Security Issues of Personal Medical Devices

Submitted in partial fulfillment of the requirements

for the degree of Master of Business Administration

Todd M. Brasel

The School of Business

University at Albany

State University of New York

ITM 698

Fall 2018

Abstract

While Personal Medical Devices (PMDs), a category which includes implantable and wearable medical devices, have immediate and lasting positive effects on patient health, these devices can have unpredictable and detrimental effects on the privacy of the patients, their families, and any groups or organizations that the patient interacts with. PMDs range from established technologies such as insulin pumps and pacemakers, fitness trackers to biometric sensors. actuators for prosthetics, and cranial implants for Parkinson's disease. Despite the different purposes of these PMDs, all PMDs share qualities, such as attack vectors, physical designs, and operational models. The data collected by PMDs is used by a wide group of practitioners, device manufacturers, and insurance providers, often without the patient's awareness. This data contains highly sensitive patient health information. PMDs, because they are integrated into a patient's biology, they also present a unique challenge to security and privacy strategies, because unlike other personal devices, the patient cannot stop using an PMD when entering a building or before engaging in conversation. The use of PMDs also carries some stigma, so patients are reluctant to reveal their usage, and the devices can be difficult to detect, so they are frequently not accounted for in organizational planning. Therefore, PMDs present both a security risk, in that they are often ignored and unprotected, and also a privacy risk, in that the data they collect is widely shared with little or no involvement from the patient. To be fully effective, any personal or organizational security plan should also account for the growing presence of PMDs. This paper will review the current threats to personal and organizational security that are presented by personal medical devices and identify key trends.

Security Issues of Personal Medical Devices

When thinking about personal medical devices, what most readily comes to mind are implanted devices, such as insulin pumps and pacemakers, used for the treatment of the elderly or severely infirm. However, in the last 30 years, new PMDs have been developed, and continue to be developed, to treat a growing number of patients and a growing number of medical conditions.

PMDs do not simply prolong life; they are designed to be integrated into a patient's body and facilitate the patient's ability to perform daily tasks and fulfill their life goals. More often than not, PMDs are present in the working-age population. Your coworker, the person who owns the restaurant near you, or the person working out next to you at the gym, could be using a PMD.

PMDs are not only an integral part of a patient's life, they are an integral part of the patent's treatment strategy. To facilitate the treatment strategy, these devices gather data about the patient, and have the ability to capture information about the patient's environment. Caregivers naturally need access to this data, so the devices have advanced wireless communication capabilities which allow doctors and caregivers to monitor the devices, upgrade them, and have ready access to patient health data.

PMDs have common capabilities and physical designs, and so also have common threats and vulnerabilities to both the patient and to the groups and organizations that the patient interacts with. The qualities and capabilities that are generally presented by PMDs include:

1. They have the ability to connect wirelessly with other devices and patients cannot control when and how their devices connect with other devices.

2. They are integral to the survival, or continued well-being, of a patient and so they are always active. PMDs cannot be removed or shut off without endangering the health of the patient.
3. They collect Protected Health Information about patients and may collect other sensitive information about their environment.

Because of the use and capabilities of PMDs, they have introduced a new and ever-changing set of vulnerabilities and problems that patients are not fully aware of, and have not fully considered. Recommendations for security controls and mitigations of vulnerabilities are rapidly evolving as well. To further compound the problem, the devices are unfamiliar to almost all security professionals. The goal of this paper is to provide background information on the patients, device designs, vulnerabilities, and threats, so that security teams can more effectively access the risk that the presence of PMDs create and make informed decisions about appropriate security controls to mitigate threats.

What Is A Personal Medical Device?

This section provides an overview of PMDs. Personal medical devices are electronic devices that can be divided into two broad categories: implantable and wearable. All PMDs share many common features, which are described in this section.

Implantable devices are designed to be housed inside a patient's body for an extended period of time, and are not intended to be removed. A caregiver interacts with the device using either Near Field Communication (in older devices) or another form of wireless communication in restricted medical frequencies or Bluetooth. A patient will periodically undergo minor surgery to repair a malfunctioning device, or about every seven years, replace the batteries in an

implanted device (Davis, 2011). Batteries of implanted devices need to be replaced every few years.

Wearable devices are designed to be carried outside a patient's body and are held in close proximity, or more commonly in contact, with the patent's body. The wearable device is more easily accessed for maintenance than an implantable device, but the devices have wireless capabilities, similar to implantable devices, to allow for data collection and system maintenance while minimizing interruptions to the patient's normal routine and to reduce the number of visits to a caregiver's office.

Both wearable and implantable devices have a two-segment design comprised of a control and communications unit and a machine-body interface unit. The command and communications unit monitors the patient's health, monitors the condition of the unit itself, dispenses therapeutic measures, uploads information to external sources, and receives information, such as firmware updates, from external sources. The machine-body interface is how the device delivers the therapeutic measures necessary for treating the patient's condition. This design style is most obvious with wearable units, such as an insulin pump. Wearable insulin pumps, for example, use a small needle that is positioned just under a patient's skin to dispense insulin. While it may be odd to think of an implantable device as having a separate unit for mind-body interface (since it is, after all, inside the patient's body) the control and communications unit is not designed to directly interact with the patient. The machine-body interface consists of a separate junction. In the case of an implantable cardiac device, electrodes in the patient's heart form the machine-body interface. Other implantable devices, such as those used for the treatment of seizures or tremors, use electrodes implanted in the patient's brain; implantable insulin pumps

(which have been phased out of production) use an injection site close to where the body naturally introduces insulin into the bloodstream.

PMDs all possess the following characteristics:

- They are constantly present with the patient. This differentiates PMDs from cell phones, and other monitoring devices such as FitBits, which the user may have in close proximity to his or her body for most of the day and can remove when necessary or desired.
- They are networked devices. They are designed to share data with a care provider and receive updates to firmware via a non-direct connection, to facilitate a patient's lifestyle and minimize office visits.
- They have considerable computing power. Like the other portable computing devices we are familiar with in today's consumer market -- smart phones and connected vehicles -- personal and implantable medical devices also have considerable computing power, yet power that is shaped by the restricted domain of their purpose for medical treatment, and design, to fit as unobtrusively as possible with the wearer's body and quality of life. The devices are fascinating from an engineering standpoint because they have to meet the goals of low cost, long lifetime, durability, and reliability. For example, an implantable cardiac defibrillator can perform many functions beyond the one function that its name implies, and contains sophisticated programming that can recognize and respond to tachy-arrhythmias (irregularities in heart rate and rhythm) with no external intervention (Maisel, Sweeney, Stevenson, Ellison, & Epstein, 2001).
- They collect very sensitive data about their users. This data can include information such as heart rhythm or brain wave patterns, which can simultaneously uniquely identify a user

and their health conditions. This data can also be combined with other data to infer patterns of behavior in the individual and to infer information about the user's environment.

- They are specialized devices, built from a hardware and software perspective to fulfill a specific medical purpose. This differentiates them from consumer devices such as smart watches, which perform many functions and are user-customizable.
- They have a very limited user interface. These devices are designed with the intention that only a care provider can modify their functionality.
- They are necessary for maintaining life, or the quality of life, in a patient. If the functioning of a PMD is disrupted, the user may suffer severe bodily harm or death.

The most common PMDs currently in use at the time this paper was written are implantable cardiac devices and insulin pumps. The number of reported users is difficult to track and varies by source, but generally there are about 1 million users of insulin pumps around the world (with most patients in the United States) and about 2.9 million patients who have implantable cardiac devices in the United States (Greenspon et al., 2012).

Legal Aspects of PMD Security

Although a comprehensive discussion of the legal aspects of PMD security is beyond the scope of this paper, there are key aspects that provide context for security issues that are related to medical devices.

In the US, The Digital Millennium Copyright Act and the Computer Fraud and Abuse Act affect both attackers and defenders. From an attacker's standpoint, these Acts provide the basis for the legal system to pursue actions against them. In an interesting twist for defenders,

however, these Acts constrain the ability of researchers to investigate both the existence of security vulnerabilities and remediation or mitigations of vulnerabilities. Because of the language of these laws, a security researcher who is attempting to reverse engineer, or to get around, the security controls of a medical device to examine how it functions could be violating the law. This arises, for example, because any action to circumvent the security controls that prevent access to copyrighted material (such as the computer code that runs on the device) would be illegal. However, the Federal Trade Commission (FTC) reviewed and put into effect an exemption that allows researchers to legally perform investigations of consumer devices. Researchers must follow strict rules, such as carrying out research in a controlled environment, perform research only for specific purposes as outlined in the exemption, and other rules. As of the time this paper was written, this exemption was fully adopted in 2015. ("Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies," 2015).

Also in the US, medical devices fall under the aegis of the US Food and Drug Administration (FDA). Therefore, US federal law also affects how manufacturers inform the government about problems with medical devices. The Medical Device Reporting (MDR) regulation 21 CFR 803 contains mandatory requirements for manufacturers, importers, and device user facilities to report certain device-related adverse events and product problems to the FDA ("CFR - Code of Federal Regulations Title 21," n.d.). One result of this ruling has been to affect how manufacturers are affected in product liability claims. In 2008, however, in a key case known as Reigel v. Medtronic, the US Supreme Court ruled to limit the liability for the manufacturers of medical devices when FDA-approved devices cause harm to patients ("Riegel v. Medtronic, Inc., 552 US 312 (2008)," 2008). This case may have had important input into how

manufacturers have or have not taken action to reduce the vulnerabilities of medical devices to adversarial and non-adversarial attacks, and in one case resulted in a US District Court judge dismissing over a thousand cases filed against a manufacturer that cited a defective component in a ICD (Curfman, Morrissey, & Drazen, 2009).

The US FDA has continued to develop guidance for medical device cybersecurity since 2003 with initial draft guidance released in 2013. The initial draft drew on elements of the National Institute of Standards and Technology (NIST) cybersecurity framework (Burns, Johnson, & Honeyman, 2016) . These draft recommendations were finalized in 2016 and provide guidance and non-binding recommendations for managing the cybersecurity of personal medical devices (US Food & Drug Administration, 2016).

Predisposing Conditions and Vulnerabilities

This section describes the predisposing conditions and vulnerabilities that arise from the use of personal medical devices. For this paper, the following definitions of the terms "predisposing condition" and "vulnerability" are used:

- Predisposing condition: "A condition that exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operation, which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts" (Joint Task Force Transformation Initiative, 2012).
- Vulnerability: "A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source" (Joint Task Force Transformation Initiative, 2012).

Characteristics of PMD Users

A common misperception is that PMDs are solely used by the elderly or infirm. The history and trends of PMD usage challenge that belief. An important trend in PMD users is that they are being used with younger people than in the past. The idea that only the elderly, or severely infirm, receive personal medical devices has changed dramatically since 1966, when pacemakers were approved for Medicare reimbursement. At that point, the American College of Cardiology determined that the use of pacemakers was a reasonable approach for the treatment of 56 heart conditions, and since then, the list of conditions approved for treatment by implantable cardiac device has increased to 88 by 2008. Approximately three million Americans had a pacemaker by 2009 (Norton, 2012).

The most common users of PMDs are currently cardiac patients and diabetics.

Regarding cardiac patients, the average age of a cardiac patient, regardless of gender, who uses a PMD is 65-85 years (Armaganijan et al., n.d., and Greenspon et al., 2012). A significant number of patients with a cardiac PMD are of working age. Overall, six percent of pacemaker patients are under 49 years old (Davis, n.d.). The largest decile of men who use cardiac IMDs are 45-54 years old (Feldman et al., 2016). One author has observed that "Out of the total pacemakers installed every year, 2 percent of patients are under 22, 4 percent are 22-49, 10 percent are 50-65 and 84 percent are 65 and older" (Davis, 2011).

One example of a contemporary cardiac patient is Frank (whose name has been changed to maintain his privacy), who is a 53-year-old owner of a physically and mentally demanding business in the field of hospitality and catering. In 2017, he survived a heart attack, and a few months later, had to have a cardiac monitoring device implanted to help his heart to maintain a

steady rhythm. Frank is physically active and has retuned to all of his daily activities, and is expected to live a normal life, though he will always have to have an ICD. In addition to managing his business, Frank returned to his weekly practice of Chon Tu Kwan ("Combat") Hapkido, a martial art in which he has attained the rank of 4th Gup ("brown belt"), and expects achieve the ran of 1st Dan ("black belt") in the next few years.

Other examples of younger patients include:

- Shoshana Davis, a magazine writer in her mid-20s. In her first article to discuss her treatment, she wrote: "While I'm not the only person under 65 with a pacemaker, it is rare, and to most security officers, I'm the only one they've ever seen." (Davis, 2011)
- Neta Alexander, a doctoral student and cardiac patient, who received her pacemaker at age 34 (Alexander, 2018).
- Marie Moe is another security researcher who has an implanted pacemaker, who also is researching the security threats that exist for these and similar devices. She describes her age as "younger than most pacemaker patients" (Moe, 2016).

Diabetics, who often use wearable PMDs such as insulin pumps, are even more frequently found in the workforce. The typical age of a diabetic patient who uses an PMD varies considerably. The average age of diagnosis for a diabetic is about 10 years ("Insulin pump statistics about adults and children with diabetes," 2018) and as young as 1 year (Nykaza, Arbiter, & Snider, 2018). Usage data on insulin pump patients is very rare. One available source estimates that there are about 1 million patients globally who use pumps, with most pump users in the United States (Heinemann et al., 2015). The author has observed insulin pump users in

different professions, such as software engineers and attorneys, and who are parents and also active athletes, such as competitive fencers.

Communication Capabilities of PMDs

IMDs and PMDs have wireless communication capabilities that make use of various frequencies and protocols. The purpose of these communication capabilities are to connect the medical device with a base station, which acts to relay medical information to the care provider's database, and connect the medical device to a "programmer," which is an industry term for a device used to configure and update the device. The frequencies and protocols that the devices use vary based on the device manufacturer. According to Williams & Woodward, information that attackers need is usually available from the agencies that certify these devices (Williams & Woodward, 2015) such as the FCC, which makes publicly available information about devices based on the the federal communications commission identifier (“FCC OET Authorization Search,” n.d.). Other details such as radio frequencies used, device manuals, and other information about IMDs and PMDs can be obtained from online sources, such as the manufacturer. Communication between the device and its base station/programmer cannot be disabled (Goodin, 2011).

Common wireless frequencies for use in communication between the medical device and its base station or programming device include the following. The typical effective communication range is about 10 meters. For smaller, more limited devices, such as Continuous Glucose Monitoring sensors, the effective range of sensors that are non-Bluetooth enabled is limited from 1.5 inches to 6 feet.

- The 402-405 MHz Medical Implant Communication Service (MICS) band (Ellouze, Rekhis, Allouche, & Boudriga, 2014 and Halperin et al., 2008).
- The 175 kHz band is used by older neurostimulators and ICDs (Marin et al., 2018 and Halperin et al., 2008)
- The 900 MHz frequency is used for insulin pumps and some ICDs (Halperin et al., 2008 and Goodin, 2011)).
- Bluetooth Low Energy (BLE) is becoming a popular protocol as manufacturers roll out phone apps that augment, or even take the place of the traditional base station necessary for the device to upload data to the care provider's database. Medtronic is one such manufacturer that is offering apps for Android and iOS to support data gathering by care providers (Medtronic, 2018).

Access and Authorization for PMDs

To understand the access model for personal medical devices, some background information about how the devices are intended to be installed in a patient is helpful. In a telephone interview with a medical technologist at an upstate New York hospital, the interviewee, who wished to remain anonymous, provided some insight into procedures regarding how personal medical devices are installed, based on procedures used in a hospital where the person works.

In many cases, hospitals, especially those that belong to smaller regional systems, do not maintain inventories of ICDs and coordinate installation with the vendors, who deliver the devices directly to the hospital.

When the care provider arranges for an operation to implant the device in a patient, the hospital makes arrangements with the device vendor. At the time of installation, sales

representatives for the medical device manufacturer transport devices to the hospital and assists surgeons with programming the devices. The sales representatives are present in the operating room when the device is installed and ensure that the device is functioning properly.

During the installation procedure, access to the device is achieved by direct contact with the device and through the use of a short PIN to unlock the device. The hospital keeps a cross-reference chart of PINs that are based on the serial number of the device. The vendor, of course, also maintains the same cross-reference information, in case the hospital or other care provider needs this information (“Interview with Hospital Medical Technologist,” 2018).

Installation and maintenance procedures for personal medical devices were developed during a time when direct contact had to be made to electrodes that are near the surface of the skin or when in the presence of a magnetic programming head with a strength of about 700 gauss (Halperin et al., 2008). However, contemporary devices, with more powerful wireless capabilities described in this paper, do not require direct contact with the patient for set up. Authorization for the devices has not kept up with changes in communication technology, as seen in the work of researchers such as Scott Erven, whose team investigated security issues in hospital medical devices. In an article for Wired magazine, Erven said that his team "found a couple of defibrillator vendors that use a Bluetooth stack for writing configurations and doing test shocks [against the patient] when they’re implanted or after surgery... They have default and weak passwords to the Bluetooth stack so you can connect to the devices. It’s a simple password like an iPhone PIN that you could guess very quickly" (Zetter, 2014).

Other research has been done into acquiring unauthorized access to implanted devices directly, such as Halperin et al., 2008, who found that communication with some types of ICDs

can be initiated through the use of open-source software such as GNU Radio and COTS software-defined radio dongles (Halperin et al., 2008).

Known vulnerabilities related to authorization also exist in the base units that are present in a patient's home. For example, for two versions of Medtronic MyCareLink monitors, there are known vulnerabilities based on hard-coded passwords in device software (CWE-259 / CVE-2018-8870) and debugging code still present in production which "provides the ability to read and write arbitrary memory values via wireless protocols" (CWE-749 / CVE-2018-8868) (“Vulnerabilities Identified in Medtronic MyCareLink Heart Monitors,” 2018).

Data Collected By And Present In PMDs

Personal medical devices contain patient-specific health information and information that they collect from the patient. As an example, ICDs collect data from the patient such as the patient's electromyography (how well the patient's heart muscle responds to nerve signals) and device responses to arrhythmia. Some devices examined by researchers contain, and will transmit in cleartext, data such as "name, date of birth, medical ID number, name and phone number of the treating physician, the dates of ICD and lead implantation (which may differ), the model, and the serial number of the ICD and leads" (Halperin et al., 2008).

Cryptographic audit logs and protection for other log information collected by the device have not been available on-device (Ellouze, Rekhis, Allouche, & Boudriga, 2014) until recently. In its marketing literature for its latest models, Medtronic states that data on some of its devices is protected through cryptographic algorithms, but does not provide information to consumers about the nature of the encryption used and does not mention logging of access attempts (Medtronic, 2018).

How Personal Medical Devices Are Deployed

Implantable Devices

Implantable medical devices are prescribed by medical specialists, such as cardiologists, as part of an overall treatment program for patients. IMDs currently fit into two similar, but related, physical design platforms: those used to monitor electrical activity and deliver corrective electrical impulses (commonly, and somewhat incorrectly, referred to as "pacemakers") and those used to deliver medication (such as implantable pumps that deliver insulin).

The reasons for implanting a medical device in cardiac patients vary, and have increased in the US in the past few decades since their approval by the FDA (Greenspon et al., 2012). The list of devices, and purposes includes:

- Actual pacemakers, which maintain heart rhythm
- Cardiac resynchronization therapy devices (to synchronize heart chambers) (“Cardiac Resynchronization Therapy (CRT),” 2017)
- Implantable cardioverter defibrillator devices, which prevent arrest in patients at risk for ventricular arrhythmia, or who have ventricular tachycardia or fibrillation (“Implantable Cardioverter Defibrillator (ICD),” n.d.). This category of devices monitors rhythm and can act as a pacemaker and defibrillator if necessary (“Pacemakers and Implantable Defibrillators,” n.d.).
- Implantable cardiac monitors are devices that can be implanted for at least 36 months. They are used to monitor cardiac health and also for investigating other health issues such as epilepsy, asymptomatic arrhythmias, and unexplained falls. They can be slightly smaller than a pacemaker. (Giada, Bertaglia, Reimers, & Noventa, 2012)

- Left ventricular assist devices, which is a pump that augments the actions of the left ventricle, which distributes blood from the heart to the body (“Implantable Medical Devices,” n.d.).

Each implantable device consists of a puck-like main unit that has electronic leads which connect to the patient's body.

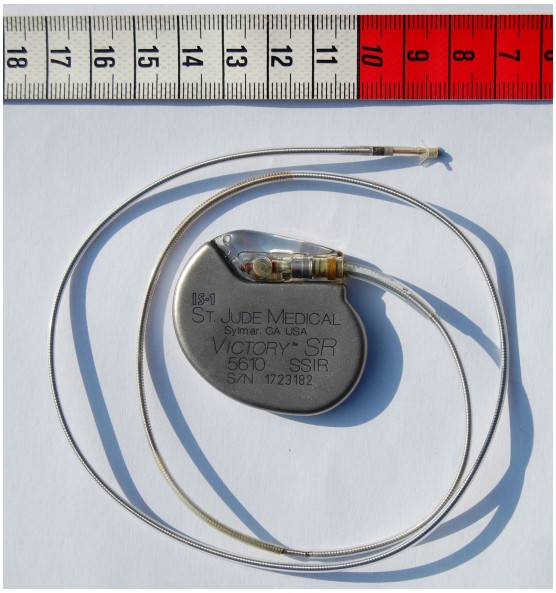

Figure 1. An implantable cardiac device (“Artificial cardiac pacemaker,” 2018)

The main unit is placed in a kind of "pocket" just under the patient's skin. For example, a pacemaker-style unit is often placed near the left front shoulder, above the pectoral muscle. After the incision heals, patients can return to a very high degree of mobility.

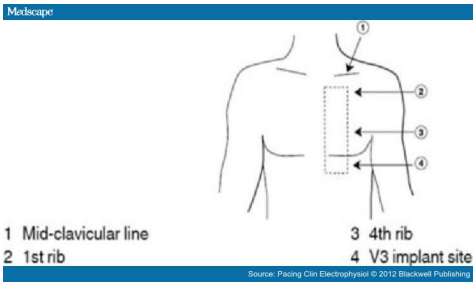

Figure 2. Typical location of an ICD in a patient's body (Giada, Bertaglia, Reimers, & Noventa, 2012)

Implantable insulin pumps were more common until Medtronic stopped manufacturing them in 2007. These pumps had a similar design platform to implantable pacemakers. The use of implantable insulin pumps has fallen out of practice in favor of wearable pumps, and research has turned away from this design platform to focus on the development of a closed-loop, "artificial pancreas" platform that is implanted in the patient's body and replaces the insulin-producing function of the pancreas. By 2017, only four users of insulin pumps remained in the United States (Hoskins, 2017).

Wearable Devices

Wearable medical devices that dispense therapeutic measures are also prescribed by medical professionals. These devices can be grouped into two physical design platforms.

The first is a small puck-like sensor designed to be hidden under clothing. The device monitors some aspect of the wearer's physiology. One example of a device in this format is a family of devices known as Continuous Glucose Monitoring (CGM) devices. Unlike manual blood glucose monitoring systems, which rely on directly sampling the patient's blood, a CGM can monitor the patient's body chemistry and calculate the wearer's blood glucose level.

By themselves, these types of sensors are unable to perform any corrective action (Brown, n.d.). They are intended to be used to gather data about the patient's health and share that data with other devices, such as an insulin pump, or monitoring software on a smart phone (Neithercott, 2015).

Figure 3. Wearable health sensor (Bowman, 2018)

The other common form of wearable medical device is an infusion pump. These wearable devices are usually attached to a belt or carried in a small pack, and medicine is delivered to the patient by means of a small diffusion needle under the skin. The devices are programmed by a medical professional. The most common form of this device provides capabilities that facilitate diabetes management, such as continuous glucose monitoring and insulin delivery (American Diabetes Association, n.d.).

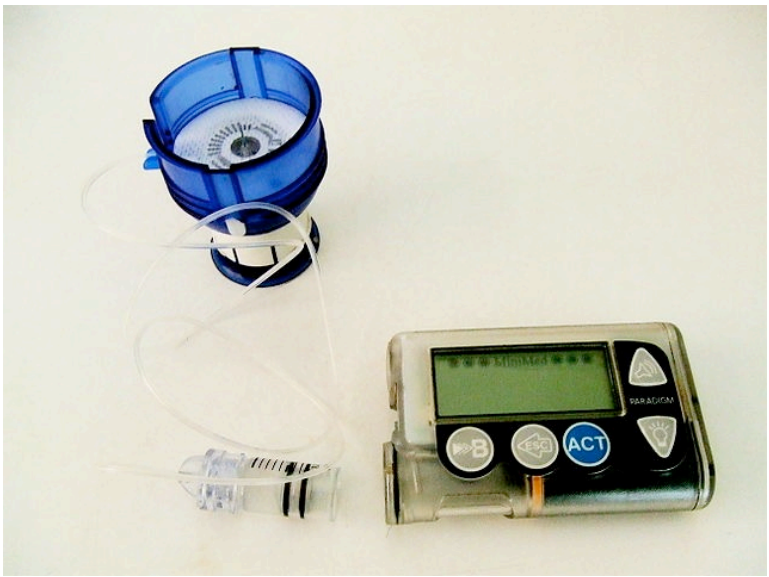

Figure 1. Insulin pump and diffusion needle (Werther, 2007)

Beginning in 2017, an increasing number of newly manufactured wearable insulin pumps have Bluetooth connectivity to allow the user to connect them to a smart phone, or other Bluetooth enabled device, to transmit data collected about insulin dosage history, temperature, and blood sugar levels and receive software updates. These devices can either connect directly to a smart phone or receiver, or connect through a small, keyfob-sized device that is carried separately from the pump itself (Integrated Diabetes Services, n.d., and “MiniMed Connect FAQs | Medtronic Diabetes,” n.d.).

Attacking Personal Medical Devices

The previous sections discussed vulnerabilities and predisposing conditions involved with the use of personal medical devices. This section will describe threat scenarios that arise from the vulnerabilities and predisposing conditions. NIST defines a threat scenario as a hypothetical situation that describes "how the events caused by a threat source can contribute to or cause harm" (Joint Task Force Transformation Initiative, 2012).

Threats and threat scenarios that can arise from the presence of PMDs are divided in the following sections into threats to individuals and to organizations, to help security professionals understand how the same, or related, threat can simultaneously affect an individual and an organization.

To further differentiate threats, each section will divide the threats into the NIST categories of "adversarial" and "non-adversarial" threats. Adversarial threats arise from "individuals, groups, organizations, or entities that seek to exploit an organization's dependence on cyber resources." In this context, the entities intend to exploit the patient's dependence on the medical device. Non-adversarial threats arise from "natural disasters or erroneous actions taken

by individuals in the course of executing daily responsibilities" (Nieles, Dempsey, & Pillitteri, 2017).

Overview of Research Into Attacks

As shown in the section on access and authorization for PMDs, these wireless-enabled medical devices are vulnerable to radio-based attacks. The communication frequencies involved make the device accessible from both stolen programmers and programmers that have been reverse-engineered by using electronic equipment such as oscilloscopes and software-defined radio equipment.

Daniel Halperin and his team were able to use a Software Defined Radio dongle and the open-source GNU Radio software to intercept and study the communication from an implantable cardiac defibrillator, which connects to a nearby programming unit on a frequency of 175 kHz and 402 MHz. The researchers were successful enough in reverse-engineering the device's communication protocol to read data from the device without the patient's knowledge, to disrupt the ability of the device to function, and harm the patient (Halperin et al., 2008). Documented vulnerabilities exist in ICDs that use the 175 kHz band, 402-405 MHz Medical Implant Communication Service (MICS) band, and Bluetooth.

Insulin pumps are also vulnerable to wireless attacks. In his research, security expert Barnaby Jack was able to compromise insulin pumps from a range of 300 feet away. He used a custom-built antenna and software to scan for devices in this radius that are vulnerable and then attack the devices (Goodin, 2011).

Based on the communication capabilities of implantable medical devices, the possible attacks involve intercepting traffic and examining it for sensitive data, analyzing traffic for

information leakage about other connected devices such as hospital equipment or smart phones, or information about networks that the device has connected to, and gaining access to the device (Ellouze, Rekhis, Allouche, & Boudriga, 2014). The attacker could, for example, replay a sufficient number of messages that would drain the device's battery, or jam the device's communications.

If an attacker can gain access to the device, by sniffing credentials or social engineering, the attacker will be able to disrupt the therapeutic function of the device and cause harm to the patient, by administering medication or treatment (shocks) or preventing the dispensing of therapeutic measures in the event of a health issue (preventing the dispensing of insulin or shocks). The attacker will also be able to cover their tracks by modifying logs -- although frequently the devices do not perform logging -- and performing other actions that any attacker of an embedded system would perform.

Because of the nature of wireless communication and the lack of authentication on the devices themselves, all devices can be considered to be vulnerable to spoofing, replay, man-in-the-middle, denial-of-service, and replay attacks. These devices are vulnerable due to weak authentication techniques (brute-force and replay), exchange of sensitive data with the programmer in plaintext or weakly encrypted communication, and no monitoring or detection of communication behavior or connections. This opens the devices to an attacker modifying settings (to alter how and when therapeutic shocks are delivered), or cause a denial or degradation of therapy by forcing the device to stay in power-burning modes, thus depleting the device battery through repetitive command execution (Ellouze, Rekhis, Allouche, & Boudriga, 2014).

FIngerprinting and Data Leakage

“Fingerprinting” is another privacy threat and a security threat to users of personal and implantable medical devices.

A common example of fingerprinting is found everyday in the use of a web browser. Each browser and device has a unique fingerprint that can be used to identify it online. In an online setting, user fingerprinting is done by code that looks at the browser, the computer (including graphics hardware), plugins or extensions to the browser, the operating system, timezone, language, settings such as Do Not Track, fonts, screen resolution, and other factors. All the information that a site can gather about a user is reduced, by means of a mathematical operation called hashing, to a long number that essentially uniquely identifies the user, and can also be easily shared between service providers. The service providers assume, since computing devices are essentially personal devices, that the device profile uniquely identifies the user when they are online. This type of fingerprinting can be up to 99% accurate based on the technique (Cao, Li, & Wijmans, 2017).

Implantable and personal medical devices can also be used to fingerprint a patient, and in much the same way that users can be fingerprinted when they browse the web. This fingerprinting is achieved by interrogating the device's wireless interface and any information that is made available according to the wireless communication standard that the interface conforms to, such as the Bluetooth standard.

If an implantable or personal medical device has the ability to connect to wi-fi or bluetooth networks, then, like other devices such as computers, phones, and internet-capable refrigerators, the device will have a Network Interface Controller (NIC) which allows it to connect to a network, and that NIC will have a Media Access Control (MAC) address (or similar

identifier), which acts as a "address" for network communication. MAC addresses, in contrast to internet protocol (IP) addresses, never change, so the MAC address uniquely identifies the device, and by extension, the patient who uses it.

When they are powered on, Bluetooth devices will provide information about their configuration, manufacturer, and other details, to devices that can interrogate them (Nordic Semiconductor, n.d.). The following illustration shows how an iPhone app, freely available in the Apple App Store, gives any iPhone user the capability to interrogate Bluetooth devices within range of its Bluetooth radio. (All screen captures were generated by the author, using LightBlue Explorer software on an iPhone 6. A non-medical commercial device was used.)

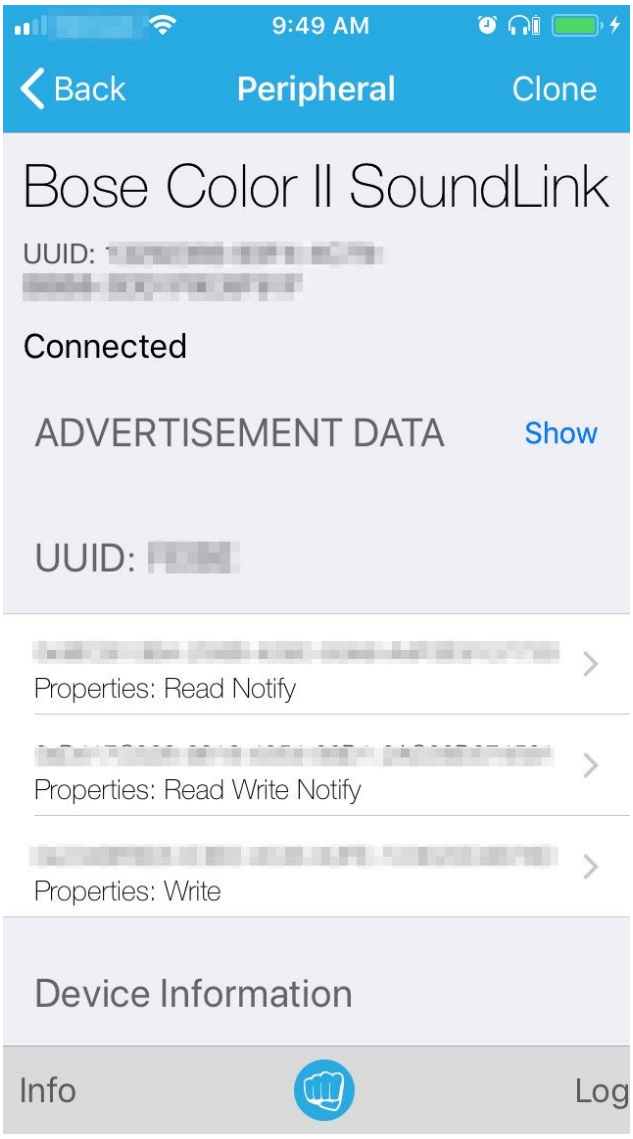

Figure 4. Displaying the device UUID

The first screen capture displays the Universally Unique Identifier (UUID), which is a 128-bit number that is not shared by any other Bluetooth device. When a Bluetooth device links to another Bluetooth device, both devices remember each other's UUID, as part of the connection (or "pairing") process.

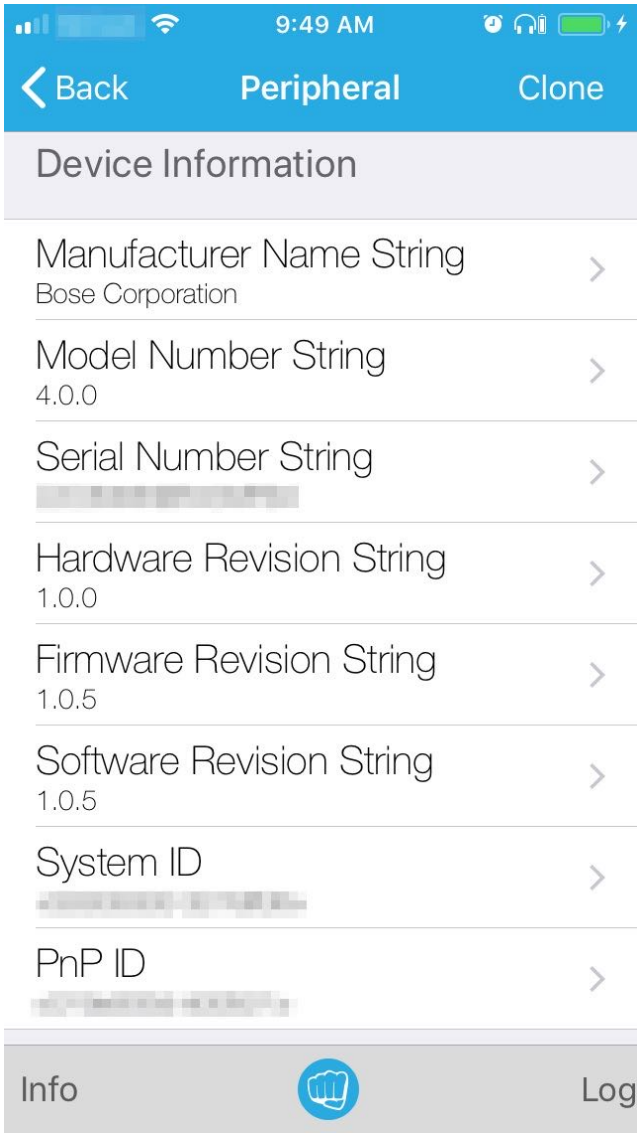

Figure 5. Information About the Device

The second screen capture displays information about the device itself, such as the manufacturer, and information about the hardware, software, and firmware in use on the device. This information is made available for diagnostic purposes and may not be available to every other device that connects to it.

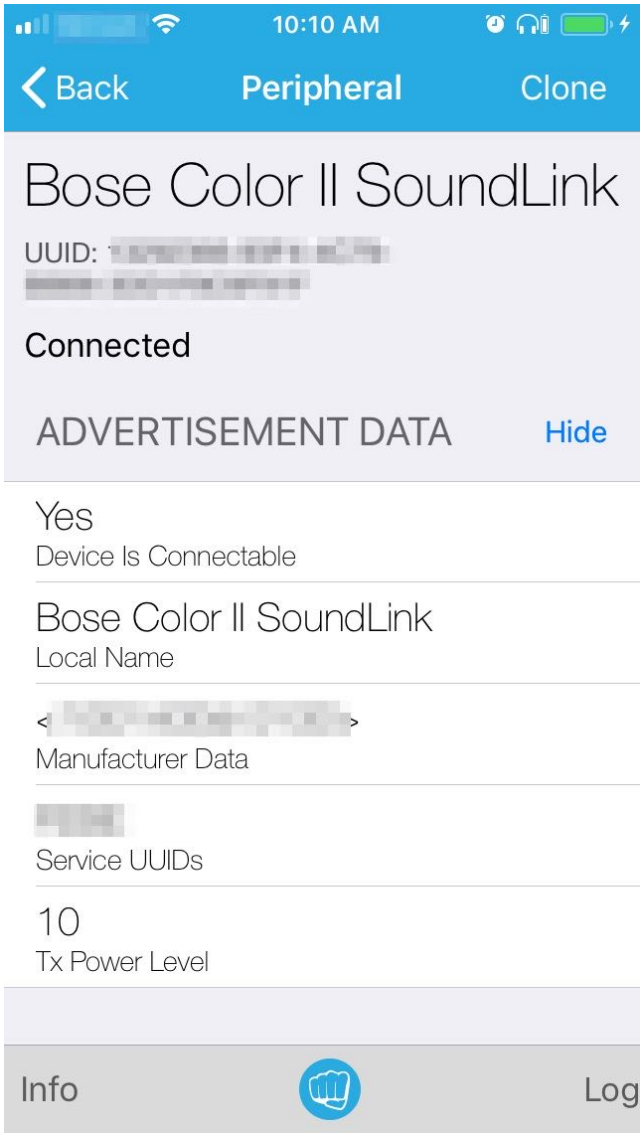

Figure 6. Advertisement Data

The third screen capture shows the "advertisement data," information that other devices use when establishing a connection. The "local name" is the human-readable identifier that will be displayed to the user of the device that is paired to this device. The other key piece of information available are the "service UUIDs," which declare what the purpose of the device is and its capabilities. In this example, the Bose speaker tells the other device (e.g. a cell phone or computer) that it is an audio output device and accepts audio output. Devices with other

capabilities will declare those capabilities here, according to the Bluetooth Service Discovery Protocol specification.

In the case of a medical device such as PMD, the device may advertise that it offers a heart rate monitoring capability with the following characteristics: the heart rate itself, the body sensor location, heart rate control point, and battery level. The characteristics offered may be mandatory or optional. In the case of the heart rate monitor, the heart rate and battery characteristics are mandatory, and the body sensor location is optional. (The body sensor location characteristic values are: chest, wrist, finger, hand, earlobe, foot, "other," and 248 values that are unused but reserved for future use (“Bluetooth Body Sensor Location,” n.d.).) Thus, it is possible for an attacker to reveal sensitive about patients who use Bluetooth-enabled PMDs simply by scanning for active Bluetooth devices in their vicinity, and without even attempting to gain access to the devices themselves. However, as of the time that this document is written, Bluetooth standards for medical devices are actively under development (Latuske, n.d.) and are drawn from IEEE standards for healthcare IT (“IEEE SA - Healthcare IT Standards,” n.d.).

History And Timeline Of Threats

While there, as yet, have been no documented cases of attacks on personal and implantable medical devices, the attack surfaces of PMDs and IMDs have changed over time, and the capabilities of attackers have evolved as well. The following section presents a timeline of the the evolving threats against personal and implantable medical devices.

Prior to 2000

In this time period, device problems were mainly due to non-adversarial threats. Any device failures were mostly limited to non-implantable devices that were used in a clinical setting or in a patient's home (Burns, Johnson, & Honeyman, 2016).

The main problem encountered with implantable devices also involved non-adversarial issues. In the ten year period leading up to the year 2000, the FDA recalled 114,645 implantable cardiac defibrillators. During this period, 95% of recalls were caused by hardware malfunctions and computer errors. The hardware malfunctions, which accounted for about 60% of problems, included malfunctioning parts, such as capacitors and oscillators (which would cause problems with pulse amplitude and cardiac pacing), poor soldering, and defective seals. The software issues, which comprised the remaining 40% of problems, included programming errors that were attributed to unanticipated complexities of interfacing computing devices with real-world situations, which in this period began to invite comparisons with the complexities of building firmware solutions for avionics, spaceflight, and nuclear energy (Maisel, Sweeney, Stevenson, Ellison, & Epstein, 2001).

2000-2005

The High Confidence Medical Device Software and Systems (HCMSS) workshop was conducted in Philadelphia in June of 2005. This conference was sponsored by five US government agencies, including NIST and NSA, and featured inter-agency participation in the form of the Networking and Information Technology Research and Development (NITRD) program. The goal of the workshop was to create a strategic plan to address issues with the creation and use of medical devices. This workshop has led to additional workshops on related topics (Goldman & Whitehead, 2007).

2005-2010

In this period, about half of medical devices available for patients included functions that were controlled by software. Research in this period included investigating the feasibility and security of updating software in embedded devices that are mobile and have intermittent network connectivity, a model for implantable medical devices that are controlled by software (Burns, Johnson, & Honeyman, 2016).

In 2008, a key attack was demonstrated by researchers against an IMD. In the attack, vulnerabilities were exploited in an FDA-approved implantable cardiac defibrillator, which allowed the researchers to use a Software Defined Radio to intercept data logged by the IMD and control how the device delivered electric shocks to a patient's heart. This was the first known attack of its kind (Halperin et al., 2008).

Daniel Halpern and others present a framework for securing implantable medical devices in (Halperin, Heydt-Benjamin, Fu, & Maisel, 2008).

2010-2015

The feasibility of several attacks against implantable insulin pumps were demonstrated in this period. The authors of Hijacking an Insulin Pump investigated the potential for attackers to eavesdrop on wireless communication between implantable insulin pumps and programmers and purposefully modify the therapeutic programming of these devices, by using Software Defined Radio hardware (which is available on the open market), and publicly-available information about the devices (Li, Raghunathan, & Jha, 2011).

In this period, Jay Radcliffe, a diabetic, gave a presentation at Black Hat, and described described how he had begun to reverse-engineer the communication protocol for the insulin

pump that he used. His work revealed a weakness for other insulin pumps that would allow an attacker to wirelessly obtain access and so control the pump (Basu, n.d.).

Hacker Barnaby Jack presented his findings at the Hacker Halted conference and described other vulnerabilities in insulin pumps that would allow an attacker to control the pump through its wireless interface (Goodin, 2011).

The feasibility of more complex attacks against implantable cardiac medical devices is also further investigated. In a "Digital Investigation of Security Attacks on Cardiac Implantable Medical Devices," the researchers explore the capabilities of this type of IMD, and determine that this class of device is vulnerable due to weak authentication techniques such as brute-force and replay attacks, that exchange of sensitive data with the programmer is done in plaintext or through weakly encrypted communication, and that there is no monitoring of communication to determine baseline behavior, or any deviations from that behavior, or monitoring of connections to determine if a connection to a device is legitimate. These devices, the researchers determined, are vulnerable to an attacker modifying settings (to alter how and when therapeutic shocks are delivered), and even depleting the device battery through repetitive command execution. The researchers outline several simple and complex attacks with the goal of determining if it is possible to forensically investigate an attack on a device. While it was found that there are several methods that investigators could use after a suspected attack to determine if an attack occurred and what type of attack, at the time the article was written, there was no methodology that exists that describes how this type of investigation would be carried out. The researchers propose a methodology for carrying out a forensic investigation into an attack on an IMD (Ellouze, Rekhis, Allouche, & Boudriga, 2014).

Barnaby Jack presented his findings related to pacemaker attacks at the Ruxcon Breakpoint Security Conference. Jack demonstrated, on a pre-recorded video, how he was able to command a pacemaker through its wireless interface and order the pacemaker to deliver a shock. He also described how implantable pacemakers would provide credentials when someone transmitted a command to the device wirelessly, which an attacker could then use to control the pacemaker (Burns, Johnson, & Honeyman, 2016).

2015-Present

Further investigation into adversarial threats on medical devices is now also pursued by security researchers who are themselves patients, and who bring a deeper understanding of the medical issues involved. All researchers are stymied by the closed-source nature of these devices, which makes it difficult to study their capabilities and properly analyze their threat surfaces (Rios & Butts, 2017).

New non-adversarial threats begin to emerge during this time period. A 66-year-old patient who was being treated for neck dystonia (tremor) by means of a direct brain stimulation IMD experienced an unusual event when her apartment was struck by lightning. The power surge from strike destroyed her air conditioner and television, but more importantly, the very strong EMF field generated as a result of the strike caused her implantable medical device to turn itself off. She was able to restart the unit without a problem, and the unit did not incur any damage. Note that the device and its base unit (programmer) were not physically connected to the main power supply during the storm - it was the electromagnetic field from the storm that caused the unit to shut itself off (Prezelj, Trošt, Georgiev, & Flisar, 2018).

Devices with GPS capabilities are involved in data breaches. The use of fitness trackers by military personnel revealed sensitive information about military bases when users uploaded that information to a fitness data sharing site Strava (Sly, 2018).

New adversarial attacks also begin to emerge in this time period as direct brain stimulation devices begin to be implanted in patients. The devices have the capabilities to record the brainwaves of a patient, and is capable of recording brain activity such as when a patient is presented with, and recognizes, information that is familiar to them, and could potentially be used as a side channel attack to uncover sensitive information. The device can also be attacked in such a way to immobilize the patient and cause damage to his or her brain (Marin et al., 2018).

Summary of Threats to Individuals

Individual threats related to implantable medical devices arise from the exploitation of vulnerabilities in the devices themselves. The patient, or data about the patient, is used to coerce the patient into taking action against their will, or to cause harm to the patient.

Individual threats fall into the two general categories: adversarial and non-adversarial.

Adversarial Threats and Threat Scenarios:

- Spear Phishing. An attacker uses their knowledge of the patient's condition, or use of a medical device, to trick them into divulging more information about themselves or their organization, or to download malicious software onto their computing devices.
- Extortion. An attacker uses their knowledge of the patient's medical device and condition to create an existential threat. The attacker uses the threat to force the patient to perform acts against their own will which cause damage to their well-being.

- Espionage or Reconnaissance. An attacker uses their knowledge of the patient's medical device to learn about the systems of that device, or to gather or infer information about systems that the device encounters as the patient goes about their daily life. The attacker can also seek to steal ("exfiltrate") data from the system under attack. In this case, the goal of the attack is to reveal information specifically about the patient, or to cause harm to the patient.
- Bodily Harm. An attacker uses their knowledge of the patient's condition and medical device to cause harm to the patient.

Non-adversarial Threats and Threat Scenarios:

- Device Configuration and Misconfiguration. A medical professional has to configure the device, after deployment, to properly conduct therapeutic interventions. The caregiver can inadvertently configures the device so that it operates in an insecure manner or causes harm to the patient. The device manufacturer may also configure the device in an insecure manner (for example, its default configuration, or a patch that disables information security safeguards), resulting in a loss of confidentiality for the patient. Usually, simply configuring the device to work properly is time-consuming; Marie Moe states that configuring her device took several months before it was properly tuned to her lifestyle and medical conditions (Moe, 2016).
- Device Malfunction. Some devices are more prone to failure than others. However, data on device failures is not readily available. One of the few studies was a US survey from the 1980s, which found that 25% of infusion pumps malfunctioned, with about 43% of those failures attributed to drive failure and battery issues. Modern pumps may be more

reliable, the authors add, "but the available information is insufficient for this to be concluded with certainty" (Heinemann et al., 2015).

- Loss of Support Infrastructure. During a natural or man-made disaster, the patient may be unable to have their device maintained, causing harm to the patient's well-being. On a less catastrophic level, the device manufacturer may cease support for the device or end manufacture altogether, which has happened in the case of implantable insulin pumps (Hoskins, 2017).
- Interference. The device may be accidentally subjected to impact, electrical fields, or other situations which cause it to behave in an unpredictable manner, putting the patient's life at risk. Even something as simple as a magnet can disrupt the functioning of some implantable devices (Allison & Mallemat, 2015).

Summary of Threats To Organizations

Organizational threats related to implantable medical devices arise from the use of the devices as a threat vector, in basically the same way that email is used in phishing attacks. Therefore, when the organization is the target, there is a thematic connection between threats to personal medical devices and phishing. With phishing, the goal isn't just to shame the recipient because they were duped into clicking on an email link; the goal is to compromise the organization's information technology infrastructure, even if in a small way, to gain a foothold for later, more involved attacks.

Organizational threats fall into the same two general categories as threats to individuals: adversarial and non-adversarial. Some of the threats have similar vectors, although with different outcomes or goals.

Adversarial Threats and Threat Scenarios:

- Extortion. An attacker uses their knowledge of the patient's medical device and condition to create an existential threat. The attacker uses the threat to force the patient to perform acts against the organization to which the patient belongs, or to perform acts against their own will which cause damage to their well-being.
- Espionage or Reconnaissance. An attacker uses their knowledge of the patient's medical device to learn about the systems of that device, or to gather or infer information about systems that the device encounters as the patient goes about their daily life. The attacker can also seek to steal ("exfiltrate") data from the system under attack.
- Bodily Harm. An attacker uses their knowledge of the patient's condition and medical device to cause harm to the patient.

Non-adversarial Threats and Threat Scenarios:

- Device Misconfiguration. A medical professional inadvertently configures the device so that it operates in an insecure manner or causes harm to the patient. This will result in a loss of organizational productivity until the staff member can return to normal duties. Additionally, the device manufacturer may also configure the device in an insecure manner (for example, its default configuration, or a patch that disables information security safeguards), thus making it easier for the device to be targeted and exploited by an attacker.
- Loss of Support Infrastructure. The device that a key staff member uses is unable to be maintained or repaired, or manufacturer support has ceased. In either case, the staff member may have their ability to function at work severely restricted as they work with

their care provider and insurance provider to find an alternative treatment. This can have a negative affect on organizational function and productivity until the staff member can return to normal duties.

- Interference. The device that a key staff member uses is accidentally damaged, or otherwise made to malfunction due to unanticipated circumstances. Because the patient performs a key function or holds an important role in the organization, the ability of the team, department, or organization to act or function may be impaired.

Trends in PMD Security

For the near future, the trends driving personal medical device security involve growth in usage, privacy concerns, the introduction of new technologies into the marketplace, and the support of forensic investigations.

Many security researchers, and organizations that support security research into medical devices, have stated that additional investigation into the vulnerabilities, potential attacks, and defensive strategies regarding medical devices need more effort. The American Diabetes Association with the European Association for the Study of Diabetes, for example, have issued statements calling for further research and review into non-adversarial and adversarial threats (Heinemann et al., 2015).

Increasing Usage

The trend in personal medical devices points to increasing use of devices both for medical and economic reasons. New applications are being developed from existing medical sensors, such as the FitBit, which can be used by patients with chronic conditions and the general population to

monitor and improve their health. The use of wearable devices is also being encouraged by some health insurance companies as a way to gather data about the people they insure and to encourage healthy living. New technologies, such as CGM sensors and neurostimulators, have been recently approved for treatment of diabetes and tremors, respectively, and these devices have been enthusiastically adopted by patients.

New Technologies

As an example of new technologies entering the market, Continuous Glucose Monitoring (CGM) is continuing to develop and gain acceptance among patients. CGM technology helps diabetics by providing data on how their blood sugar levels change over time and activity, and also provide warnings when blood sugar is too low or too high. One such device, introduced in 2015, connects to iOS devices (Neithercott, 2015). As of the time that this paper was written, there are eight devices on the market that function as either CGM devices or combined CGM device and insulin pump ("Consumer Guide to Continuous Glucose Monitors," 2018) . Because of the convenience of monitoring and increased awareness of health, these devices could become more commonplace in the general market, in much the same way that smart watches have slowly evolved into fitness monitoring devices for professional and serious amateur athletes. An additional push may come from health insurers. The types of devices used for medical monitoring and treatment continues to evolve. In 2017, FitBit gained approval from the National Institutes of Health to use their watch-style fitness monitors as a type of medical device, with the intention of supporting people who are undergoing physical therapy, weight loss, or health improvement program ("Fitbit Selected for National Institutes of Health (NIH) Precision Medicine Research Program with The Scripps Research Institute (TSRI)," n.d.). In a related

action, John Hancock Insurance began offering subsidized Apple Watches to people in its health insurance programs to encourage health-improvement habits (Brown, n.d.).

Neurostimulators are another emerging medical technology used for patients who are being treated for tremors and other neurological disorders. Being built on a similar platform to ICDs, neurostimulators can be attacked in similar ways, and with the result of disrupting the current that the device continuously applies to the patient's brain. Such an attack could immobilize a patient or put their life at risk by stopping voluntary or involuntary muscle actions, or causing brain damage (Marin et al., 2018).

Emerging Privacy Concerns

Another emerging threat comes from the amount of personal health data, and other data, that PMDs can collect. Data is collected from the patient, is stored on the device, and then uploaded to a database or cloud service. Along the way, the data is touched by the device itself, the device that relays data to the caregiver (which can be a patient's personal smart phone) and then is stored somewhere. The potential for a breach of private medical data is significant.

The type of information affected by a breach of personal medical device privacy is also changing. Today's devices reveal the state of a person's health, but devices are being developed now that can reveal a patient's thoughts. Researchers who are examining implantable neurostimulators have discovered that these devices, by tracking the P-300 wave, a type of brain wave that is generated 300ms after a stimulus, can be used in a side-channel attack to "leak sensitive personal information such as passwords... or even reveal emotions and thoughts" (Marin et al., 2018).

Supporting Forensic Investigations

The lack of support for forensic investigations into the misuse of personal medical devices greatly inhibits the efforts of investigators to determine the cause of PMD security issues. As noted in "Digital Investigation of Security Attacks on Cardiac Medical Devices," there are several methods that investigators could use after a suspected attack to determine if an attack occurred and what type of attack. However, is no methodology that exists that describes how this type of investigation would be carried out (Ellouze, Rekhis, Allouche, & Boudriga, 2014). The further development of capabilities to support forensic investigation of medical devices will provide both a deterrent to attack, and the means for investigators to pursue suspects in the event of an attack on a personal medical device.

Conclusion

The three unique qualities of personal medical devices -- the ability to wirelessly connect with other devices outside of a patient's control, the collection of protected health information, and the integral role that the devices play in the health of a patient -- present great challenges to security professionals.

Security professionals need to be aware that the use of personal medical devices is increasing. New therapies, and new technologies, are being developed and approved for use in treating an expanding variety of conditions among all ages of patients. The marketing of wearable devices to the general population, such as the FitBit and Apple Watch as heath tracking devices, is also increasing the percentage of the general population who use personal medical devices.

On the positive side, there is growing recognition that vulnerabilities exist in these devices that must be addressed. Researchers have begun to define and explore the attack surface of PMDs, and their efforts are raising awareness of the lack of security controls. There are also laws in the US that both support research into medical device vulnerabilities and legal action against parties who attempt to illegally exploit the vulnerabilities in these devices.

The combination of sensitive data, weak security, and growing usage of personal medical devices presents a tempting target for attackers. As seen with the tremendous growth of attacks against smart phones, a platform which, like medical devices, combines sensitive data, weak security, and ubiquity, the likelihood of a life-threatening attack on a PMD or IMD will increase over time. The security community must continue to meet the challenge of integrating these devices into the lives of patients and the organizations to which the patients belong.

References

Alexander, N. (2018, January 27). My Pacemaker Is Tracking Me From Inside My Body. Retrieved August 4, 2018, from https://www.theatlantic.com/technology/archive/2018/01/my-pacemaker-is-tracking-me-from-inside-my-body/551681/

Allison, M. G., & Mallemat, H. A. (2015). Emergency Care of Patients with Pacemakers and Defibrillators. Emergency Medicine Clinics, 33(3), 653–667. https://doi.org/10.1016/j.emc.2015.05.001

Alva, A. (2016, October 28). DMCA security research exemption for consumer devices. Retrieved August 9, 2018, from https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices

American Diabetes Association. (n.d.). How Do Insulin Pumps Work? Retrieved August 4, 2018, from http://www.diabetes.org/living-with-diabetes/treatment-and-care/medication/insulin/how-do-insulin-pumps-work.html

Armaganijan, L. V., Toff, W. D., Nielsen, J. C., Andersen, H. R., Connolly, S. J., Ellenbogen, K. A., & Healey, J. S. (n.d.). Are Elderly Patients at Increased Risk of Complications Following Pacemaker Implantation? A Meta-Analysis of Randomized Trials. Pacing and Clinical Electrophysiology, 35(2), 131–134. https://doi.org/10.1111/j.1540-8159.2011.03240.x

Artificial cardiac pacemaker. (2018). In Wikipedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Artificial_cardiac_pacemaker&oldid=853102862

Basu, E. (n.d.). Hacking Insulin Pumps And Other Medical Devices From Black Hat. Retrieved October 29, 2017, from https://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/

Bowman, N. (2018, February 11). 'CGM Lite': The Freestyle Libre! Retrieved August 10, 2018, from https://medium.com/@bowmannancy/abbott-freestyle-libre-d83dd03eb024

Bluetooth Body Sensor Location. (n.d.). Retrieved August 8, 2018, from https://www.bluetooth.com/specifications/gatt/viewer?attributeXmlFile=org.bluetooth.characteristic.body_sensor_location.xml&u=org.bluetooth.characteristic.body_sensor_location.xml

Brown, K. V. (n.d.). When An Insurer Sells You an Apple Watch For $25, How Much Are You Giving Away? Retrieved August 4, 2018, from https://gizmodo.com/when-an-insurer-sells-you-an-apple-watch-for-25-how-m-1819912738

Burns, A. J., Johnson, M., & Honeyman, P. (2016, October). A Brief Chronology of Medical Device Security. Retrieved August 4, 2018, from https://cacm.acm.org/magazines/2016/10/207766-a-brief-chronology-of-medical-device-security/fulltext

Cao, Y., Li, S., & Wijmans, E. (2017). (Cross-)Browser Fingerprinting via OS and Hardware Level Features. Presented at the NDSS Symposium, Internet Society. https://doi.org/10.14722/ndss.2017.23152

Cardiac Resynchronization Therapy (CRT). (2017, October 3). Retrieved August 4, 2018, from https://www.heart.org/HEARTORG/Conditions/HeartFailure/Cardiac-Resynchronization-Therapy_UCM_452920_Article.jsp

CFR - Code of Federal Regulations Title 21. (n.d.). Retrieved August 9, 2018, from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=803

Consumer Guide to Continuous Glucose Monitors. (2018). American Diabetes Association. Retrieved from http://main.diabetes.org/dforg/pdfs/2018/2018-cg-continuous-glucose-monitors.pdf

Curfman, G. D., Morrissey, S., & Drazen, J. M. (2009). The Medical Device Safety Act of 2009. New England Journal of Medicine, 360(15), 1550–1551. https://doi.org/10.1056/NEJMe0902377

Davis, S. (2011, August 10). It Happened to Me: I Got a Pacemaker at 25. Retrieved July 26, 2018, from https://www.xojane.com/it-happened-to-me/it-happened-me-i-got-pacemaker-25

Davis, S. (n.d.). My WebMD: In My 20s With a Pacemaker. Retrieved July 25, 2018, from https://www.webmd.com/heart-disease/features/in-my-20s-with-a-pacemaker#1

Drive, A. D. A. 2451 C., Arlington, S. 900, & Va 22202 1-800-Diabetes. (n.d.). Insulin Pumps Need Greater Safety Review: American Diabetes Association Issues Joint Statement with European Association for the Study of Diabetes. Retrieved August 4, 2018, from http://www.diabetes.org/newsroom/press-releases/2015/insulin-pumps.html

Ellouze, N., Rekhis, S., Allouche, M., & Boudriga, N. (2014). Digital Investigation of Security Attacks on Cardiac Implantable Medical Devices. Electronic Proceedings in Theoretical Computer Science, 165, 15–30. https://doi.org/10.4204/EPTCS.165.2

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies. (2015, October 28). Retrieved August 9, 2018, from https://

www.federalregister.gov/documents/2015/10/28/2015-27212/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control

FCC OET Authorization Search. (n.d.). Retrieved August 5, 2018, from https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm

FCC Search Tools. (2012, April 13). Retrieved August 5, 2018, from https://www.fcc.gov/general/fcc-search-tools

Feldman, A., Kersten, D., Chung, J., Asheld, W., Germano, J., Islam, S., & Cohen, T. (2016, February 8). Gender-Related and Age-Related Differences in Implantable Defibrillator Recipients: Results From the Pacemaker and Implantable Defibrillator Leads Survival Study ("PAIDLESS") [Text]. Retrieved July 25, 2018, from https://www.eplabdigest.com/articles/Gender-Related-and-Age-Related-Differences-Implantable-Defibrillator-Recipients-Results

Fitbit Selected for National Institutes of Health (NIH) Precision Medicine Research Program with The Scripps Research Institute (TSRI). (n.d.). Retrieved August 4, 2018, from https://investor.fitbit.com/press/press-releases/press-release-details/2017/Fitbit-Selected-for-National-Institutes-of-Health-NIH-Precision-Medicine-Research-Program-with-The-Scripps-Research-Institute-TSRI/default.aspx

Giada, F., Bertaglia, E., Reimers, B., & Noventa, D. (2012, April 24). Indications for Implantable Cardiac Monitors. Retrieved August 4, 2018, from http://www.medscape.com/viewarticle/770618

Goldman, J., & Whitehead, S. (2007). Joint Workshop on High Confidence Medical Devices, Software, and Systems (HCMDSS) and Medical Device Plug-and-Play (MD PnP)

Interoperability. Presented at the Joint Workshop on High Confidence Medical Devices, Software, and Systems (HCMDSS) and Medical Device Plug-and Play (MD PnP) Interoperability.

Goodin, D. (2011, August 27). Insulin pump hack delivers fatal dosage over the air. Retrieved August 5, 2018, from https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

Greenspon, A. J., Patel, J. D., Lau, E., Ochoa, J. A., Frisch, D. R., Ho, R. T., … Kurtz, S. M. (2012). Trends in Permanent Pacemaker Implantation in the United States From 1993 to 2009. Journal of the American College of Cardiology, 60(16), 1540–1545. https://doi.org/10.1016/j.jacc.2012.07.017

Halperin, D., Heydt-Benjamin, T., Fu, K., & Maisel, W. (2008). Security and Privacy for Implantable Medical Devices. Pervasive Computing, 7(1), 30–39.

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 (pp. 129–142). IEEE. https://doi.org/10.1109/SP.2008.31

Heinemann, L., Fleming, G. A., Petrie, J. R., Holl, R. W., Bergenstal, R. M., & Peters, A. L. (2015). Insulin Pump Risks and Benefits: A Clinical Appraisal of Pump Safety Standards, Adverse Event Reporting, and Research Needs: A Joint Statement of the European Association for the Study of Diabetes and the American Diabetes Association Diabetes Technology Working Group. Diabetes Care, 38, 716–722. https://doi.org/10.2337/dc15-0168

Herrmann, F., & Aalders, K. (n.d.). Bluetooth Health Device Profile, Part 1. Tritech, Ltd. Retrieved from http://www.tritech.co.il/Editor/assets/HDP%20Article_Stollmann_en_Part1.pdf

Hoskins, M. (2017, February 22). Implantable Insulin Pumps Are Near Extinction, But Still Alive. Retrieved August 4, 2018, from https://www.healthline.com/diabetesmine/implantable-insulin-pumps

IEEE SA - Healthcare IT Standards. (n.d.). Retrieved August 8, 2018, from https://standards.ieee.org/findstds/standard/healthcare_it.html

Implantable Cardioverter Defibrillator (ICD). (n.d.). Retrieved August 4, 2018, from https://www.heart.org/en/health-topics/arrhythmia/prevention--treatment-of-arrhythmia/implantable-cardioverter-defibrillator-icd

Implantable Medical Devices. (n.d.). Retrieved August 4, 2018, from https://www.heart.org/en/health-topics/heart-attack/treatment-of-a-heart-attack/implantable-medical-devices

Insulin pump statistics about adults and children with diabetes. (2018, July 25). Retrieved July 26, 2018, from http://www.insulin-pumpers.org/about.shtml

Integrated Diabetes Services, I. D. (n.d.). Insulin Pump Comparisons. Retrieved August 4, 2018, from http://integrateddiabetes.com/insulin-pump-comparisons/

Interview with Hospital Medical Technologist. (2018, May). [Telephone].

Joint Task Force Transformation Initiative. (2012). Guide for conducting risk assessments (No. NIST SP 800-30r1). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Latuske, R. (n.d.). Bluetooth Health Device Profile and the IEEE 11073 Medical Device Frame Work, 6.

Li, C., Raghunathan, A., & Jha, N. K. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services (pp. 150–156). https://doi.org/10.1109/HEALTH.2011.6026732

Maisel, W. H., Sweeney, M. O., Stevenson, W. G., Ellison, K. E., & Epstein, L. M. (2001). Recalls and safety alerts involving pacemakers and implantable cardioverter-defibrillator generators. JAMA, 286(7), 793–799.

Marin, E., Singelée, D., Yang, B., Volski, V., Vandenbosch, G. A. E., Nuttin, B., & Preneel, B. (2018). Securing Wireless Neurostimulators. In Proceedings of the Eight ACM Conference on Data and Application Security and Privacy (pp. 287–298). Tempe, AZ: ACM Press. https://doi.org/10.1145/3176258.3176310

Medtronic. (2018, January). Introducing Azure with Bluetooth Technology. Medtronic. Retrieved from https://www.medtronic.com/content/dam/medtronic-com/01_crhf/brady/pdfs/201801292-en-p26_web.pdf

Medtronic. (n.d.). Azure pacing system. Retrieved August 5, 2018, from /us-en/healthcare-professionals/products/cardiac-rhythm/pacemakers/azure.html

MiniMed Connect FAQs | Medtronic Diabetes. (n.d.). Retrieved August 5, 2018, from https://www.medtronicdiabetes.com/customer-support/minimed-connect-faqs

Moe, M. (2016, March 14). Go Ahead, Hackers. Break My Heart. Wired. Retrieved from https://www.wired.com/2016/03/go-ahead-hackers-break-heart/

Neithercott, T. (2015, April). Monitor Your Glucose With the Apple Watch. Retrieved August 10, 2018, from http://www.diabetesforecast.org/2015/may-jun/glucose-monitoring.html

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security (No. NIST SP 800-12r1). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1

Nordic Semiconductor. (n.d.). Bluetooth low energy Services, a beginner's tutorial - Bluetooth low energy - Tutorials - Nordic DevZone. Retrieved August 8, 2018, from https://devzone.nordicsemi.com/tutorials/b/bluetooth-low-energy/posts/ble-services-a-beginners-tutorial

Norton, A. (2012, September 26). More Americans getting pacemakers. Reuters. Retrieved from https://www.reuters.com/article/us-more-americans-getting-pacemakers/more-americans-getting-pacemakers-idUSBRE88P1LN20120926

Nykaza, E., Arbiter, B., & Snider, C. (2018, February 15). Let's Talk About Your Insulin Pump Data. Retrieved July 26, 2018, from https://tidepool.org/lets-talk-about-your-insulin-pump-data/

Pacemakers and Implantable Defibrillators. (n.d.). [Text]. Retrieved August 4, 2018, from https://medlineplus.gov/pacemakersandimplantabledefibrillators.html

Prezelj, N., Trošt, M., Georgiev, D., & Flisar, D. (2018). Lightning may pose a danger to patients receiving deep brain stimulation: case report. Journal of Neurosurgery, 1–3. https://doi.org/10.3171/2017.12.JNS172258

Riegel v. Medtronic, Inc., 552 U.S. 312 (2008). (2008). Retrieved August 9, 2018, from https://supreme.justia.com/cases/federal/us/552/312/

Rios, B., & Butts, J. (2017, May 23). Understanding Pacemaker Systems Cybersecurity. Retrieved August 8, 2018, from http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html

Sly, L. (2018, January 29). U.S. soldiers are revealing sensitive and dangerous information by jogging. Retrieved August 8, 2018, from https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html

US Food & Drug Administration. (2016). Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, 30.

Vulnerabilities Identified in Medtronic MyCareLink Heart Monitors. (2018, July 2). Retrieved August 5, 2018, from https://www.hipaajournal.com/vulnerabilities-identified-in-medtronic-mycarelink-heart-monitors/

Werther, J. (2007). A picture I took of my Minimed Medtronic Paradigm 512 insulin pump, showing an infusion set attached to a reservoir. The blue object is a spring-loaded insertion device to insert the metal needle (which is surrounded by a plastic cannula) beneath the skin. The metal needle is then removed, leaving the cannula in place. Retrieved from https://commons.wikimedia.org/wiki/File:Insulin_pump_and_infusion_set.JPG

Williams, P., & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: Evidence and Research, 305. https://doi.org/10.2147/MDER.S50048

Zetter, K. (2014, April 25). It’s Insanely Easy to Hack Hospital Equipment. Retrieved October

29, 2017, from https://www.wired.com/2014/04/hospital-equipment-vulnerable

###