International Journal of Innovative Studies in Sciences and Engineering Technology (IJISSET)

ISSN 2455-4863 (Online) www.ijisset.org *Volume: 2 Issue: 8 | August 2016*

Pacemakers: A Survey on Development History, Cyber-Security Threats and Countermeasures

Paul Boulos, Arman Sargolzaei, Armin Ziaei, and Saman Sargolzaei[1]

[1]Rancs Group LLC, USA

Abstract: *The vital role of pacemakers justifies the its safety amongst top priorities at the current age of cyber security. The aim of the study is to survey the history of pacemakers development through the decades and the current standing of cyber-security malfunctions, threats and potential countermeasures in such devices to prevent and control the issues.*

1. INTRODUCTION

600,000 pacemakers are implanted into patients' heart every year, adding to the current total of around 3 million units. Pacemakers play a huge role in the lives of the patients that they are implanted into, as the pacemakers helps keep the rhythm of the heart in check [1-4]. Without pacemakers, patients with irregular heartbeats or heart problems would be at a severe risk which could result in fatal incidents. Modern day pacemakers consist of 4 parts, being the battery, the leads, the motherboard, and the casing itself. They weigh less than an ounce, are slightly larger than the face of a wristwatch, and have the ability to monitor the heart's natural electrical activity [6-8]. The battery used in modern day pace makers is a lithium/iodine cell battery, which has the power that energize the pacemaker for around 5-7 years [9]. The leads are wires that consist of a metal alloy, which is treated with a polymeric insulator and then fitted to the device itself. The motherboard contains all the circuitry of the device, which consists of the connection between the battery, the pulse generator, the a trial sensor, the ventricular sensor, the leads, and the various transistors in the device. All of this is cased within a titanium, or titanium-alloy, case, so to be safe while inside the body, and not deteriorate in any way.

The main goal of a pacemaker is to monitor and to help control abnormal heart rhythms in the patients they are usually implanted into. They are usually implanted into patients who have heart problems or undergo abnormal pacing patterns with their heart. There are three different kinds of pacemakers, which are Single-Chamber, Dual- Chamber, and Bi-ventricular pacemakers [8]. A single chamber pacemaker is a pacemaker that only has one lead, which is placed in the rather the right atrium or the right ventricle in the heart. It is the most basic kind of pacemaker, closest resembles the Elema 135 Pacemaker, which was the first implantable pacemaker. A dual chamber pacemaker is a pacemaker that has two leads, which are located in both the right atrium and right ventricle in the heart. Having both leads gives the pacemaker a bit more control of the heart, as it has control of both the upper and the lower parts of the heart and, as a result, more closer resembles the natural pacing of the heart. The Bi-ventricular pacemaker is a pacemaker that has three leads, which are located in the right atrium, right ventricle, and left ventricle of the heart. With leads in both ventricles, it allows the pacemaker to resynchronize the contraction of the heart, giving full control over the heart. It is used in patients who have a weak heart due to heart attacks, and other complications. Regardless of the type of pacemaker, they are all implanted the same way, which is through a small surgery [1,4]. This surgery requires a small incision beneath the collarbone of the patient to be made, in order for the leads to be inserted into the patient. After the incision is made, the leads of the pacemaker are sent through the subclavian vein down to the heart, where they are then placed in the location of the heart where the pacemaker is designed for. After the leads have been inserted, a small pouch is then created under the collarbone of the patient and the pulse generator of the pacemaker is placed into the pouch then sewn into the patient.

Researchers and scientists are continuously working towards improving pacemakers over the past seven decades, making the device more and more accessible, comfortable and user-friendly. A very small malfunction in the pacemaker operation can mean the difference between life and death for a patient. One main issue with the current age of pacemaker development is that they are susceptible to being interfered with or being hacked into. This is due to the fact that up until recently, there has been little or no research going towards the cyber-security of the

pacemakers. When pacemakers were first created and up until now, the cyber-security of a pacemaker was never taken into consideration as it was never a concern that someone would want to break into a medical device such as a pacemaker. With malfunctions [9,10] and cyber-attacks to pacemakers being potentially fatal to the patient, this justifies the importance of cyber-security research and development in pacemakers.

The aim of current research paper is to survey the possibility of cyber-attacks toward pacemakers. The survey was performed by first looking into the developmental phases of pacemakers since pacemakers were first a concept all the way up until the recent modern models of pacemakers. Milestones in the pacemaker designs were highlighted. According to the current technological standings, potential areas of malfunctions [11-14] or cyber-threats [15-19] were surveyed and finally existing solutions as a countermeasure to the threat were analyzed.

2. PACEMAKER HISTORICAL DEVELOPMENT

Throughout the years, advancements have been made in pacemaker technology improving different aspects, ranging from battery life enhancement and user-friendliness to most recent wireless communication capabilities. Below is a break down, by decade, of the pacemaker historical developments.

A. 1940's

Created by John Hopps in 1949, the initial design for an artificial pacemaker was an external bulky device using vacuum tubes to generate electrical pulses. The pulses were transmitted through the jugular vein into the heart inducing artificial paces. Being an external device and the need for power outlet limited its portability.

B. 1950's

Smaller size and being mercury battery powered were amongst the features of a portable pacemaker developed by Earl Bakken in 1957. Major improvement on Earl's developed pacemaker made by Ake Senning and Rune Elmqvist in 1958 down scaled the size and resulted in the first implantable pacemaker. The built-in mercury battery was rechargeable via an antenna once a week for about 12 hours. Being lead-based and its inability to resist the repetitive bending were among the limitations of first implantable device.

C. 1960's

The 1960's was a relatively quiet decade for the development of pacemakers. Variations from Elema-135 model, Elema-137 and E142, created by Rune Elmqvist, were introduced. The main difference between the two is that instead of the nickel-cadmium cells that the 135 model used, the 137 and 142 models use zinc-mercury oxide cells, which eliminated the need for the periodic recharging that the nickel-cadmium batteries required. Two other models created at this decade were the Zoll model (1961) and the Kantrowitz model (1962). They bear similarities to the aforementioned Elema models, but had some aesthetic differences.

D. 1970's

The 1970's included key innovations, including the establishment of power source, as well as inclusion of telemetry link. In 1972, a radioisotope pacemaker was created where the device was powered by nuclear energy (Plutonium-238). Triple-layer titanium casing was added to prevent the user from undergoing radiation. The power was expected to last for 20 years, but fell out of favor due to the extensive regulatory maintenance paperwork. Lithium batteries, being effective and long lasting source, came to be used in pacemakers. In the mid 1970's, a radio-frequency telemetry link was created to allow pacemaker parameters to be adjustable to follow the changing clinical needs. Dualchamber pacemakers were invented in the late 1970's.

E. 1980's

First advancement was the creation of first implantable cardioverter-defibrillator (ICD). ICD works very similar to pacemaker, in that they sense and regulate the pace of the heart. However, it also holds the capability to send a more powerful shock, known as a defibrillation, to the heart, in an attempt to get it to pace regularly. Development of steroideluting leads, which decreases the inflammatory response evoked by the lead when placed in the heart allowing more comfort to the user happened during at this time. Rate response pacemakers, developed in mid-1980's, equipped with sensors to detect body movement (a measure of activity), which would then be utilized to alter pacing up or down.

F. 1990's

The 1990's was another quiet decade, although there was one major innovation, the implementation of a microprocessor into the pacemaker. Microprocessor driven pacemakers were capable of detecting and storing events. They could then deliver therapy and modified internal pacing parameters according to the changing needs of the patients in an automatic fashion.

G. 2000's

In the 2000's, two major advancements in pacemakers came to be. The first was the development of bi-ventricular pacemakers. These included the traditional leads to the right atrium and ventricle, as well as a specifically-designed lead, which was introduced via the coronary sinus, to the left ventricle, allowing left and right ventricles to be paced simultaneously for resynchronize contraction. The second major advancement was that pacemakers could upload data telephonically to a central server, via the internet. This allows the heart to be monitored by doctors, without actually being with the patient.

H. 2010's

One major downside to modern day pacemakers is the leads that they use, and their susceptibility to deterioration. Solutions to this include the development of a wireless cardiac stimulation device, using ultrasound to stimulate a receiver in the heart, allowing wireless pacing. Another solution includes the same wireless receiver in the heart, but instead using magnetic fields instead of ultrasound. The issue with modern day pacemakers is the lack of encryption in pacemaker's micro-processor, which leads to complications with interference, as well as its ability to be hacked into. In the lights of advancements to the pacemaker over the last 60 years, there is still development going towards them, in an attempt to make them more accessible, user-friendly and secured.

3. PACEMAKERS CYBER-ATTACKS

A. Problems with Current Pacemakers

Today's pacemakers are equipped with an embedded microprocessor. Variety of sensing and acting tasks, ranging from identifying the required shock signal to be applied t are performed under its control. This microprocessor is where all of the processes are in pacemaker are done, from determining the shock to send to the heart, all the way to acquiring measurements from the heart and providing it to patients and medical care providers. This computer is accessible for the patient and care provider via a remote interface or a computer that connects to the pacemaker itself through a 'backdoor' to monitor heart activity and control pace pattern. Like any other remote device technology, 'backdoor' is not immune to be penetrated into, for good or for bad reasons. This is evident with the amount of computer hackers there are around the world, breaking into computers and databases every day, and in this case, a pacemaker is not different from the rest. When broken into, these pacemakers can undergo a few type of attacks, which can include a strong shock being sent to the patient, disturb the hearts functions, as well as stopping the pacemaker from proper functioning altogether, neglecting any potential issues in the pacemaker itself.

With computers and databases, there is usually an encryption that prevents the device from being accessed, denying access to any other than verified devices. However, when it comes to pacemakers, they are lacking in a couple departments, the first being this encryption. The 'backdoor' that is in the pacemaker is there to serve a special purpose, and that is to allow accessibility to the pacemaker, if something needed to be done to it. This wireless connection is convenient as without it, the patient would have to be cut open in order to apply changes or monitor parameters, which would just be both inconvenient and costly. However, the problem that arises with this, is that since it is a direct opening to the pacemaker's functions, it would need to heavily be encrypted to prevent any unverified device from accessing it, and this is where the pacemaker is lacking in security.

Current pacemakers, even modern day ones, are made with very little to no encryption leaving their 'backdoor' very susceptible to being broken into. Barnaby Jack, director of embedded device security for the computer security firm IO Active, worked towards this kind of cyber-medical attack research and was able to develop a system [18]. The system is able to remotely send a shock to any pacemaker within a 50-foot radius, as well as break into other medical devices such as insulin pumps, and this can all be done wirelessly without requiring any identification numbers or any other type of security verification. The system was built based upon a process of reverse-engineering and fining several flaws in the devices structure. With the amount of hackers that a prevalent in the world right now, it wouldn't be that uncommon for someone with a few skill set to be able to break into a pacemaker, not to mention all of the medical engineers that also possess this ability. This makes the chances of actually getting hacked much higher than just a rare anomaly, but a threatening possibility.

Having access to a pacemaker for malefic purposes not only can be threatening to a patient life, but instead of harming the patient, the hacker could also use the pacemaker as a gateway to access to patients medical records, which could contain even more valuable

information. Added to that, not only is the backdoor the only way into the pacemaker, but also the pacemakers themselves can be implanted with compromised software, which could result in the same security breach. The reason is hospitals rarely update their operating software to be equipped with the most recent anti breach tools, in order to follow FDA regulations, and this out of- date software causes them to be affected by potential malware. Malware entrance to on unit of the whole system serves a huge threat as it can infest the machines and devices utilized in the hospital and therefore penetrating into the implanted devices of the patients and compromise those devices. These two huge faults in the security of these medical devices can very well lead to life threatening situations, as well as private information being compromised.

B. Solutions and Revisions

Jammer

The first of the proposed security measures would be utilizing a jammer in the pacemaker. This type of device is used in many different other scanning devices, such as radar systems. The way that it works is that when an unverified signal is being sent to the pacemaker, the internal computer recognizes it as a bad signal and uses this jammer to try and break apart the signal, neutralizing the threat. The issue with this type of solution though, is that the pacemaker itself has to make sure to only neutralize malefic signals, and not the ones from an actual care provider or verified user, especially at the times of emergency.

Firewall

The other solution to control and prevent hackers from getting into the pacemaker is to implement and strengthen a firewall or encryption into the device. This is the more software-focused solution, and it is used in many, if not all, computers and other devices that access the internet, in order to keep them safe from hackers and other viruses. It is based around creating a wall that prevents signals from unverified devices from entering into the pacemaker. Figure 1 describes the principles of Jammer and Firewall operations. A request to send data is sent to the device and they are accepted and sent if they follow a set of predetermined handshaking rules, or denied if otherwise. In the case of pacemakers, a doctor would pre-set these firewalls to allow medical devices and verified hospitals to be able to connect to pacemakers and give them the ability to get through these firewalls, but still block off unverified requests.

Password Lock

A third solution for control and prevent cyber-attacks would be a password lock onto the pacemaker, allowing access to only those who know it. This is the most practical solution to control and prevent unverified outside accesses from breaking into the pacemaker. However the main problem with this type of security is that it if only the patient knows the password, then it would cause an issue if they were to have to go into surgery or being in an emergency situation, and the doctor wouldn't be able to access it because the patient is unconscious and unable to unlock the pacemaker. A few modern day pacemakers have passwords on them, however, for accessibility in emergencies, the passwords themselves are writing on the outside of the devices themselves, which is also accessible by the hackers.

4. CONCLUSION

The aim of this research was to survey the development history of pacemakers as well as discussing the possibility of cyber attacks towards medical devices, more specifically pacemakers. The ubiquity of pacemakers brings forth an alarming threat of being hacked, which could result in the death of those who use them.

Understanding the history of pacemakers and all of the developments up to now allows us to understand the importance of the device that is in question here. Recently, the threat of hacking into pacemakers has become more of a possibility than ever before thought, and has struck fear into both patients and doctors alike. The result of these attacks can be anywhere from minor health attacks, to a fatal manipulation, with very few solutions. It is solutions to these issues that are being worked to today, but up until now, there

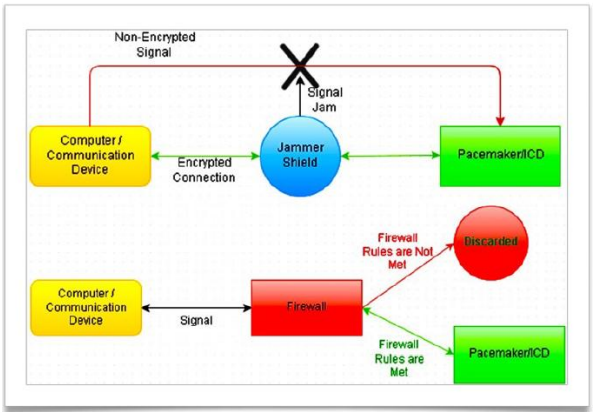

Figure 1: *Diagram describing the principles of Jammer (top) and Firewall (bottom) operation.*

is very little put forward to prevent these cyber-attack issues, as well as even some common malfunctions in pacemakers.

ACKNOWLEDGMENT

The authors wish to acknowledge the support from Rancs Group LLC.

REFERENCES

[1] Shea, Julie B. "Pacemaker Insertion and Long-term Follow-up." *Brigham and Women's*. Brigham and Women's Hospital, 18 Sept. 2015.

[2] Chan, Vivian. "Engineering Heartbeats: The Evolution of Artificial Pacemakers." *Illumin*. University of Southern California, 6 May 2013.

[3] "Pacemaker." How Products Are Made. 1998. *Encyclopedia.com.* 5 Oct. 2015.

[4] "Heart Pacemaker Surgery: Procedure, After Surgery, & More." *WebMD*. WebMD, n.d. Web.

[5] Mohee, By Kevin. "Cardiac Pacing: A Brief History in the Development of Pacemakers."

[6] Mittal, Tarun. "Pacemakers—A journey through the years." *Indian Journal of Thoracic and Cardiovascular Surgery* 21.3 (2005): 236-249.

[7] Aquilina, O. "A brief history of cardiac pacing." *Images in paediatric cardiology* 8.2 (2006): 17.

[8] Mallela, Venkateswara Sarma, V. Ilankumaran, and N. Srinivasa Rao. "Trends in cardiac pacemaker batteries." *Indian pacing and electrophysiology journal* 4.4 (2004): 201.

[9] Mittal, Tarun. "Pacemakers—A journey through the years." *Indian Journal of Thoracic and Cardiovascular Surgery* 21.3 (2005): 236-249.

[10] Schultz, Daniel G. "Possible Malfunction of Electronic Medical Devices Caused by Computed Tomography (CT) Scanning." *FDA Preliminary Public Health Notification: Possible Malfunction of Electronic Medical Devices Caused by Computed Tomography (CT) Scanning*. U.S. Food and Drug Administration, 14 July 2008.

[11] Ortega, Daniel F., et al. "Runaway pacemaker: A forgotten phenomenon?." *Europace* 7.6 (2005): 592-597.

[12] Burns, Edward. "Pacemaker Malfunction - Life in the Fast Lane ECG Library." *Life in the Fast Lane Medical Blog*. N.p., n.d. Web.

[13] Gul, Enes Elvin, and Mehmet Kayrak. *Common pacemaker problems: lead and pocket complications*. INTECH Open Access Publisher

[14] Burns, Edward. "Pacemaker Malfunction" - Life in the Fast Lane ECG Library." *Life in the Fast Lane Medical Blog*. N.p., n.d. Web.

[15] Cherry, Steven. "Hacking Pacemakers." *IEEE Spectrum*. IEEE, 30 Apr. 2013. Web. 16 Nov. 2015.

[16] Carr, David F. "Hackers Outsmart Pacemakers." *InformationWeek*. Healthcare, 12 Dec. 2013. Web. 16 Nov. 2015.

[17] Sutter, John D. "Scientists Work to Keep Hackers out of Implanted Medical Devices." *CNN*. Cable News Network, 16 Apr. 2010. Web. 16 Nov. 2015.

[18] Alexander, William. "Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode." *VICE*. N.p., 25 June 2013. Web. 16 Nov. 2015.

[19] Talbot, David. "How to Prevent Medical Device Attacks." *MIT Technology Review*. N.p., 16 Sept. 2013. Web. 16 Nov. 2015.