Review of Cybersecurity in the Radiology Department

Arthur Pangemanan

***Abstract*—This paper will review the cyber threat of modern medical device within the radiology department.**

***Index Terms*—Cyber-security, Security, Risk, Safety, Wireless, Medical devices.**

I. Introduction

THE medical industry has change ever since the first computer were introduced. The healthcare technologies have the potential to extend, save and enhance the live of patients. Furthermore, hospitals have witnessed a proliferation of networked medical equipment in the past decade. There is an emergent trend of connection medical equipment to the hospital network for easy accessibility and manageability. As healthcare devices continue to evolve, so does the inter-connectivity. For example, it provides efficiency, error reduction, automation, and remote monitoring. Interconnected technology allows health professionals to monitor and adjust devices without the need for hospital visit or invasive procedure [1]. With integration comes complexity and challenges in management and this protection [4]. However, interconnected technology introduces new cyber-security vulnerabilities in the same way other networked computing systems are vulnerable. Recently, securing medical devices against cyber-attacks or malware outbreaks and safeguarding protected health information (PHI) stored on devices or exchanged between a device and the provider's network is a growing challenge for clinical engineers and hospital information technology (IT) professional [2]. The number of high-profile public demonstrations of successful attacks on devices and medical networks have increased. This fact raises the concern that inter-connectivity will directly affect clinical care and patient safety.

Over the past few years, the question of inadequate clinical security has been gaining attention from both industry leaders and clinical practitioners. The integration of medical devices, networking, software, and operating systems means that the relative isolation and safety of medical devices are challenged [4]. These vulnerability is also due to many manufacturers focus their efforts on innovation and functionality, with little emphasis on the network security of this devices [5].

Designing a secure medical device is fundamentally different from any other devices that only focus on safety and efficacy. Safety design decisions are based on the assumption that hazardous condition or failure occur accidentally. However, the assumption that hazardous condition or failure occurs accidentally no longer holds true as malicious attackers try to trigger hazards in devices through intentional repeated attempts [10]. Thus manufacturer tends to not implement the necessary security check against these malicious attacks. This fact become more important as the radiology departments usually have the highest density of networked medical equipment in a hospital [5]. This paper will review the cyber threat of modern medical devices within the radiology department.

II. Background

With the numerous data breaches in healthcare over the last several year, it seems to be unreasonable for patients having any expectation of privacy and security in their health information. In 2012, 780,000 patients records were stolen from the State of Utah Department of Health, Department of Technology server, by an Eastern European hacker. Another at Saint Joseph's Health System in California, approximately 31,800 patients' record was made potentially available through basic Internet search engines for about a year because security settings on the system were set incorrectly [7].

A. Implantable Medical Devices

B. Electronic Health Records

C. Radiology Devices

III. Cybersecurity in Radiology Department

A. Types of Cyber Threats

IV. Future Security Challenges

The medical industry face many challenges

V. Conclusion

The conclusion goes here.

References

[1] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[2] A. Wirth, "Cybercrimes pose growing threat to medical devices," *Biomedical instrumentation & technology*, vol. 45, no. 1, pp. 26–34, 2011.

[3] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Commun. ACM*, vol. 58, no. 4, pp. 74–82, Mar. 2015. [Online]. Available: http://doi.acm.org/10.1145/2667218

[4] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices (Auckland, NZ)*, vol. 8, p. 305, 2015.

[5] V. Moses and I. Korah, "Lack of security of networked medical equipment in radiology," *American Journal of Roentgenology*, vol. 204, no. 2, pp. 343–353, 2015.

[6] A. Ferrara, "Cybersecurity in medical imaging," *Radiologic technology*, vol. 90, no. 6, pp. 563–575, 2019.

[7] S. Murphy, "Is cybersecurity possible in healthcare," *National Cybersecurity Institute Journal*, vol. 1, no. 3, pp. 49–63, 2015.

[8] M. Stites and O. S. Pianykh, "How secure is your radiology department? mapping digital radiology adoption and security worldwide," *American Journal of Roentgenology*, vol. 206, no. 4, pp. 797–804, 2016.
[9] Z. Wang, P. Ma, Y. Chi, and J. Zhang, "Medical devices are at risk: Information security on diagnostic imaging system," pp. 2309–2311, 2018. [Online]. Available: http://doi.acm.org/10.1145/3243734.3278513
[10] A. Ray and R. Cleaveland, "An analysis method for medical device security," pp. 16:1–16:2, 2014. [Online]. Available: http://doi.acm.org/10.1145/2600176.2600192
[11] P. Gerard, N. Kapadia, J. Acharya, P. T. Chang, and Z. Lefkovitz, "Cybersecurity in radiology: access of public hot spots and public wi-fi and prevention of cybercrimes and hipaa violations," *American Journal of Roentgenology*, vol. 201, no. 6, pp. 1186–1189, 2013.
[12] T. Mahler, N. Nissim, E. Shalom, I. Goldenberg, G. Hassman, A. Makori, I. Kochav, Y. Elovici, and Y. Shahar, "Know your enemy: Characteristics of cyber-attacks on medical imaging devices," *arXiv preprint arXiv:1801.05583*, 2018.
[13] P. Ma, Z. Wang, X. Zou, J. Zhang, Q. Liu, X. Lyu, and W. Wang, "Medical imaging device security: An exploratory study," *arXiv preprint arXiv:1904.00224*, 2019.
[14] M. Busdicker and P. Upendra, "The role of healthcare technology management in facilitating medical device cybersecurity," *Biomedical instrumentation & technology*, vol. 51, no. s6, pp. 19–25, 2017.
[15] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: how safe are we?" *Bmj*, vol. 358, p. j3179, 2017.
[16] M. Marwan, A. Kartit, and H. Ouahmane, "Design a secure framework for cloud-based medical image storage," pp. 7:1–7:6, 2017. [Online]. Available: http://doi.acm.org/10.1145/3090354.3090361
[17] D. Foo Kune, K. Venkatasubramanian, E. Vasserman, I. Lee, and Y. Kim, "Toward a safe integrated clinical environment: A communication security perspective," in *Proceedings of the 2012 ACM Workshop on Medical Communication Systems*, ser. MedCOMM '12. New York, NY, USA: ACM, 2012, pp. 7–12. [Online]. Available: http://doi.acm.org/10.1145/2342536.2342540
[18] H. Almohri, L. Cheng, D. D. Yao, and H. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*, ser. CHASE '17. Piscataway, NJ, USA: IEEE Press, 2017, pp. 114–119. [Online]. Available: https://doi.org/10.1109/CHASE.2017.69
[19] C. TK, "Inside risks controlling for cybersecurity risks of medical device software," *Communications of the ACM*, vol. 56, no. 10, 2013.
[20] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," *Biomedical instrumentation & technology*, vol. 48, no. s1, pp. 38–41, 2014.
[21] G. Tanev, P. Tzolov, and R. Apiafi, "A value blueprint approach to cybersecurity in networked medical devices," *Technology Innovation Management Review*, vol. 5, no. 6, 2015.
[22] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Commun. ACM*, vol. 58, no. 4, pp. 74–82, Mar. 2015. [Online]. Available: http://doi.acm.org/10.1145/2667218
[23] C. J. Lewis, "Cybersecurity in healthcare," Ph.D. dissertation, 2014, copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2016-06-05.