2008)

Once the attacker has decoded the transmissions between the programmer and the IMD, it is possible, as demonstrated previously, to reverse-engineer the communications from the programmer in order to create new data packets containing malicious commands that are broadcasted repeatedly to the IMD and can elicit changes within it since they mimic the transmissions of the programmer. These replay attacks have a large variety of outcomes depending on what commands are being sent out. Halperin et al. demonstrated the possibility of changing stored patient information, turning off therapies, and even prompting a fatal shock to the heart to induce fibrillation. Li et al., Radcliffe, and Jack showcased how they could stop therapies or cause an administration of the entire supply of insulin in an insulin pump. They also proposed that someone could potentially change the dosage settings to cause the pump to provide to much or too little insulin in response to high glucose levels, cause a false reading to be displayed on the patient's continuous blood glucose monitor to trick the patient into administering an incorrect dose, or disable all alarms to allow a high glucose reading to go unnoticed and untreated (Li, Raghunathan, & Jha, 2011). (Klonoff, 2015)

Even without prior knowledge of the transmission protocols of the programmer, another easily launched attack on IMDs is a resource depletion attack. This type of attack exploits the limited resource availability of the IMD, such as a short battery life and little data storage capacity, by forcing it to repeatedly participate in multiple wireless communications. The first step of communication between an IMD and a programmer is authentication. If the programmer does not pass this step, the IMD will end communication with that particular

device. This single step, however, requires the IMD to do decent amount of information processing and transmission which uses battery power; therefore, an unauthorized programming device could be able to repeatedly try to connect to an IMD, causing a drain of a lot of battery power as well as a generation of many security logs that use up storage space. With resource depletion attacks, the lifespan of a wireless IMD could decrease by years, which is especially dangerous for ICDs since they are surgically implanted and, thus, difficult to replace frequently (Hei & Du, 2013). Keeping the IMD in constant communication with an unauthorized device can also lead to an inability of authorized devices like an authorized programmer or a blood glucose monitor to access it when needed, thus leading to a denial of service attack (Slobbe, 2013).

Although some of these attacks may require previous knowledge to specific information on certain devices like its individual serial number, attackers could also simply manipulate social engineering to accomplish this. By exploiting unaware healthcare employees or patients, an attacker could use the guise of some healthcare professional in order to coax the information of them. Thus, the users can actually aid the hackers in their endeavors (Slobbe, 2013).

VII. Challenges with Defense of IMDs

Each one of these attacks poses a threat to the person having the wireless IMD. These devices contain a wealth of information about patients that is legally confidential and can be highly sensitive. This data could be desired for multiple reasons; an insurance company could use this information to increase rates or deny a claim, politicians could be blackmailed with such personal medical details, or it could just be embarrassing for that information to become

common knowledge. When attempting to design security defenses against these wireless attacks, the goal is to ensure confidentiality, integrity, and availability. Data stored on IMDs should only be accessible to authorized entities and be kept confidential both in storage and while in transmission, the device should have authentication protocols to prevent modifications from unauthorized entities, and the device needs to be easily accessible when the patient or physician needs to use it (Rushanan et al., 2014). Some security proposals for IMDs employ cryptographic methods of authorization to ensure confidentiality and integrity. However, secret key storage and data encryption require a decent amount of memory and processing power to be used, something that is extremely lacking in IMDs, and would require replacement of the existing device to implement; additionally, device encryption may prevent its accessibility in an emergency situation when an emergency room physician is attempting to access the ICD of an unconscious patient to gain his or her patient information and ensure proper treatment (Ankarali et al., 2014). Another proposed defense is the use of an external cloaking device that prevents signals of any kind to reach the IMD, which can be turned on and off readily; however, when communications are enabled, the transmission is still unsecured and can be subject to eavesdropping attacks (Ankarali et al., 2014). Thus, how to design a secure yet accessible storage and transmission method while still taking into account the limited resources of the IMD is the major problem with designing security measures.

However, defenses against telemetry attacks of any kind have not been widely implemented by device manufacturers because medical equipment has only ever regulated for reliability, effectiveness, and safety rather than for security (Zetter, 2014). Additionally, manufacturers adhere to what the consumers want, which is simplicity and accessibility; thus, devices are being made with Wi-Fi and Bluetooth capabilities for more convenient monitoring

and treatment, but are keeping their limited security protocols to not overcomplicate the user interface, thus creating more mediums of vulnerability with little protection (Moses, 2013). Even if security measures are implemented in IMDs, the average review process for medical devices by the FDA is 6 months, which, at the rate technology is changing currently, could result in the security measure being obsolete by the time it actually hits the market (Moses, 2013). Thus, it seems public opinion and policy must change in order to effectively combat the threat of healthcare cybersecurity vulnerability.

VIII. Awareness Study of Pre-Health Students and Results

As previously noted, the ability for people to perform a cyber attack against wireless IMDs is not a very publicized topic, and it is necessary that people know about such attacks so that there is more impetus to create proactive solutions to the current vulnerabilities. Additionally, even if someone does know that there are possibilities of such a thing happening, he or she may not think the risk is very high because simply because the hackers would have more to gain from a higher-profile individual. In fact, vice-President Dick Cheney disabled the wireless features of his heart pump to prevent a possible act of cyber terrorism (Gupta, 2013). Regardless of social status however, everyone with one of these devices is at potential risk of information theft and personal harm from such an unforeseeable attack, and the lack of awareness would only help attackers to go undiscovered. Thus, we decided to survey a group of people about to enter into the healthcare field in the coming years to gauge their awareness level on the security of wireless IMDs to see get an idea of how much need for awareness there actually is.

Methods:

A total of 88 pre-health professions students, ranging from second- to fourth-year students, were surveyed for their awareness about wireless IMDs and their security risks. Before conducting this survey, an Institutional Review Board (IRB) application was submitted to and approved by Texas Christian University (TCU), which required successful completion of the National Institutes of Health's (NIH) training course "Protecting Human Research Participants", to allow surveying of TCU undergraduate students. The survey was distributed to students in various pre-health classes at TCU. Classes were selected by compiling a list of all the classes from the TCU course catalog in the Fall semester of 2014 that had most, if not all, of their enrolled students fall into the pre-health category, excluding first-year courses due to the high attrition rate of pre-health majors after their first year of their undergraduate degree; once this purposed list of classes was established, we utilized a simple random sampling approach to select 4 classes to survey. Permission was obtained from the professor of each class to administer the survey prior to the start of class, and participation in the survey was completely voluntary with no incentives provided. Anyone indicating that they were not pre-health professions students was excluded from the survey.

The survey itself consisted of 10 questions. Questions 1-4 gauged the factual knowledge level of wireless IMD trends and security. Questions 5, 7, and 8, assessed the confidence level of their knowledge of wireless IMDs. Question 6 was an attention question designed to ensure participants were responding to their surveys thoroughly. Questions 9 and 10 concerned individual interest in the subject matter. Responses to each question were collected through a Likert-scaling method, with responses ranging from 1="Very Strongly Disagree" to 7="Very Strongly Agree" with 4="Neutral". We also employed the intermittent

use of reverse-worded questions to diminish response bias from answer patterns. Finally, there was socio-demographic section at the end of the survey to indicate gender (male or female), classification (second-year or third- and fourth-year), and number of hours of hospital experience (<25 hours or >25 hours working, volunteering, or shadowing in a hospital or clinic). It should be noted that the gender ratio that exists in our study (46.6% male) is very close to the gender ratio of TCU's College of Science & Engineering ratio in 2014 (45.8% male) (Student Characteristics, 2015), giving evidence that our sample is representative of the population we are studying, at least in terms of gender.

Results:

For the purpose of analysis, the reverse-worded items, which included questions 2, 5, 7, and 8, were recoded so that all the values were measured in the same direction as those that were not reversed. Responses were then put into two groups: questions 1-4 were combined into a summative index of knowledge, and questions 5, 7, and 8 were combined into a summative index of confidence.

The summative index of knowledge is scaled from 4-28, the higher numbers indicating correct knowledge of wireless IMD facts and trends. The mean of the responses was 16.57, indicating a moderate level of knowledge seen on average. There were no significant differences between genders, classifications, or hours of experience in a series of t-test two-sample mean comparisons.

The summative index of confidence is scaled from 3-21, the higher numbers indicating higher levels of confidence in the previously assessed knowledge. The mean of the responses was 8.01, indicating a low confidence in level of knowledge on average. An OLS linear

regression was conducted to examine whether gender, experience, or classification were significant predictors of self-reported confidence in level of knowledge. Combined, the three independent variables were able to explain 13.4% of the variation in the dependent variable. The overall regression model $F(3,84)=4.34$ was found to be highly significant, $p<0.01$. Of the three entered independent variables, only classification failed to be significant. Experience was found to be the strongest ($\beta=-0.32$) significant predictor variable ($p<0.01$) followed by sex of the respondent ($\beta=-0.27$) at $p<0.01$ (see Table 1). These regression results show that respondents with more experience also report lower confidence levels, as do female respondents.

Discussion:

As the results show, the level of knowledge that pre-health students have about wireless IMDs is moderate, on average, across the board. Since the responses are not skewed towards the side of having accurate knowledge, we can assume that, on average, the typical TCU undergraduate pre-health student lacks basic information about the security and vulnerabilities of wireless IMDs; and since there are no significant differences among socio-demographic groups, it would appear that whether or not someone has been informed is not influenced heavily by gender, length of time in college, or number of hours of hospital experience.

In turn, the responses to the level of confidence in that same knowledge indicates that, on average, pre-health students have low confidence in the information they have about IMDs; this is somewhat expected since their only moderate scores in the knowledge-based responses showed that they lack the pertinent knowledge. However, the significant difference

between those with <25 hours of clinical experience versus those with >25 hours of experience indicates, somewhat surprisingly, that those who have spent less time in hospitals and around patients have more confidence in their knowledge-base than those who have spent more time in a clinical setting. Perhaps this finding shows that people with more clinical experience and have learned more about the healthcare environment have a greater awareness of what areas of medicine they lack knowledge of, while those who have rarely engaged in medical settings do not have enough experience to know what topics they need to be informed about. Whether this notion holds true or not, our survey points towards there being a need for some type of education on the emerging security risks of IMDs, especially within this group of people since these are the students that would be experiencing such cyber attacks, should they occur, within their generation of being doctors or other health care professionals due to the vast increase in technological necessity in the medical field.

IX. Current and Future Concerns and Responses

As more and more technological innovations become available to the public, most people see only the benefits that they are afforded, such as increased interconnectivity, and overlook the security risks that accompany them. In the healthcare industry, increased interconnectedness is becoming essential for hospitals to run fluidly, like with doctors needing to monitor and alter treatments of patients in one area while tending to another patient at the other side of the medical center by controlling their medical devices from any hospital computer. Additionally, emerging Wi-Fi and Bluetooth-compatible IMDs allow patients to interact conveniently with them using their smart phones and smart watches, monitoring vitals and changing therapies (Zawoad and Hasan, 2015).

There has been plenty of research dedicated to the vulnerabilities of IMD telemetry and how to control their functions using a programmer mimic, yet software security among the devices that already control IMDs, such as hospital equipment or even a cell phone, has yet to be largely addressed (Rushanan et al., 2014). In a two-year study, starting in 2012, of the security of the medical equipment used at a large chain of Midwest healthcare facilities under Essentia Health, Scott Erven and his team found many devices, including drug infusion pumps, Bluetooth-enabled defibrillators, and even temperature settings on blood-storage refrigerators, shared a handful of common security holes, such as lack of authentication to access or manipulate the equipment, weak or default and hardcoded passwords, and web server interfaces, that could allow hackers to control these devices remotely. Unauthorized parties could gain access by infecting a single employee computer connected to the hospital server through a phishing attack or by simply plugging in their own laptop into the network if already in the hospital, and they could then explore the internal network to find vulnerable devices and information (Zetter, 2014).

This ease in accessing a healthcare network server was shown in the February of 2016 when Hollywood Presbyterian Medical Center fell victim to a crypto-ransomware lockout. Crypto-ransomware is a type of malware, typically activated by a phishing attack, that infects the computer that downloaded it as well as possibly spreading to other computer systems it is linked to; it then encrypts the files on the computer that requires an encryption key to unlock them, which the attacker exploits by demanding a ransom for the key typically in the form of untraceable bitcoins. The Los Angeles hospital was unable to access their electronic medical records and other computer systems, which forced the staff to move back to paper and fax machines while their IT team struggled to regain access to their medical files. After being

locked out for ten days, the hospital agreed to pay the $17,000 ransom in order to regain access to their system. Though the hospital administration claims that there was no breach in confidential patient information or any other tampering of information aside from the encryption, hospital functions were still crippled for over a week; however, in comparison to what else the hackers responsible could have done, Hollywood Presbyterian was merely bruised by the attack (Gallagher, 2016).

Taking both of these recent events into consideration, the increased connectivity among healthcare devices opens up new mediums for hacking, with intentional as well as unintentional attacks being a serious threat for the future of IMDs and medial cybersecurity in general. Concern for such cyber risks in medicine has only just started emerging amongst lawmakers and the healthcare industry. The Cybersecurity Act of 2015 is currently prompting the Secretary of the Department of Health and Human Services (HHS), in consultation with the Director of the National Institute of Science and Technology and the Secretary of the Department of Homeland Security, to establish a healthcare industry task force that will assess the current state of cybersecurity of healthcare in the United States. The task force will 1) analyze how other industries, such as financial services and the government, have implemented safeguards for protecting data to propose defenses for healthcare, 2) review the challenges of securing medical devices and other systems connected to electronic medical data networks, 3) investigate challenges that private healthcare organizations face when securing data, 4) spread information to healthcare industry stakeholders for improving preparedness against cybersecurity threats, 5) establish a plan for the government and the healthcare industry to share updated information about cyber threats and defensive strategies, and then 6) report all of their findings and recommendations to Congress within a year of the

task force's formation (Burr, 2015). Though this act is a good start to defending against emerging cyber threats, there are a number of drawbacks that may limit the effectiveness of the task force. For instance, the FDA is not part of the task force even though it oversees and approves medical devices. Additionally, the healthcare industry's participation in the task force's initiatives, such as their research or abiding by their recommendations, is strictly voluntary with no consequences or incentives, meaning that it is still up to the medical device manufacturers to produce more secure devices even though their main focus has traditionally been on effectiveness, reliability, and treatment safety rather than security (Zetter, 2014). Furthermore, the task force is only in operation for one year, which makes it impossible to assess every vulnerability in healthcare security and provides only a snapshot of current cybersecurity which could be obsolete before any the findings are put to any use. (Trinckes, 2016)

Though lawmakers and healthcare industry stakeholders are beginning to wake up to the threat of cybersecurity vulnerabilities, there is still not enough pressure from the public to elicit meaningful responses to this growing threat because of their lack of awareness on the matter. Not only that, but there is also little knowledge at the level of the healthcare provider on how to defend against cyber attacks and how to handle them should they appear because there is little to no required education of medical cyber safety outside of the basic HIPPA training. In order to combat this widespread lack of awareness and information, the National Science Foundation is funding an education initiative called TECH MeD, or Transdisciplinary Education for Critical Hacks of Medical Devices. TECH MeD is attempting to "educate undergraduate and graduate-level students from various disciplines, healthcare professionals, patients, and the general public about the ethical, legal, social, and technical implications" of

remotely accessible, implantable medical devices (Research Areas, 2015). Led by the principal investigator Dr. Michael Bachmann, this program will create an open-access website and online course to increase public awareness, undergraduate and graduate courses to prepare individuals for dealing with the challenges surrounding this evolving technology, and a certified Continued Medical Education (CME) course that will educate medical professionals about the issues they could encounter surrounding wireless IMDs in a medical setting. Thus, the goal is to educate everyone from laypeople to medical professionals about the security risks of these healthcare devices in a way that is easy to understand in hopes to start a conversation on how to better protect these devices with those who have the power to create and implement cyber defenses (Research Areas, 2015).

X. Conclusion

As technology advances at a constantly increasing rate, the level of awareness of certain vulnerabilities does not proportionally correlate, thus creating higher risk of attack. Implantable medical devices fall into the same pattern; as their machinery and capabilities grow to provide better quality treatment, so does their risk of being the target of a malicious cyber terrorist.

It has been shown that unauthorized parties can trick wireless IMDs into divulging sensitive personal information, changing settings, and even eliciting inappropriate responses that can be harmful or fatal to the patient. Though it is possible for such an attack to occur, the level of awareness on the topic is highly limited to those who go out of their way to research it, while most of the world goes on completely oblivious to such a scenario. Our study found that the typical pre-health college student falls into the latter category of people who are

unaware of the potential threat. This only allows the threat to become greater by allowing such security flaws to go unnoticed and unfixed. The best possible way to prevent future attacks is to raise both physician and patient awareness of the weaknesses of wireless IMDs and pressure manufacturers to come up with better security measures. In one study by Denning et al., the views of patients with individual IMDs were surveyed; the findings revealed that the majority of the 13 participants were concerned about the privacy of their electronic information and personal safety, yet they were not worried that an unauthorized attacker might alter the settings on their device. Regardless of this, the participants tended to agree that something should be done to ensure the future security of wireless IMDs (Denning et al., 2010).

Even though the risk of someone hacking into a personal medical device is minimal at this period in time, it could become a very real possibility in the near future. In order for there to be any advancement toward securing these devices against future attacks, awareness on the matter has to be spread to those who are put at risk by the vulnerabilities of the devices keeping them alive and healthy. Manufacturing companies for anything, including IMDs, will pay more attention and work to fix or improve something about their product if there is a large public opinion demanding something to be changed. Since there is a great lack of awareness about the vulnerabilities of implantable cardioverter defibrillators and insulin pumps, they remain overlooked when these devices are upgraded over time, and more important and noticeable aspects such as battery life and interconnectivity are focused on. Therefore, the best way to prepare for possible cyber attacks is to know that they exist and increase public concern. Then, perhaps more stringent regulations on software integrity and data encryptions

will pass and the threat can be diminished before awareness is spread when news headlines about the deaths of patients with IMDs due to cyber attacks begin emerging.

References

Aleppo, G., MD. (2015, May 21). Insulin Pump Overview. Retrieved March 9, 2016, from http://www.endocrineweb.com/guides/insulin/insulin-pump-overview

Alexandria, V. (2015, March 16). Insulin Pumps Need Greater Safety Review: American Diabetes Association Issues Joint Statement with European Association for the Study of Diabetes. Retrieved March 31, 2016, from http://www.diabetes.org/newsroom/press-releases/2015/insulin-pumps.html

Ankarali, Z., Abbasi, Q., Demir, A., Serpedin, E., Qaraqe, K., & Arslan, H. (2014). A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security. *Proceedings of the 4th International Conference on Wireless Mobile Communication and Healthcare - "Transforming Healthcare through Innovations in Mobile and Wireless Technologies"*

Burr, R. (2015, October 28). Cybersecurity Information Sharing Act of 2015. Retrieved March 31, 2016, from https://www.congress.gov/bill/114th-congress/senate-bill/754/text#toc-id9d4d6969369a4054a8bb7e0880c6555b

Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno, T., & Maisel, W. H. (2010). Patients, pacemakers, and implantable defibrillators. *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*.

Gallagher, S. (2016, February 16). Hospital pays $17k for ransomware crypto key. Retrieved March 31, 2016, from http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/

Gupta, S. (2013, October 20). Dick Cheney's heart. Retrieved January 31, 2016, from http://www.cbsnews.com/news/dick-cheneys-heart/

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., . . . Maisel, W. H. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. *2008 IEEE Symposium on Security and Privacy (sp 2008)*.

Hei, X., & Du, X. (2013). Security for Wireless Implantable Medical Devices.*SpringerBriefs in Computer Science*.

Klonoff, D. C. (2015). Cybersecurity for Connected Diabetes Devices. *Journal of Diabetes Science and Technology, 9*(5), 1143-1147.

Li, C., Raghunathan, A., & Jha, N. K. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. *2011 IEEE 13th International Conference on E-Health Networking, Applications and Services*.

Medtronic. (n.d.). Basics of Insulin Pump Therapy. Retrieved March 15, 2016, from https://www.medtronicdiabetes.com/sites/default/files/library/support/Basics of Insulin Pump Therapy.pdf

Meng, E., & Sheybani, R. (2014). Insight: Implantable medical devices.*Lab on a Chip Lab Chip, 14*(17), 3233. doi:10.1039/c4lc00127c

Moses, M. (2013). Securing Implantable Medical Devices: An Alternative to Government Regulation. *Introduction to Information Security Management,* 95-752.

Nichols, H. (2015, July 24). Diabetes: The Difference Between Type 1 and Type 2 Diabetes. Retrieved April 25, 2016, from http://www.medicalnewstoday.com/articles/7504.php

Park, C. (2014). Security Mechanism Based on Hospital Authentication Server for Secure Application of Implantable Medical Devices. *BioMed Research International, 2014*, 1-12.

Research Areas. (2015, June 3). Retrieved April 25, 2016, from http://www.nsf.gov/awardsearch/showAward?AWD_ID=1500077

Rushanan, M., Rubin, A. D., Kune, D. F., & Swanson, C. M. (2014). SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. *2014 IEEE Symposium on Security and Privacy*.

Scrase, R. (2015, August 4). Top ten medical inventions: Pacemakers. Retrieved March 31, 2016, from http://www.understandinganimalresearch.org.uk/news/communications-media/top-ten-medical-inventions-pacemakers/

Slobbe, J. (2013). On security of Implantable Medical Devices.*Technical University of Eindhoven*.

Student Characteristics. (2015, September 9). Retrieved April 2, 2016, from http://www.ir.tcu.edu/factbooks/2015/student_data.asp

Trinckes, J. (2016, February 12). Cybersecurity & Healthcare: Does Cybersecurity Act Help or Hurt? Retrieved April 2, 2016, from http://www.darkreading.com/endpoint/cybersecurity-and-healthcare-does-cybersecurity-act-help-or-hurt/a/d-id/1324292

Whitney, L. (2015, February 9). Apple Watch app will track glucose levels for diabetics. Retrieved February 25, 2016, from http://www.cnet.com/news/apple-watch-app-will-track-your-glucose-levels/

Zawoad, S., & Hasan, R. (2015). The Enemy Within: The Emerging Threats to Healthcare from Malicious Mobile Devices. *University of Alabama at Birmingham*.

Zetter, K. (2014, April 25). It's Insanely Easy to Hack Hospital Equipment. Retrieved March 31, 2016, from http://www.wired.com/2014/04/hospital-equipment-vulnerable/

Appendix A

Table 1: OLS Regression Coefficients for estimated Effects of Gender, Classification, and Experience on Total Amount of Hacking Attacks

Variable	B	β
Experience	-2.82**	-.32 (.95)
Sex	-2.31**	-.27 (.89)
Classification	.798	.091 (.92)
Constant	14.1	
R-squared	.134	

Note. Standard errors are listed in parenthesis.
*p<.05. **p<.01. ***p<.001.