Personal Medical Devices

Ann Funk

East Carolina University

ABSTRACT

Technology in any field has been growing at a rapid pace, but one of the field's that has seen the fastest growth would be that of the medical community. With this fast growth, security management and security of personal medical equipment has become a huge concern, especially with the field of personal medical devices. In this paper we will define what personal medical devices are, as well as discuss some of the threats and challenges that surround them. Some of the biggest threats against personal medical devices will be identified, in addition to, some of the solutions that can help keep these devices safe, not only now but also in the future.

Personal Medical Devices

Starting in 1993, the World Wide Web was made available free of charge. Since that time, technology has blossomed into things that could have only been seen in movies or in our imaginations just a short time ago. Phones with no cords, computers with no keyboards or mice, devices that talk to us and send us reminders. We are now a society that is in tune 24 hours a day, 7 days a week. This growth in technology has touched every facet of our lives, including our health. The healthcare industry has experienced huge growth thanks to technology, especially in the area of personal medical devices. Personal medical devices are now being used in the medical community to provide information to doctors within minutes instead of days or weeks. They are also providing ways for patients to monitor their stats and administer medicine in their own homes. While this technology has helped many people live long, productive lives, we need to ask questions about it the same as we do of all technology we use. How safe is it? Can anything be done to make it more safe?

Before we can begin to answer these questions, we need to talk a little bit about what personal medical devices are and how they are used. Apurva Mohan (2014) describes a personal medical device as a medical device that is attached to a patient and serves the critical function of providing automated lifesaving assistance continuously. These medical devices can be implanted in the patient's body, or attached to the patient in an external manner. These devices can be something as simple as a Glucometer or Blood Pressure Monitor, that the patient will use at his leisure to track blood pressure and glucose levels, to something more advanced, such as insulin pumps, cardiac pacemakers/defibrillators, and portable intravenous medication devices.

These types of personal medical devices will be implanted under the skin or attached to the patient by a doctor.

Once implanted, the doctor or technician will be able to configure the devices using customized software and a commercial programmer specifically designed for each device. This process can be done using wireless communication standards such as Bluetooth, radio-frequency (RF) signals, Wireless Medical Telemetry Services (WMTS), Medical Implant Communication System (MICS), and Near Field Communication (NFC). Not only can these devices be configured wirelessly, but they can also upload any data that has been collected about the patient wirelessly as well. These transmissions can be completed by the medical device itself, or a cradle that the medical device can communicate with or attach itself to. The reader or cradle will collect the information from the device and then transmit the collected information over the internet. While this is both incredible efficient for both doctor and patient, it does not come without risks. A new age of patient comfort (quality of life), treatment efficacy, and efficiency through increased software control and electronic interconnectivity also brings many challenges, a major one of which is security (Ray, Jones, & Zhhang, 2013).

One of the threats with any device that connects to the internet is that of personal information being stolen and sold to the highest bidder. We all know that credit card information has been bought and sold for years but now it seems that personal health information is now worth much more on the black market. In fact, the value of a patient health record in the black market is estimated to be $50, compared to $3 for a social security number, and $1.50 for a credit card (Altawy, & Youssef, 2016). One of the reasons this is something that anyone with a personal medical device needs to think about, is the fact that personal medical devices sometimes have no authentication mechanisms. This means if a person has obtained a commercial

programmer they can hack into the device and illegally obtain any private information that is stored on this device. This information will most likely have the person's name, date of birth, social security number, and any and all health information about the patient that is stored on the device.

Another threat that can happen when using a personal medical device is that of impersonation. This type of attack usually occurs when the wireless channel the device is using, is not properly protected. With this type of attack, a hacker can imitate either a commercial programmer or an actual device, listen in on legitimate communications, to gather and record the genuine handshake reply of the personal medical device to the programmer. With this information an attacker can impersonate any medical device that uses this handshake. They will now have access to much more information but from many different patients. Not only will they be able to get information, but they will also be able to provide false information to the system. Doctors will now have wrong information that could delay treatments that patients need, in some cases these delays could endanger a person's life and even become fatal.

Relaying attacks are another threat that happens to personal medical devices. Personal medical devices that use Medical Implant Communication Systems or Wireless Medical Telemetry Services only have a communications range of about 2 meters. This means the programmer needs to be quite close in order to connect with the device. With a relaying attack, the attacker can trick the device by convincing the personal medical device that the programmer is within proximity of the device. It does this by using a device called a ghost and another device called a leech. Both of these devices supports fast long range communication. In this setting, the ghost impersonates the personal medical device to a genuine programmer, and the leech pretends to be the programmer to the personal medical device. In proximity-based authentication

protocols, the leach and ghost keep relaying the messages between the two devices to trick the personal medical device into believing that it is talking to an authorized programmer (Altawy, & Youssef, 2016).

The last major threat for personal medical devices that will be discussed in this paper is one that almost every computer technician has heard of, Denial-of-Service (DOS) attacks. A DOS attack works pretty much the same way for a personal medical device as it would for any computer or website. Attackers can simply jam the communication channel between the medical devices, causing incorrect operation (Burleson & Carrara, 2014). Besides jamming the communication between the personal medical device and the programmer, an attacker may try to request a task from the personal medical device that requires the use of a great deal of power. This will cause a massive power drain to the system making it almost impossible for it to perform any other tasks. Just like in other systems, a DOS attack of a personal medical device is easily identifiable by the patient and in most cases, can quickly be handled.

Even though there are many similarities in the threats that face both computer systems networks and personal medical devices, they don't always face the same challenges. Personal medical devices are created and used in such unique ways that it causes them to have their own unique challenges. And the unique challenges they face require different kinds of techniques to protect them from these threats are not always the same as a computer system. In the case of personal medical devices that are implanted under the skin, there are several issues that make things much more challenging. One of these challenges is that of physical environment. Since some of the devices are actually implanted in the human body and come in contact with vital tissues, it is imperative that they be made of materials that do not react to their environments.

These devices also need to be small and light weight so that they become as unobtrusive as possible to the patient.

Constrained resources are another challenge that is faced by personal medical devices. Since most personal medical devices are quite small and implanted under the skin, they are equipped with a non-rechargeable battery that is supposed to last between 5 to 15 years. This means that every process that the device is asked to do affects this power source and depending on the complexity, these can lead to a loss of life to the device. With these constraints it becomes almost impossible to implement cryptographic techniques. In other words, a typical authentication protocol to control who is granted the right to access the personal medical device requires multiple executions of a symmetric encryption algorithm, a public key algorithm (usually adopted in key distribution via public key infrastructure), and sometimes a hash function, all of which if implemented, require high processing power which will deplete the battery much sooner than its expected lifetime (Altawy & Youssef, 2016). If there is a loss of life to the device, the device will have to be surgically removed and replaced with a new device. So the power restraint on the battery is a huge concern.

Whenever any changes are discussed in securing personal medical devices, the topic of backward or legacy compatibility is one of the top challenges that must be overcome. As we mentioned before these devices have a life span between 5 and 15 years and any changes need to take into consideration the battery life as well as the age of the processor chips that may be used in old devices. If a chip is too old and the new and improved software has not taken that into consideration it could render the device useless making it unable to do its job and putting the patient's life at risk.

An additional challenge with personal medical devices is that of bureaucracy. As with most things in the medical industry, there are many rules and guidelines not only in how to use a device, but also on what things can and can't be changed about a device. The field of personal medical devices are no different. In fact, whenever a change is made in a security mechanism, it must go through a set of quality control testing by various regulatory bodies before it can be approved. In the United States, changes to the devices also need to meet criteria set up by that regulatory body that is known as the Food and Drug Administration or (FDA) (Hyman, 2012). On one hand this is good that changes are being tested and tracked, on the other hand it can take up to 7 years for the FDA to approve any changes. When new technology is being created every day, the changes being requested could be obsolete by the time the FDA gets around to approving them.

The last challenge I will talk about with personal medical devices is that of emergency authentication. Whenever a medical device has been implanted into a patient, there needs to be a way for healthcare professionals to gain access. So that no matter where the patient is in the world, if an emergency occurs, and the patient is unresponsive, a health care professional will be able to shut the device down if it is causing problems or access the device to gather personal, lifesaving information about the patient. This can be done if there is a backdoor installed into the system or if one account is created for all devices that has the same password. Both of these put the devices at risk since backdoors are widely used by hackers to gain control of computers and a standard, default account that uses the same password is just an invitation for anyone access the devices.

Now that we have spoken about some of the challenges and threats to personal medical devices, it is time to turn our attention to some of the things that are being done to solve these

issues. Many personal medical device designers and technicians feel that when trying to secure the device itself, they have to look for software-based technologies. They feel a good place to start is to monitor the devices system behavior on a daily basis. When this behavior does something that does not follow the normal pattern, there will be software that will not allow the behavior to continue and actually shut down that behavior. Another security system that they feel could be in place is one that will verify the boot and software of the device by comparing system resources and any files that are executable to a given standard. This could potentially protect the device from unwanted changes caused by a hacker.

One of the main things that is being used to solve some of the issues with personal medical devices deals is that of encryption. There is a strong belief that the use of cryptography should be used judiciously in the design and deployment of personal medical devices when they deal with the storage or transmission of sensitive data. The goals of data encryption and device authorization are relatively well defined, but choosing appropriate ciphers, cipher modes, and authentication protocols is a top priority (Burleson & Carrara, 2014). In fact, in 2013, the Food and Drug Administration issued recommendations that include the use of encryption and authentication for wireless personal medical devices to secure the devices against unwarranted attacks and users. One company has taken this guideline to a whole new level by using a method that actually encrypts the patient's heartbeat. In this scenario, a heartbeat reading will be taken from the patient with a special device. Then the special device will take that reading and compare it to the one that is being transmitted by the personal medical device that is implanted into the patient. The data being transmitted by the personal medical device will of course be encrypted, thwarting any attempt by a hacker of hijacking the data.

Personal medical devices currently face many different threats that are way more complicated than most any other computer issue. Programmers, designers, makers and security technicians not only have to deal with the threat of data being leaked through these devices, they also to deal with threats that could cost a person their life. That is why it is extremely important for all sides to work together and integrate security into these devices starting with product development all the way to the lifecycle of the device. In this paper we have discussed a lot of the threats and challenges that they will have to overcome to secure these devices. We have also documented a few ways in which they are working to fix these issues. If all parties work together, it will create a safer, more cohesive environment for personal medical devices to flourish in the future.

References

*Altawy, R., & Youssef, A. M. (2016). Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access, 4*, 959-979. doi:10.1109/ACCESS.2016.2521727

Burleson, W. (. P.)., & Carrara, S. (2014;2013;). *Security and privacy for implantable medical devices* (2013;1;2014; ed.). New York: Springer. doi:10.1007/978-1-4614-1674-6

Cryptography. (n.d.). In Wikipedia online. Retrieved July 12, 2016, from https://en.wikipedia.org/wiki/Cryptography

Fan, J., Reparaz, O., Rožić, V., & Verbauwhede, I. (2013). Low-energy encryption for medical devices: Security adds an extra design dimension. Paper presented at the 1-6. doi:10.1145/2463209.2488752

*Hyman, W. A. (2012). The integrating the healthcare environment - PCD - MEM medical device cyber security white paper: An overview. *Journal of Clinical Engineering, 37*(1), 24.

Katzis, K., Jones, R. W., & Despotou, G. (2016). The challenges of balancing safety and security in implantable medical devices. *Studies in Health Technology and Informatics, 226*, 25.

*Mohan, A. (2014). Cyber security for personal medical devices internet of things. Paper presented at the 372-374. doi:10.1109/DCOSS.2014.49

Ray, A., Jones, P., & Zhang, Y. (2013). Medical device security-A new frontier. *Biomedical Instrumentation & Technology, 47*(1), 72.

Tech Timeline: A Brief History of the Information Technology Industry - VincentBenjamin. (2015, July 23). Retrieved July 12, 2016, from http://vincentbenjamin.com/tech-timeline-a-brief-history-of-the-information-technology-industry/

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices (Auckland, N.Z.)*, *8*, 305.