Security Defense Strategy for Cardiac Medical Diagnosis System (CMDS)

Ying He[1], Ruben Suxo Camacho[1], Cunjin Luo[2,3], Henggui Zhang[4]

[1]De Montfort University, Leicester, UK
[2]Southwest Medical University, Luzhou, China
[3]Northeastern University, Shenyang, China
[4]The University of Manchester, Manchester, UK

Abstract

The medical systems have been targeted by the cyber attackers. This paper is motivated by the recent attacks that have resulted in the compromise of diagnosis results. This study was undertaken to show how the Cardiac Medical Diagnosis Systems (CMDS) can be hacked and propose security recommendations to prevent such attacks. We build a simulation platform by implementing an open source medical system. We feed the ECGs data from the PhysioNet/Computing in Cardiology (CinC) Challenge 2017 to the open source medical system. We then follow the OWASP pen-testing methodology to perform the ethical hacking. The hacking was successful and we have identified a major vulnerability of the system related to authentication. Finally, we are able to gain access to the sensitive ECG data. We then proposed cyber recommendations to prevent such attacks. Future work will consider using a mature CMDS, such as the arrhythmia detection and classification in ambulatory ECGs to investigate how the core of the algorithms can be attacked and protected.

1. Introduction

The growth in technology has increased the efficiency of hospitals, eliminated queues in medical centres and improved the bureaucratic processes. Nevertheless, even when there is a notable improvement in the healthcare industry, it comes with risks. For example, attackers can intercept information of patients while they are asking for an appointment or capture emails of doctors and nurses, depending on the aim of the attacker. The most common target for malicious attackers is critical information that affects healthcare services [1].

The ransomware called WannaCry affected thousands of private and public corporations worldwide. The NHS was one of those victims. Approximately, 80 out of 236 hospitals across England were affected. Since the attack, the healthcare organisations have started to tackle cyber challenges to protect their healthcare systems [2].

Healthcare has become the most attacked sector during the last few years. Even when there are security standards, such as ISO 27001 [3] and HIPAA [4] to strengthen their security, this sector still has the highest number of recorded incidents. In addition to this, it is important to understand the data that this sector should take care of and an analysis of the impact of diagnosis components [5-10] such as ECG to understand the impact in case it is vulnerable and the ECG record compromised.

Pen-testing can help to identify the vulnerabilities and demonstrate potential security breaches, but this practice has to be over-controlled and it cannot be applied over a real-world environment. For that reason, it needs to be performed following an appropriate methodology and in a secure environment. Therefore, a virtual environment for testing is required. There is existing work demonstrating cyber-attacks towards healthcare system and proposing cyber security strategies to defend against such attacks [11-15], however, it is not against a realistic healthcare system.

In this paper, we implemented an open source healthcare system called OpenEMR on a virtual machine. We also integrated an ECG database into the OpenEMR system, where the scenario was developed to carry out the pen-testing. One major vulnerability was found which is related to authentication.

This paper makes the following contribution,

- Implements an open source healthcare system, that accomplish with HIPAA and ONC standards with a ECGs component added into the system.
- Demonstrates the pen-testing of the implemented healthcare system and identified a vulnerability related to system authentication.
- Proposes cyber security solution to address the identified vulnerability.

2. Related work

2.1. Security in medical systems

Healthcare organisations have been targeted by a variety of threats both inside and. Table 1 provides a list of potential threats to the healthcare organisations.

Target	Integrity	Availability	Confidentiality
Healthcare system	- Modification of the system.	- A denial of services to loss connectivity. - Loss communication to third party systems/companies. - Malware infection.	- Specific configuration leak of the internal systems.
Healthcare staff	- Manipulation of patient records. - Change of appointment schedules.		- Unauthorized access to the staff account. - Exposure of personnel data.
Patients	- Manipulation of personal information. - Change of appointment schedules.		- Exposure of patients' data.

Table 1: Security Threats (Confidentiality, Integrity, Availability) to Healthcare Organisations

2.2. Healthcare related security standard

Depending on the country, there are regulations or laws to accomplish in order to prevent cyber attacks. In UK, GDPR [16] is the legislation that applies to all the companies who process, store and gather any data that belongs to EU citizens including UK. It is important to accomplish this regulation to provide more control over individual data. HIPAA is a US legislation for data privacy and security management specifically for medical information. All the organisations covered by HIPAA must comply with this standard, especially in the US. That is, all the entities covered by HIPAA must ensure the information that is stored, processed, held or transmitted in any way, including verbal, digital or physical in terms of integrity, confidentiality and availability.

3. Methods

The OWASP pen-testing methodology [17] is followed to carry out the study. Figure 1 illustrates pen-testing processes step by step. This study starts with setting up a simulation environment through implementing an open source medical system, OpenEMR. We then launch cyber attacks to identify the vulnerability. Finally, we propose security recommendations to address the vulnerabilities.

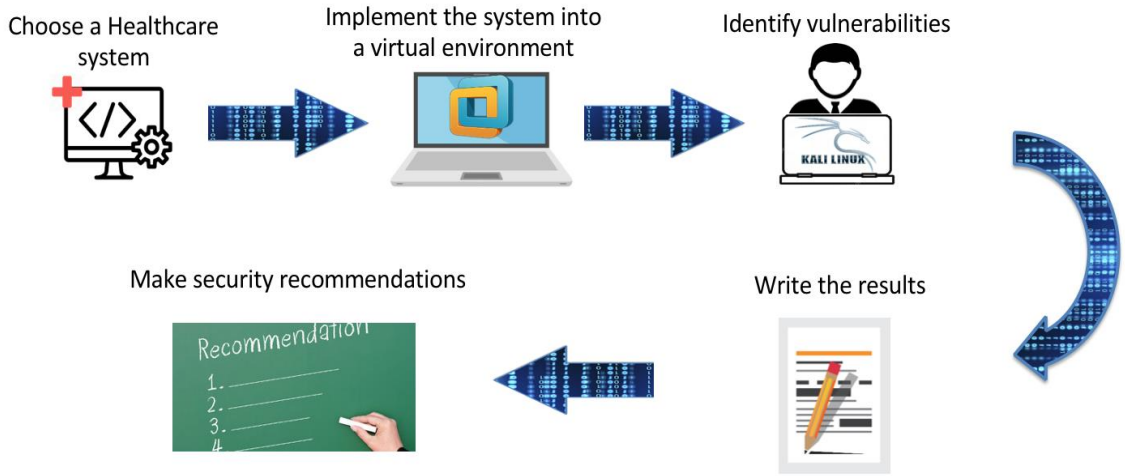

Figure 1. Ethical Hacking Processes.

3.2. Medical system preparation

We develop a simulation environment where pen-tester can test the system without worrying about how it could affect a real-world environment. We have created a virtual environment using software for virtualisation, in this case, VMware software. Once it is installed, we add an ECG component by modifying the internal code to integrate and visualize the ECG records inside the system.

4. Ethical Hacking & Result Analysis

We have launched brute force and dictionary attack [18, 19]. We have been successful in the dictionary attack and identified a vulnerability related to authentication which is one of the listed OWASP Top 10 vulnerability "A2 2017-Broken Authentication". This vulnerability requires a bit of practice using certain specific tools. It is also possible to try infinite authentication attempts until get the correct username and password. Once this is successful, we are able to log into the system and gain further access to the ECG data in the ECG component. Figure 2 provide an example of ECG record (sensitive information) that we could access.

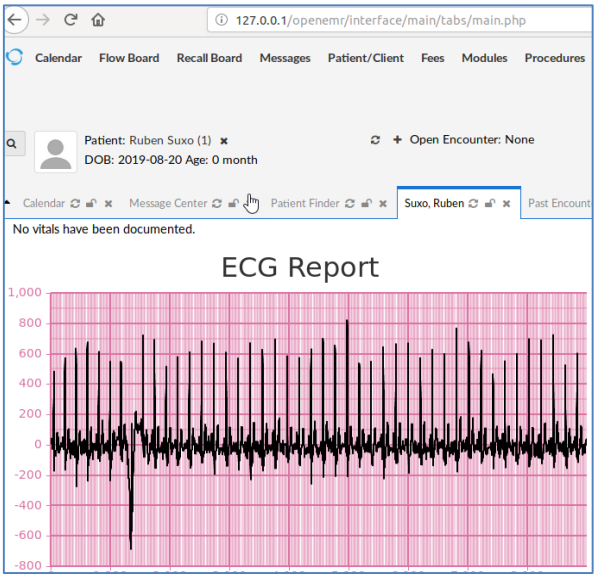

Figure 2. Sensitive ECGs Record Accessed.

5. Security Recommendations

To counteract against such attack, it is recommended to apply a captcha for login or to use two-factor authentication [20]. For example, after entering the password, the user is also asked to enter a PIN that will be send to his phone where the PIN represents the second factor of authentication. Another option is to limit the number of attempts and block the users during time when wrong passwords are attempted.

6. Discussion and Conclusion

This research created a simulated environment through implementing an open source healthcare system, called OpenEMR, that allows for carrying out pen-testing and identify the vulnerabilities. We have carried out the pen-testing following the OWASP method and identified a major vulnerability related to authentication. This study sets the fundamental work for further research into the investigation of a comprehensive set of vulnerabilities of the OpenEMR system. OpenEMR has been widely used by organisations in healthcare industry. The findings have significance for those organisations to prevent against similar attacks that are targeting healthcare.

Future work will focus on establishing a realistic cardiac intelligence medical diagnosis systems with complicated computational models such as the arrhythmia detection and classification in ECG data [21-24] and see how these models can be compromised and protected. Future work will also focus on borrowing experience from other industries in applying security mechanisms to detect and prevent, counteract cyber attacks in healthcare [25-29].

Acknowledgments

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

References

[1] Consolidate Tech (2019). 8 Big Security Threats to Cybersecurity in Healthcare | 2018. [online] Consolidated Technologies, Inc. Available at: https://consoltech.com/blog/security-threats-healthcare-systems/ [Accessed 1 Aug. 2019].

[2] Martin, Guy, Saira Ghafur, James Kinross, Chris Hankin, and Ara Darzi. "WannaCry—a year on." (2018): k2381.

[3] Calder, Alan. Nine Steps to Success: an ISO 27001 Implementation Overview. IT Governance Ltd, 2017.

[4] Cohen, I. Glenn, and Michelle M. Mello. "HIPAA and protecting health information in the 21st Century." Jama 320, no. 3 (2018): 231-232.

[5] 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.

[6] 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.
[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. "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.
[9] 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.
[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] 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.
[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] 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.
[15] 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.
[16] Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." A Practical Guide, 1st Ed., Cham: Springer International Publishing (2017).
[17] Al Shebli, Hessa Mohammed Zaher, and Babak D. Beheshti. "A study on penetration testing process and tools." In 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1-7. IEEE, 2018.
[18] Heule, Marijn JH, and Oliver Kullmann. "The science of brute force." Commun. ACM 60, no. 8 (2017): 70-79.
[19] Wang, Ding, and Ping Wang. "Offline dictionary attack on password authentication schemes using smart cards." In Information security, pp. 221-237. Springer, Cham, 2015.
[20] Wang, Ding, and Ping Wang. "Two birds with one stone: Two-factor authentication with security beyond conventional bound." IEEE transactions on dependable and secure computing 15, no. 4 (2016): 708-722.
[21] 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.
[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, 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.
[24] 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.
[25] 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).
[26] 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.
[27] 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.
[28] 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.
[29] 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