ADA University

Either Healthy or Secure: A Literature Review on Cyber Threats to Medical Devices and Measures to Protect Them

Khalil Asadzade

Introduction

In 2007, vice-president of the USA, Dick Cheney, hires engineers to modify his cardiac implant to alter wireless communication with the device, due to the fear of terrorist cyberattacks that could be aimed to disable the device and potentially lead to a lethal outcome. In 2015, Anthem, one of the biggest healthcare and insurance providers in the USA, was attacked by hackers to commit an identity theft of thousands of its employees and clients. In May 2017, WannaCry, the biggest cyber virus ever known, has infected about 300 000 computers worldwide and has been spread to over 600 different healthcare organizations in the UK, leading to one of the greatest invasions into hospitals ecosystems up to date: from almost 7000 medical appointments cancelled due to the technical issues to disabled ambulances and infected diagnostic equipment.

Today, when we free ourselves from the physical world and bound to the digital one, the security of such steps up as one of the most important aspects to be implemented, as the latter offers much greater ground for different types of attacks on our "online lives", directly affecting the real ones. Being able to track the development of digital world since childhood, thanks to the generation I have been born in, I observed how the biggest companies have been investing huge amounts of their financial holdings to the security of their products, websites, office chats, etc. Indeed, if we have a closer look at the statistics, it appears that cybersecurity vulnerabilities have been declining significantly as time passes and hackers are left with fewer and fewer tools to infect our beloved devices such as phones and computers. Nevertheless, it seems that this is not the case with regards to the health sector, which should be standing to protect us and our health, yet, fails to comply with many of the cybersecurity standards developed in other sectors and therefore puts us in threat of cyberattacks, resulting into identity theft or manipulations of the electronic devices we have injected into our bodies

due to the health status. By above, having a vast interest in the cybersecurity systems themselves and with healthcare being one of the most vital aspects of our lives, I have decided to investigate the current situation of cybersecurity in the medical sector by employing the following research question: which cyber threats, if they exist, is the medical sector being exposed to and how cybersecurity systems are and should be dealing with those? In this paper, I am going to look at the cybersecurity systems in medical devices and hospitals in order to investigate the potential threats those are being exposed to and measures that can be or are taken to cope with those, because it will address the bigger problem of healthcare control in the developing world of digital medicine.

Threats are There

In 2015, early concerns about the cybersecurity of medical devices were raised by NIST (National Institute of Standards and Technology) as stated in the article by InsideHealthPolicy.com, what coincides with the cases of cybersecurity vulnerabilities in some devices in 2015 and 2016, which are described by Laurie Pycroft and Tipu Z.Aziz (2018) in their research on existing threats in cybersecurity systems. A paper by J. Conn (2016) on IT systems in healthcare indicates that 2015 has been a record year for the medical sector in terms of cybersecurity breaches and that medical experts expressed concerns that the number of such will only be increasing with years. Indeed, if we consider records from year 2009, number of major breaches in cybersecurity levels at 1470, which exposed medical records of 115.6 million individuals, with 97% of those being hacked in 2015 (HHS' Office for Civil Rights as cited in J. Conn, 2016). It is also identified that the medical sector is one of the most affected by cyber threats, levelling at 24% out of all violations in all sectors (Cristian Martignani, 2019). A paper by Karsten Weber, Michele Loi, Markus Christen and Nadine Kleine (2018) describes the particular standards that cybersecurity systems in medical sector are expected to meet: quality and efficiency of services, the privacy of information and confidentiality, usability, and safety. Out of those, the privacy of information and confidentiality is one of the highest concerns of medical device cybersecurity experts (Cristian Martignani, 2019; Laurie Pycroft & Tipu Z. Aziz, 2018; K. L. Offner, E. Sitnikova, K. Joiner & C. R. MacIntyre, 2020).

Laurie Pycroft and Tipu Z.Aziz (2018) are describing various occasions of hacker attacks, distinguishing between clients' private information manipulations and active attacks, shutting down electronic healthcare systems in hospitals, thus disabling the medical devices which sustain lives of people (Cristian Martignani, 2019; Laurie Pycroft & Tipu Z. Aziz,

2018; K. L. Offner, E. Sitnikova, K. Joiner & C. R. MacIntyre, 2020). Disabled medical devices might lead to the significant damage to the patient's health, even though few instances of such have been detected yet; nevertheless, potential vulnerabilities that hospitals cybersecurity systems exhibit are of the highest concern of medical experts, as it appears that many of those systems fail to approach certain standards that are expected to be met or are applied in other sectors and huge industries (Laurie Pycroft & Tipu Z. Aziz, 2018).

With regards to the single target oriented attacks - focusing on a specific medical device, previous researches have discovered vulnerabilities in devices from different manufacturers, who have themselves admitted those during 2015 and 2016, calling back large batches of the devices from the hospitals (Laurie Pycroft & Tipu Z. Aziz, 2018). Another study, conducted in Australia by K. L. Offner, E. Sitnikova, K. Joiner and C. R. MacIntyre (2020), has gathered about 300 records of cybersecurity violations in healthcare systems to discover that even during the simple electronic interactions such as scanning the documents or sharing the medical history of patients, valuable information can be stolen. Being specific, whenever any electronic "communication" happens between the receiver and the sender, information passes through certain base-stations, which can be attacked by hackers and private information or credentials can be obtained by those illegally (Cristian Martignani, 2019). However, those attacks are not limited to the electronic devices, with analogue sensors also being under the threat, due to the phenomenon known as social engineering (Laurie Pycroft & Tipu Z. Aziz, 2018). Social engineering refers to the manipulation of people which aims to obtain their personal information or credentials by a means of language and different indistinguishable traps usually placed in emails and chats. By that, required input information can be retrieved to then bypass the analogue devices.

Existing and Possible Solutions

In cybersecurity, solutions and tools are developed as issues arise, but to lower the number of incidences of hacker attacks, certain regulations are imposed beforehand by healthcare control organizations. Those regulations are directed to check the software of the medical devices being shipped to the hospitals and pharmacies. Nevertheless, it appears that even such giant organizations as FDA (U.S. Food and Drug Administration) are having leakages when some software corrupted medical devices are being passed to the hospitals for use (Ronquillo J. & Zuckerman D., 2017). It becomes especially vital when those devices are cardiac implants, which are directly controlling the lives of the patients.

It is identified that most of the medical devices lack auditing, which is the process of keeping track of all the events happening in the ecosystem of the medical device so that whenever an issue arises, its logs are recorded – alternative to journaling in the digital world (Cristian Martignani, 2019; Laurie Pycroft & Tipu Z. Aziz, 2018). Addition of such feature is a crucial component of any cybersecurity system, as it allows experts to analyze the corrupting events and build a strong defensive mechanism from such. Moreover, it is being noted that many of the bugs (an error that cannot be explicitly observed) are not being reported to manufactures due to the outdated mechanisms for determining the security flaws (Laurie Pycroft & Tipu Z. Aziz, 2018). It is mentioned by Laurie Pycroft & Tipu Z. Aziz (2018) that, today, the number of independent researchers who attempt to determine bugs in the devices and report those to manufacturers has significantly increased - a trend that potentially builds a solid ground for elimination of cybersecurity violations in the medical sector.

Both Cristian Martignani (2019) and Laurie Pycroft & Tipu Z. Aziz (2018) report that multi-factoring authentication is another solution that would drastically decrease the number

of cyber threats to medical devices. Multi-factoring authentication is a process when access to the device is only granted if the user has passed two or more security locks. The authors note that it is very easy to implement and is quite effective, as one of the access requirements could be set up to be some factors in relative proximity to the patient, therefore, could only be hacked by a means of social engineering (see “Threats are There” section). However, the trade-off between the cybersecurity of the device and its capabilities in its primary functions exists, as do both authors note. IMDs (implantable medical device) are usually small devices that should be operating in human bodies for years, sustaining comfortable and long life. This becomes a challenge when a battery lifetime is reduced due to the additional software implemented to ensure cybersecurity, therefore, a balance between these two should be found to successfully introduce better means of cybersecurity to the devices.

Conclusion

Overall, this paper attempts to outline the possible cyber threats to medical devices that were discovered by the previous studies and offer a combination of various effective solutions offered in different journal articles. Although many of the articles have successfully utilized the records found to analyze the cyber threats, they frequently appear to be employing a hard-to-understand language for the casual readers, therefore, by this research, I tried to reach a greater audience with such a vital issue, which otherwise might be overlooked due to its technical content. Limitation of this study that I am able to observe is the lack of appropriate resources to access other databases having many qualitative papers on the subject. In all other aspects, it appears that the study does contain no matter to undermine its reliability, as studies selected are of the most recent publication date, keeping it highly relevant, which is possibly the only determinant of the reliability in the subject of the technical content, where no ambiguous assumptions are usually made and all the information is based on factual records.

This paper clearly identifies that cyber threats do exist in the medical sector, therefore, actions are to be applied to deal with those to ensure the very nature of the healthcare: the safety of people. Solutions such as multi-factor authentication and log tracking are relatively easy and fast to implement, provided the funding by the government, as they are already employed in many cybersecurity systems today and are performing at the desired levels, ensuring security for millions of users of different digital platforms. Additionally, I believe it is important to emphasize on the spread of awareness about this issue globally, as many people do not even know at what threats they are being posed by simply accessing the services of the hospitals and healthcare systems and few studies, websites, media platforms do mention it. By not ignoring the problems that humans face, we

step forward into a more secure future, therefore, here arises another important key to deal with cybersecurity threats in medical devices: those who are put into awareness of such issue and have or willing to have the power to influence the development of appropriate techniques and standards for cybersecurity systems should not be ignoring opportunities to do so. Ignorance only facilitates the problem, leading to worse outcomes, more undesirable cases, better tools for hackers, and greater breaches in the cybersecurity systems.

REFERENCES

Inside Cybersecurity. (2015). Medical Institute Flags Medical Device Cybersecurity As Top 2015 Concern. *InsideHealthPolicy.com*, 13-13.

Jay, R. G., & Zuckerman, D. M. (2017). Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health. *The Milbank Quarterly*, 535-553.

Joseph, C. (2016). Cybersecurity rising as health IT concern. *Business Premium Collection*, 31-34.

Martignani, C. (2019). Cybersecurity in cardiac implantable electronic. *Expert Review of Medical Devices*, 437-444.

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, 556-585.

Pycroft, L., & Aziz, T. Z. (2018). Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices*, 403-406.

Weber, K., Loi, M., Christen, M., & Kleine, N. (2018). Digital Medicine, Cybersecurity, and Ethics: An Uneasy Relationship. *The American Journal of Bioethics*, 52-53.