AI-Based Security Attack Pathway for Cardiac Medical Diagnosis Systems (CMDS)

Ying He[1], Cunjin Luo[2 3], Ruben Suxo Camacho[4], Kuanquan Wang[5], Henggui Zhang[6]

[1]University of Nottingham, Nottingham, UK
[2]University of Essex, Colchester, UK
[3]Southwest Medical University, Luzhou, China
[4]De Montfort University, Leicester, UK
[5]Harbin Institute of Technology, Harbin, China
[6]The University of Manchester, Manchester, UK

Abstract

The Cardiac Medical Diagnosis Systems (CMDS) are targeted by the cyber attackers. This paper is motivated by the recent cyber-attacks happened during the COVID 19 that have resulted in the compromise of medical data. This study was carried out to demonstrate how the CMDS can be breached into using an AI-based ethical attack pathway and propose security solutions to prevent such beaches. This study is based on an established simulation platform with an open source medical system, the OpenEMR. The system was fed with the ECGs data from the PhysioNet/ Computing in Cardiology (CinC) Challenge 2017. This paper proposed the AI based hacking pathway following the NIST pen-testing methodology based on our previous identified vulnerability related to authentication. We then presented cyber security recommendations to prevent such AI-based attacks. Future work will consider a realistic CMDS, such as the arrhythmia detection and classification in ambulatory ECGs to find out how the algorithms core can be hacked and protected.

1. Introduction

The sustainability and resilience of medical systems, which falls into the category of global sustainable goal of health and wellbeing, has attracted attention worldwide. This issue becomes outstanding due to the fast-increasing health data aggregated from different medical systems and devises/sensors, the need of intelligent medical systems, which is extremely helpful in rural places where there is a lack of doctors. Other auxiliary medical services such as remote and personalised medicine also have impact on the improvements of health and wellbeing.

The high profile ransomware attack called WannaCry has affected thousands of organisations around the globe. The NHS was one of those victims. After the attack, the healthcare organisations started taking actions to protect their medical systems [1]. The COVID 19 has further challenged the sustainability and resilience of the medical systems, evidenced by the recent incidents happened to Brno University Hospital in Czech Republic, the US Department of Health and Human Services, the World Health Organization (WHO) and its Partners [2].

It is important to protect the sensitive data that should be taken care of and an analysis of the impact of diagnosis components [3-8] such as ECGs to understand the impact if the ECG diagnosis records are compromised.

Ethical hacking which is also called pen-testing can help identify the weaknesses of the system and demonstrate security breaches. It is usually performed following an systematic methodology such as NIST or OWASP in a secure environment. There is existing work demonstrating cyber breaches towards medical system as well as its protection mechanisms [9-14], however, it is not against a realistic healthcare system.

Our previous work has built a simulation environment through implementing an realistic medical system, the OpenEMR, on a virtual platform. We demonstrated ethical hacking and identified a major vulnerability related to authentication [15]. This paper builds on and extends our previous work by proposing an AI-based attack pathway. This paper then presents the security defense solutions to counteract AI-based cyber attacks.

2. Related Work

2.1. Healthcare Cyber Security

Medical data can be classified into two groups, sensitive and non-sensitive. The data related to the patients especially the diagnosis data is categorised as sensitive data. For example, Electrocardiogram (ECG) data includes

 ISSN: 2325-887X DOI: 10.22489/CinC.2020.439

both patient information and the ECG waveform data and is classified as sensitive data. Such data has been targeted by the attackers using various attack vectors. Previous work demonstrated ethical hacking to the medical system [14, 15], but AI based ethical hacking has not attracted the attention of the healthcare community.

2.2. AI Based Ethical Hacking

AI based ethical hacking can automate the traditional ethical hacking to help identify system weakness. Table 1. lists the difference between manual and AI based ethical hacking,

Manuel	**AI based**
Less accurate	More accurate
Time consuming	The algorithms can be deployed on thousands of systems at a time
Investment on human	Less investment on human
Suitable for running the tests once or twice.	Suitable for repeatable tests.

Table 1: Manual and AI based Ethical Hacking

3. Methods

3.1. NIST Pen-Testing

The ethical hacking was carried out following the NIST pen-testing methodology, consisting of four stages, which are information gathering, discovery, attack and reporting [16]. Figure 1 shows the NIST pen-testing work flow.

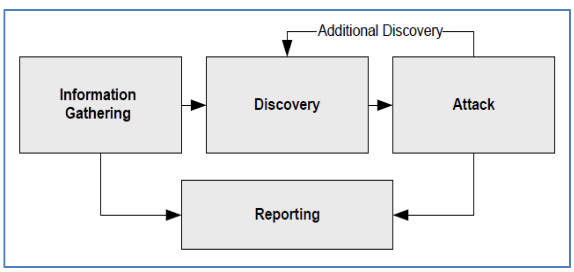

Figure 1. NIST Pen-testing Methodology [16]

3.2. The Simulated Medical System

In previous work, we have set up a simulation system on a virtual platform (using VMware software) through implementing an open source medical system, OpenEMR. We also add an ECG component by modifying the internal code to integrate and visualize the ECG records inside the system [15]. The context of the study is based upon this simulation platform.

4. AI based Ethical Hacking

In a previous study, we have launched brute force and dictionary attack [17, 18]. We have successfully performed the dictionary attack and identified a vulnerability related to authentication “A2 2017-Broken Authentication”, one of the listed OWASP Top 10 vulnerability.

This section proposes AI based ethical hacking methods. Figure 1 shows the weak points where AI can be applied to enter the system. As discussed in a previous study [15], the login through web interface is the main entry point. Figure 1 illustrates the AI-based ethical hacking pathway,

Trained password cracking algorithms. An algorithm can be trained initially to identify the most common patterns when a user utilises his password. Then, the algorithm will be applied to a set of words related to the user trying to find combinations based on the previous patterns. The output will be a set of possible passwords more accurate to the victim.

Face Recognition linked with Social Engineering. The attacker is able to check the mood of employees and take advantage of that to know how to approach the victim and to steal his passwords or other internal information. In Figure 1, the Face Recognition block points to the square number 1 and 4 because the attacker is able to steal the password of the website or servers and get access.

Trained directory discovery algorithms. This is similar to the concept of the password cracking. In this case, the algorithm learns what letter comes after another according to the language of study. And that concept is applied to discover hidden directories, instead of a dictionary attack or a brute force attack to the directories minimizing the time in performance.

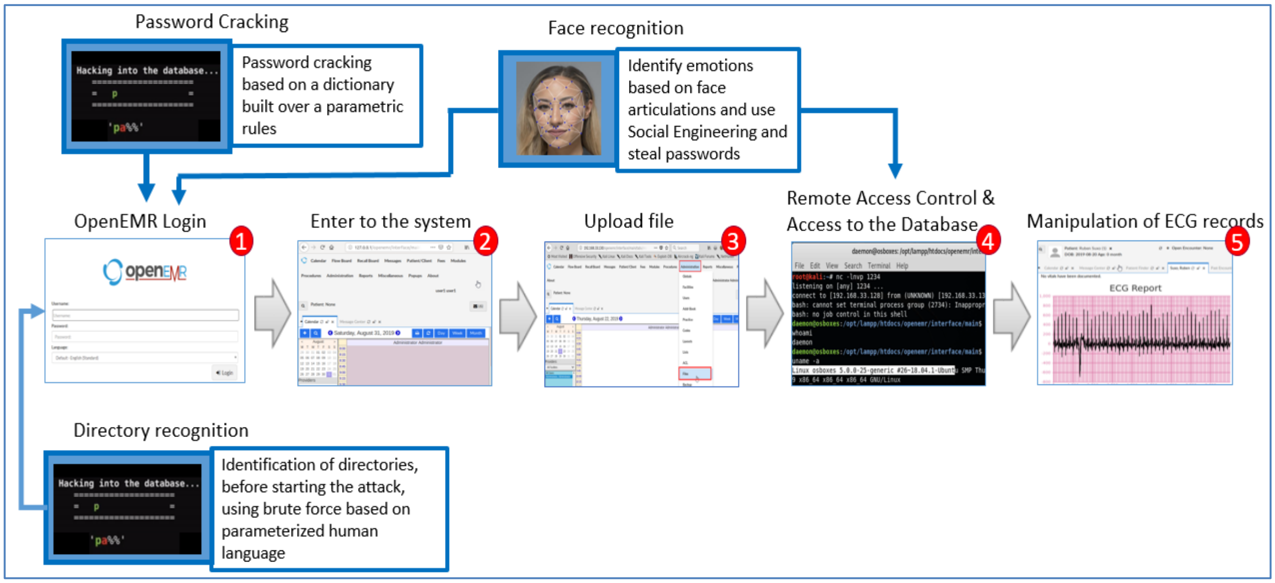

Figure 2. AI based Ethical Hacking.

5. Security Solutions

The traditional ways of counteracting such attack is to use multi-factor authentication (MAF) [19]. MAF can verify the users' identity by requiring multiple credentials. For example, a user can use a combination of elements to authenticate: a PIN sent through SMS, a code generated by the smartphone apps, or other physical devices. Another option is to limit the number of attempts and block the users after a number of failed login attempted.

Captcha can help identify the malicious AI based written programs and prevent the password decryption [20]. It is a common web based technique that can be used to identify whether the respondents are real human beings or a robot.

6. Conclusion and Future Work

Built on a previous study on the ethical hacking of the OpenEMR system, this study presented AI-based attacking pathway and cyber security solutions. It has implications for further research into the AI based attacks and the defence strategies in healthcare. Since the OpenEMR has been widely used in health prganisations, the findings can help them prevent against AI based attacks.

Future work will look into integrating the simulated environment with a real world intelligent cardiac diagnosis systems with sophisticated computational models such as the arrhythmia detection and classification in ECG data [21-24] and see how the core of the models can be hacked and protected. Future work will also consider borrowing experience from other sectors to deter and prevent cyber attacks in healthcare [25-30].

Acknowledgments

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

References

[1] Martin, Guy, Saira Ghafur, James Kinross, Chris Hankin, and Ara Darzi. "WannaCry—a year on." (2018): k2381.
[2] Eddy, Nathan. "Healthcare cyber attacks increasing during Covid-19 pandemic". [online] Healthcare IT News. Available at: https://www.healthcareitnews.com/news/who-coronavirus-testing-lab-hit-hackers-opportunistic-attacks-ramp [Accessed 6 Jun. 2020].
[3] 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.
[4] 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.
[5] Luo, Cunjin, Kuanquan Wang, and Henggui Zhang. "Modelling the effects of chloroquine on KCNJ2-linked short QT syndrome." Oncotarget 8, no. 63 (2017): 106511.
[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. "Effects of amiodarone on short QT syndrome variant 3 in human ventricles: a simulation study." Biomedical engineering

online 16, no. 1 (2017): 69.
[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] 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.
[10] 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.
[11] 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.
[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] 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.
[14] Luo, Cunjin, Hasan Soygazi, Helge Janicke, and Ying He. "Security Defense Strategy for Intelligent Medical Diagnosis Systems (IMDS)." In 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 3454-3457. IEEE, 2019.
[15] He, Ying, Ruben Suxo Camacho, Cunjin Luo, and Henggui Zhang. "Security Defense Strategy for Cardiac Medical Diagnosis System (CMDS)." In 2019 Computing in Cardiology (CinC), pp. Page-1. IEEE, 2019.
[16] Baloch, Rafay. Ethical hacking and penetration testing guide. CRC Press, 2017.
[17] Wang, Ding, and Ping Wang. "Offline dictionary attack on password authentication schemes using smart cards." In Information security, pp. 221-237. Springer, Cham, 2015.
[18] Zuo, Chaoshun, Qingchuan Zhao, and Zhiqiang Lin. "Authscope: Towards automatic discovery of vulnerable authorizations in online services." In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 799-813. 2017.
[19] 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.
[20] Gao, Haichang, Mengyun Tang, Yi Liu, Ping Zhang, and Xiyang Liu. "Research on the security of microsoft's two-layer captcha." IEEE Transactions on Information Forensics and Security 12, no. 7 (2017): 1671-1685.
[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] 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.
[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] Zamani, Efpraxia, Ying He, and Matthew Phillips. "On the Security Risks of the Blockchain." Journal of Computer Information Systems (2018): 1-12.
[28] 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).
[29] 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.
[30] He, Ying, Chris Johnson, Yu Lu, and Yixia Lin. "Improving the information security management: An industrial study in the privacy of electronic patient records." In 2014 IEEE 27th International Symposium on Computer-Based Medical Systems (CBMS), pp. 525-526. IEEE, 2014.

Address for correspondence:

Cunjin Luo

Email: cunjin.luo@essex.ac.uk
School of Computer Science and Electronic Engineering
University of Essex
Colchester CO4 3SQ
UK