Attacking Pathways of Health Information System (HIS)

Ying He[1], Kun Ni[1], Cunjin Luo[2,3]

[1]University of Nottingham, Nottingham, UK
[2]University of Essex, Colchester, UK
[3]Southwest Medical University, Luzhou, China

Abstract

The health information system (HIS) has been targeted by the hackers especially during the pandemics of COVID 19. This paper is motivated by the recent cyber incidents happened to healthcare organisations. This study was conducted to demonstrate how the HIS can be hacked and provide some recommendations to protect the HIS. We created a simulated virtual environment by implementing an open-source medical system. We then followed the NIST pen-testing methodology to perform ethical hacking. The hacking was successful, and we have managed to exploit several vulnerabilities of the simulated HIS. We then proposed cyber security recommendations to protect the HIS. Future work will consider demonstrating attacks to a specialized cardiac diagnosis medical system, e.g. the arrhythmia detection and classification in ambulatory ECGs, and explore how the core of its algorithms can be hacked and protected.

1. Introduction

Health sector has been targeted by the cyber attackers who aims to bring down the health critical infrastructure. This research is motivated by the recent security incidents happened to the healthcare organisations, including the US Department of Health and Human Services [1], the World Health Organisation [2] and some pharmaceutical companies, etc [3]. The United States Public Health Service reported that about 100 million pieces of patient information were stolen every month in 2020 [4]. Cyber attackers can not only destroy HIS, but also gain access to or modify sensitive medical diagnosis records produced by diagnosis components such as the ECGs [5-10].

Ethical hacking can help identify vulnerabilities and is an active defense to protect systems through discovering attack paths in the targeted system [3]. It is demonstrated through launching security attacks towards the targeted system. However, this practice can potentially damage the system, and cannot be applied directly over a real-world setting. Therefore, a virtual environment is required to simulate a HIS that can be used for ethical hacking purpose. There are some research efforts demonstrating ethical hacking towards HIS as well as some diagnosis and proposing solution to counteract such attacks [11-15], however, their work considers only a limited number of vulnerabilities (e.g. the OWASP top 10 vulnerabilities).

In this paper, we created a simulation platform through implementing an open-source health information system, OpenEMR, on a virtual environment. In order to simulate a realistic environment, we also installed some software, which health organisations always use. We then launched ethical hacking towards the simulated HIS using various tools. We were able to exploit some vulnerabilities and penetrated the system.

This paper makes the following contribution,

- Builds a HIS simulation platform by implementing an open-source medical system.
- Demonstrates ethical hacking (pen-testing) to the HIS simulation environment using various ethical hacking tools following the NIST ethical hacking framework.
- Proposes security solutions to mitigate security risks and protect the HIS.

3. Methods

We adopted the NIST ethical hacking framework [16] to carry out the study following key stages of planning, discovery, attack, and reporting. Firstly, we set up a simulation platform by implementing an open-source HIS, the OpenEMR. We then launched ethical hacking to exploit vulnerabilities of the simulated HIS. Finally, we propose security solutions to counteract such attacks.

3.1 HIS Simulation

We created a simulation environment to simulate a medical worker's machine with the OpenEMR installed. The targeted machine was set to have some open ports,

which is common for medical workers computer. We also installed some software that health organisations always use. The system, software, and service versions are old because the medical organisation's machines always lack upgrade. Figure 1 depicts the structure of the simulated network. Two machines: the targeted host and the attack host, were set up. The targeted host machine got a cyber-attack, and the attack host machine launched an attack.

3.2. Ethical Hacking & Result Analysis

We have launched a series of attacks using various ethical hacking tools. Those includes, Nmap scanning, Xray scanning, SQLMap and Metasploit. Table 1 shows the tools used in different stages following the NIST framework,

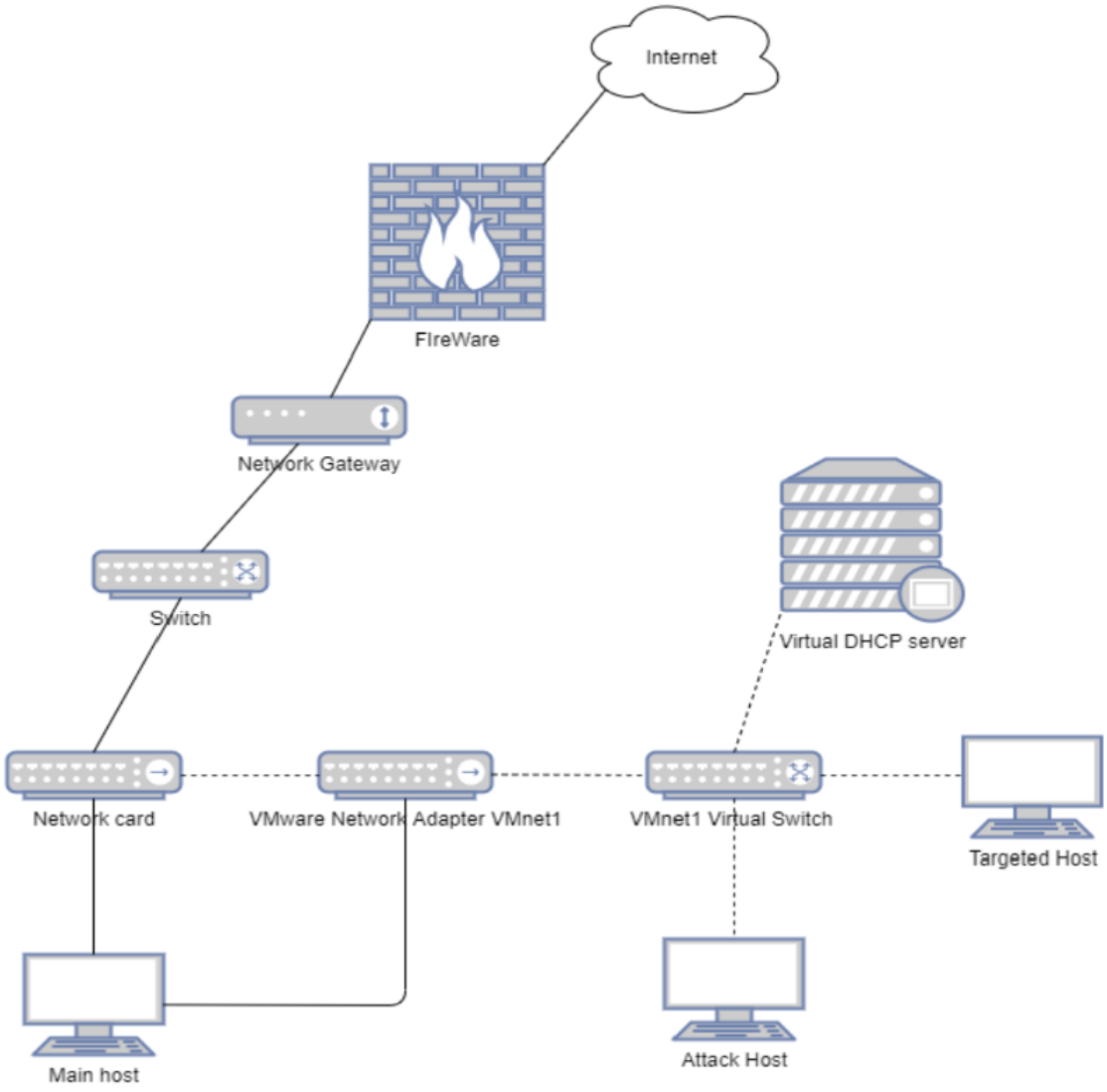

Figure 1. The Network Structure of Targeted Host and Attack Host

Table 1: Ethical Hacking Actions Following NIST Ethical Hacking Framework

NIST Stages	Key Activities
Scanning	Use Nmap scanning tool to identify the number of ports, port status, protocol, and operating system.
	Use Xray scanning tool to identify the vulnerabilities.
Discovery	Use information collected from the scanning stage to decide about the exploits.
Attack	Use SQLMap tool to exploit SQL injection related vulnerabilities.
	Use Metasploit tool to probe networks and applications related flaws and vulnerabilities
Reporting	Produce report using information collected from ethical hacking tools.

The results show that the ethical hacking was successful. There were 7 successful exploits out of 24 exploits. These exploits are related to improper input validation, cross-site request forgery, remote code execution, denial of service attack, improper authentication, remote access backdoor, deserialization of untrusted data. 3832 seconds expert time were taken for the exploits.

5. Security Recommendations

To prevent such attacks, improper input validation can be mitigated by using an input validation framework such as the OWASP ESAPI Validation API [17]. Cross-site request forgery and deserialization can be counteracted by using the OWASP XSS Prevention Cheat Sheet [18]. Remote code execution and remote access backdoor can be addressed using web application firewall (WAF) [19]. Denial of service (DoS) attack should be stopped at an earlier stage through enabling DoS protection, dropping packets from malicious sources [20]. Multi-factor authentication should be used to address improper authentication [21].

6. Discussion and Conclusion

This research created a simulated health information system (HIS) by implementing OpenEMR, that allows for carrying out ethical hacking. We have carried out the pen-testing following the NIST framework and identified a set of vulnerability related to improper input validation, cross -site request forgery, remote code execution, denial of service attack, improper authentication, remote access backdoor, deserialization of untrusted data. As OpenEMR is widely used by health organisations, this research has significance for health organisations to address similar security vulnerabilities and prevent similar attacks.

Future work will establish a cardiac intelligent medical diagnosis system with computational models [22-25] and explore how the core of its algorithms can be hacked and protected. Future work will also consider AI-based ethical hacking to automate the testing processes and applying a comprehensive set of security mechanisms to prevent against cyber-attacks in health information system [26-30].

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61803318).

References

[1] Jacobs, S.S.a.J., Cyber-attack hits U.S. health agency amid covid-19 outbreak. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.

[2] Beware of criminals pretending to be WHO https://www.who.int/about/communications/cyber-security

[3] Bing., J.S.a.C., Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker gilead – sources https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV

[4] Evans, Melanie, and McMillan, Robert, "Cyberattacks Cost Hospitals Millions During Covid-19. " The Wall Street Journal, February 16 ,2021.

[5] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang. "Modelling the effects of quinidine, disopyramide, and E-4031 on short QT syndrome variant 3 in the human ventricles." Physiological measurement 38, no. 10 (2017): 1859.

[6] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang. "In silico assessment of the effects of quinidine, disopyramide and E-4031 on short QT syndrome variant 1 in the human ventricles." PloS one 12, no. 6 (2017): e0179515.

[7] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang. "Modelling the effects of chloroquine on KCNJ2-linked short QT syndrome." Oncotarget 8, no. 63 (2017): 106511.

[8] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang. "Effects of amiodarone on short QT syndrome variant 3 in human ventricles: a simulation study." Biomedical engineering online 16, no. 1 (2017): 69.

[9] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang.

"Modeling the effects of amiodarone on short QT syndrome variant 2 in the human ventricles." In 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 4273-4276. IEEE, 2017.

[10] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang. "Modeling the effects of amiodarone on short QT syndrome variant 2 in the human ventricles." In 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 4273-4276. IEEE, 2017.

[11] Evans, Mark, Ying He, Cunjin Luo, Iryna Yevseyeva, Helge Janicke, and Leandros A. Maglaras. "Employee perspective on information security related human error in healthcare: Proactive use of IS-CHEC in questionnaire form." IEEE Access 7 (2019): 102087-102101.

[12] Evans, Mark, Ying He, Leandros Maglaras, and Helge Janicke. "Heart-is: A novel technique for evaluating human error-related information security incidents." Computers & Security 80 (2019): 74-89.

[13] He, Ying, and Chris Johnson. "Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization." Informatics for Health and Social Care 42, no. 4 (2017): 393-408.

[14] He, Ying, and Chris Johnson. "Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template." International journal of medical informatics 84, no. 11 (2015): 941-949.

[15] Evans, Mark, Ying He, Leandros Maglaras, Iryna Yevseyeva, and Helge Janicke. "Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector." International journal of medical informatics 127 (2019): 109-119.

[16] Souppaya, Murugiah P., and Karen A. Scarfone. "Technical guide to information security testing and assessment." (2008).

[17] Kachhadiya, Rakeshkumar, and Emmanuel Benoist. "Development of the security framework based on OWASP ESAPI for JSF2. 0." (2013).

[18] Vishnu, B. A., and K. P. Jevitha. "Prediction of cross-site scripting attack using machine learning algorithms." Proceedings of the 2014 International Conference on Interdisciplinary Advances in Applied Computing. 2014.

[19] Prandl, Stefan, Mihai Lazarescu, and Duc-Son Pham. "A study of web application firewall solutions." International Conference on Information Systems Security. Springer, Cham, 2015..

[20] Yan, Qiao, et al. "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges." IEEE communications surveys & tutorials 18.1 (2015): 602-622. APA.

[21] Dasgupta, Dipankar, Arunava Roy, and Abhijit Nag. "Toward the design of adaptive selection strategies for multi-factor authentication." computers & security 63 (2016): 85-116.

[22] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang. "Effects of island-distribution of mid-cardiomyocytes on ventricular electrical excitation associated with the KCNQ1-linked short QT syndrome." In 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 3684-3687. IEEE, 2017.

[23] Luo, Cunjin, Kuanquan Wang, Ming Yuan, Zhili Li, Qingjie Wang, Yongfeng Yuan, Qince Li, and Henggui Zhang. "Effects of amiodarone on ventricular excitation associated with the KCNJ2-linked short QT syndrome: Insights from a modelling study." In 2015 Computing in Cardiology Conference (CinC), pp. 1093-1096. IEEE, 2015.

[24] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang. "Functional effects of island-distribution of mid-cardiomyocytes on Re-entrant excitation waves in the KCNQ1-linked short QT syndrome." In 2016 Computing in Cardiology Conference (CinC), pp. 933-936. IEEE, 2016.

[25] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang. "Effects of amiodarone on short QT syndrome variant 3 in human ventricles: a simulation study." Biomedical engineering online 16, no. 1 (2017): 69.

[26] Tzokatziou, Grigoris, Leandros A. Maglaras, Helge Janicke, and Ying He. "Exploiting SCADA vulnerabilities using a human interface device." Int J Adv Comput Sci Appl (2015): 234-241.

[27] Wood, Andy, Ying He, Leandros Maglaras, and Helge Janicke. "A security architectural pattern for risk management of industry control systems within critical national infrastructure." (2017).

[28] Evans, Mark, Leandros A. Maglaras, Ying He, and Helge Janicke. "Human behaviour as an aspect of cybersecurity assurance." Security and Communication Networks 9, no. 17 (2016): 4667-4679.

[29] Ayres, Nicholas, Leandros A. Maglaras, Helge Janicke, Richard Smith, and Ying He. "The mimetic virus: a vector for cyberterrorism." International Journal of Business Continuity and Risk Management 6, no. 4 (2016): 259-271.

[30] Zamani, Efpraxia, Ying He, and Matthew Phillips. "On the Security Risks of the Blockchain." Journal of Computer Information Systems (2018): 1-12.

Address for correspondence:

My Name.
Cunjin Luo

My Full postal address.
Key Laboratory of Medical Electrophysiology, Ministry of Education, Institute of Cardiovascular Research, Southwest Medical University, Luzhou 646000, China

My E-mail address.
cunjin.luo@yahoo.co.uk