Daniel Navon

Comp 116

14 December 2016

The Security of Medical Devices: How and Why Poor Security Puts People's Lives In Danger

Abstract

It seems as if every day the Internet of Things breaks into another aspect of daily life, providing a sense of futurism that both comforts and astonishes. But as these devices become introduced into our daily lives, the vulnerabilities they bear begin to invade our lives. Where previously the draconian answer of turning off your computer provided the paranoid among us with a sense of safety, now the exposed wire of an interconnect world effects our daily lives. Medical applications and devices have now begun to play a central role in this as the internet of things becomes a literal part of our body. Implants and devices such as pacemakers pose a potential vector of attack for those with malicious intent. This essay will discuss the security risk that these devices hold as well as the reasons for these vulnerabilities. It will also examine possible vectors of attack and the factors that can be used to defend from such attacks on medical devices.

Introduction

The internet of things has become a signifier of modern live, with internet connected devices all around us. One of the largest progresses of the Internet of things, is the field of medical devices (Lars). This has turned the internet of things, to an Internet of People. However, instead of people being relying on laptops and computers, the Internet of People relies on the stability of the many medical devices that keep people alive. There is a proven danger with IoT devices; however, the danger of medical devices has yet to be brought to public attention. Medical devices are provably vulnerable to cyber attacks, and there are reasons to fear that such attacks are eminent.

To the Community

Any device connected to the internet is guaranteed to receive some attempt to access the device. Early this October, the Atlantic demonstrate this by building a fake "internet toaster" as a honeypot for such attack. The article, titled, the Inevitability of Being Hacked, demonstrated that "anyone hooking up a poorly secured IP device to the internet can expect to see that gizmo hacked within a week, if not much sooner" (McGill).

Medical devices are no exception to this rule. Earlier this year, a company called MedSec claim that they were able to attack St. Jude heart devices. This claim was challenged by St. Jude's to be finically motivated, however, a third-party security firm

confirmed these claims. The firm, Bishop Fox, demonstrated a capability to perform successful attacks on the devices from up to 100 feet away, interrupt normal function, and even force a patient into cardiac arrest. Though the medical implants were not directly connected to the internet, they communicate with other devices over RF. People with the STJ implants use the Merlin@Home device to communicate with their implants. Attackers can purchase such a device easily on site like ebay, and use them to interface with implants due to their "easily exploitable vulnerabilities" (Muddy Waters Capital). STJ decided to recall the implants, but the level of negligence demonstrated STJ hints at a larger problem.

Indeed STJ's implants are not the only medical device shown to be vulnerable to attacks. Jim Finkle of Reuters writes, "The U.S. Department of Homeland Security is investigating about two dozen cases of suspected cybersecurity flaws in medical devices and hospital equipment that officials fear could be exploited by hackers." Jerome Radcliffe reverse engineered his own insulin pump to expose such a cybersecurity flaw. Using an Arduino and a $20 Wireless chip off ebay, Radcliffe reverse engineered the communication system between his insulin pump and glucose monitor. He found that the easily accessible JAR file used to construct and transmit messages between the devices and discovered the complete source to the message encoding had not been obfuscated. He writes, "Being able to view these library files, it was trivial to reproduce not only the encoding method, but all of the message formats and command codes for the device" (Radcliffe). The most dangerous potential attack of such an exploit would be altering the configuring settings of the device causing the insulin

pump to administer harmful amounts of insulin. Like the STJ implant exploit, an attacker could only attack from a short physical range of 100-200 feet due to the limits of RF technology. However, an attacker could place a device in proximity to such a person that has a remote connection with an attacker at a distance.

To a layperson, attacks such as these might seem frightening but unlikely. Few people believe that they will be the target of a cyber attack. History has shown, however, that mass hacking attempts are significantly more likely than targeted cyber attacks. Though many of these exploitable devices communicate through RF channels, an exploit into their interface can be extended to the web. Furthermore, many devices do connect directly to the internet and pose a massive threat to their users.

For example, the DDoS attack on the DNS provider Dyn relied on the use of IoT devices such as security cameras. These devices were accessed through mass scanning and bonnets that enabled the take down of many popular sites that relied on Dyn for service. Honeypots, such as the aforementioned one created by the Atlantic, have shown that attacks such as this DDoS depend on access connected devices. Even in the more likely scenario that such an attack does not breach an internet connected medical device, the attempt could interfere with the devices normal function. Invalid authentication attempts could look users out of devices and, if an attacker does gain access to the system, attempts to run malicious code could tamper with the normal function of these devices.

Moreover, the increase in ransomware attacks demonstrates that harmful attackers will target non-public figures and corporations. Ransomware denotes a

category of attacks in which takers encrypt the personal data of victims and hold the encryption key ransom. According to Osterman research, almost half of all organizations surveyed has experienced a ransomware attack (Jones Coughlin). Ransomware as a service has become a huge industry were these malicious programs are sold to exploit normal citizens for cash. Considering the prevalence of internet connected medical devices, and ransomware itself, it seems likely that ransomware coulda appear on medical devices.

Instead of holding photos and work files hostage, attackers could hold private medical information hostage for public figures. Black hat hacking groups could utilize these already existing tools to threaten the release of sensitive medical information of public figures for financial or political gain. Even more frightening, a modified version of ransomware could be placed onto vulnerable implanted medical devices, such as the ones previously described, that would threaten to kill or harm the hostage if they did not pay out. It may seem unlikely that such a situation would occur, but the technology to do so exists. In fact, an internet connected medical device could even have normal ransomware loaded by malware through weak credentials or open ports. If the encryption of the devices files could severely affect its ability to function and communicate with other devices, while a victim would not be able to even pay off the ransom to alleviate the problem.

One most also consider the implications this has in connection with cyber terrorism. Should a terrorist group or state power with malicious intent gain access to these devices, a mass death situation could occur. Instead of mass shootings or

bombings, an attacker could walk through a crowd with an RF devices to send every person with a pacemaker into cardiac arrest. Luckily, the offending STJ products were recalled, but we cannot know if more insecure devices exist.

Action Items

The only way to stop such attacks from happening is to increase public knowledge, accountability, and regulation of the security concerns of medical devices. According to the official FDA website, "The FDA is not aware of any patient injuries or deaths associated with cybersecurity incidents, nor are we aware that any specific devices or systems in clinical use have been purposely targeted." The FDA has released multiple guidances documenting their suggestions for safe practices. However, according to the FDA website, "Guidance documents represent the Agency's current thinking on a particular subject. They do not create or confer any rights for or on any person and do not operate to bind FDA or the public." In other words, the FDA does not hold organizations accountable to a standard of cybersecurity (FDA). For patients to be properly aided by there medical devices, they must have some semblance of a guarantee that these devices are secure and regulated. Legislation must be passed that holds device manufacturers accountable to security standards. This legislation should include a mandatory review of all medical devices with a security audit by an independent party.

Another side to this legislation is the legalization of security research. People have a right to know about the code that's inside of them. Recently, lawmakers temporarily excused a section of the DCMA that prevented reverse engineering on copyrighted devices for a two year trail period to benefit security research (Greenberg). While this represents a step in the right direction, many people still avoid exposing vulnerabilities due to fear of retribution. Good samaritan laws should be enacted to permanently protect those provably trying to secure systems by exposing vulnerabilities.

The next step, is education. The general public must be made aware of the dangers posed by the vulnerabilities of these devices. Increasing public awareness in these fields is the most important factor in ensuring the future security of medical devices.

Until people are educated on the dangerous that these vulnerabilities pose to their livelihood, security will continue to take a back seat. If people do not become aware of these threats soon, they might only learn about them after a serious attack has been made.

Conclusion

Medical devices have been pushing the forefront of the Internet of Things, and, while they may benefit consumers in some areas, these devices pose a serious risk to their users. Security experts have already shown that devices such as pacemakers and

insulin pumps can be hacked. The vulnerability of these devices also demonstrates a lack of proper regulation of the cybersecurity aspect of the medical device industry. Due to the increase in commonalty of exploits as services, consumers with wirelessly connected medical devices can be exposed to future attacks on their devices. Additionally, they face a risk from unintentional vulnerabilities that can affect the normal operation of their device. The only way to mitigate these risk factors is regulation, legislation, and eduction. These actions must be taken immediately before one of these theoretical attacks becomes a historical attack.

Works Cited:

Greenberg, Andy. "It's Finally Legal To Hack Your Own Devices (Even Your Car)." Wired. Conde Nast, n.d. Web. 14 Dec. 2016.

The Atlantic. Atlantic Media Company, n.d. Web. 14 Dec. 2016.

"Cybersecurity." Cybersecurity. FDA, n.d. Web. 14 Dec. 2016.

Bruce, Schiener. "DDoS Attacks against Dyn." Schiener on Security. N.p., n.d. Web. 14 Dec. 2016.

"Go Ahead, Hackers. Break My Heart." Wired. Conde Nast, n.d. Web. 14 Dec. 2016.

"Hired Experts Back Claims St. Jude Heart Devices Can Be Hacked." Reuters. Thomson Reuters, 2016. Web. 14 Dec. 2016.

Https://www.facebook.com/PrivacyPC. "History and Evolution of the Locky Ransomware." HackRead. N.p., 2016. Web. 14 Dec. 2016.

Https://www.facebook.com/PrivacyPC. "History and Evolution of the Locky Ransomware." HackRead. N.p., 2016. Web. 14 Dec. 2016.

Jones, Russel L., and Sheryl Coughlin. "Networked Medical Device Cybersecurity and Patient Safety: Perspectives of Health Care Information Cybersecurity Executives." Deloitte Isuee Breif. Deloitte, n.d. Web. 14 Dec. 2016.

Lars, Nile. "Connected Medical Devices, Apps: Are They Leading the IoT Revolution — or Vice Versa?" Wired. Conde Nast, n.d. Web. 14 Dec. 2016.

Lui, Spandas, and Hayley Williams. "Cerber Is A Ransomware That Is Run Like A Franchise." Lifehacker Australia. N.p., 2016. Web. 14 Dec. 2016.

"Muddy Watter STJ Report." Muddy Watter STJ Report. N.p., 25 Aug. 2016. Web. 14 Dec. 2016.

Radcliffe, Jerome. "Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System." Blackhat. Blackhat, n.d. Web.

Schneier, Bruce. "Hacking Medical Devices." Schneier on Security. N.p., n.d. Web. 14 Dec. 2016.

Storm, Darlene. "Black Hat: Lethal Hack and Wireless Attack on Insulin Pumps to Kill People." Computerworld. Computerworld, 2011. Web. 14 Dec. 2016.