Security Defense Strategy for Intelligent Medical Diagnosis Systems (IMDS)

Cunjin Luo, Hasan Soygazi, Helge Janicke, Ying He

***Abstract*—Aims: The Intelligence Medical Diagnosis System (IMDS) has been targeted by the cyber terrorists, who aim to destroy the Critical National Infrastructure (CNI). This paper is motivated by the most recent incidents happened worldwide and have resulted in the compromise of diagnosis results. This study was undertaken to show how the IMDS could be attacked and diagnosis results compromised and present a set of cyber defense strategies to prevent against such attacks.**

Methods and Results: This study used the ECGs data from the PhysioNet/Computing in Cardiology (CinC) Challenge 2017. We fed the data into our IMDS and launched a series of ethical hacking, which is specifically tailored to target IMDS. We proposed a set of cyber security strategies to prevent such compromise. We tested the effectiveness of our cyber defense strategies using an experiment. The results showed that the strategies were effective in protecting the IMDS diagnosis results from being compromised.

Conclusions: This study provides novel insights into the protection of IMDS and concludes that our cyber defense strategies can protect IMDS from being compromised by Brute Force and SQL Injection attacks.

I. Introduction

The Intelligence Medical Diagnosis System (IMDS) has revolutionized the way of diagnosing diseases. However, any advancement of IMDS will be in vain if the diagnosis is compromised. IMDS is now targeted by the cyber terrorists, who aim at destroying the Critical National Infrastructure (CNI). This paper is motivated by the most recent incidents happened worldwide that have resulted in the compromise of diagnosis results [1, 2]. This creates challenges to the sustainability of IMDS, which fall in the category of global sustainability of health and wellbeing.

The governments and research communities have realized the importance to protect their IMDS [3-6]. However, there is limited research on how the compromise has happened and how this can be prevented. Current cyber security research in healthcare focuses on protecting medical devices from cyber attacks [3-10], however, those strategies cannot be applied to protect IMDS. Accordingly, this study was undertaken to show how the IMDS diagnosis results can be compromised and present a set of cyber defense strategies to prevent such compromise.

* This study was supported by National Science Foundation of China (NSFC) under Grant No. 61803318, and Scientific-Technological Collaboration Project under Grant No. 2018LZXNYD-FP02.

C. Luo is with the Key Laboratory of Medical Electrophysiology, Ministry of Education, Collaborative Innovation Centre for Prevention and Treatment of Cardiovascular Disease/Institute of Cardiovascular Research, Associate Professor, Southwest Medical University, Luzhou, 646000, China He is also with the School of Computer Science and Engineering, Associate Professor, Northeastern University, Shenyang, 110819, China (email: cunjin.luo@ yahoo.co.uk).

H. Soygazi is with the School of Computer Science and Informatics, MSc Student, De Montfort University, Leicester, LE1 9BH, UK (e-mail: P17241568@alumni365.dmu.ac.uk).

H. Janicke is with the Cyber Technology Institute, School of Computer Science and Informatics, Professor, De Montfort University, Leicester, LE1 9BH, UK (e-mail: heljanic@dmu.ac.uk)

Y. He is with the Cyber Technology Institute, School of Computer Science and Informatics, Senior Lecturer, De Montfort University, Leicester, LE1 9BH, UK (e-mail: ying.he@dmu.ac.uk).

II. Methods

A. Intelligence Medical Diagnosis Data Preparation

We used the ECGs data from the 2017 PhysioNet/Computing in Cardiology (CinC) Challenge: AF classification from a short single lead ECG recording (http://physionet.org/challenge/2017/). It contains ECGs data including record names, date and ECGs waveform data. The data is then fed into our IMDS. The IMDS is an interactive system, allowing clinicians to search and retrieve patients ECGs record. Figure 1 illustrates the database schema of the IMDS, which contains record information and record data. Unique record names with dates and time taken are stored in one table, and ECGs waveform data is stored in a separate table.

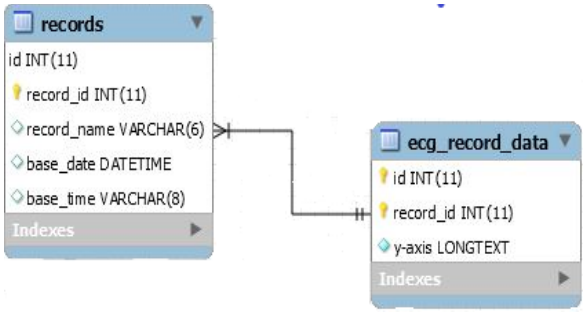

Figure 1 Database Schema for the ECGs Intelligence Medical Diagnosis Data

B. Attack Pathways and Entry Point

Figure 2 shows the attack pathways and entry points to the IMDS. In general, there are various entry points for attackers whereas in our IMDS structure, main entry point is the user interface login page which is interacting with the database. If the user interface is poorly designed, it can be vulnerable to bruteforce or code injection attacks. The follow scripts is an example of a code injection attack.

```
$usernameEnt = $_POST['username'];
$passwordEnt = $_POST['password'];
$servername = "localhost";
$username = "auser";
$password = "auserpassword";
$dbname = "imds_database";
```

Figure 2 Attack Pathways and Entry Point - Code Injection

C. *Ethical Hacking*

A series of ethical hacking have been launched, which are specifically tailored to target IMDS. This study follows the NIST pen-testing framework to perform the ethical hacking [11]. It targets on the ECGs record and its waveform data, aiming to compromise the diagnosis results. This section will demonstrate two ethical hacking scenarios, Brute Force and SQL Injection, which are the two bacis web based application ethical hacking methods according to the *Open Web Application Security Project (*OWASP).

Ethical Hacking Scenario 1 – Brute Force. We launched brute force attack [12] in order to obtain login details of the database. The attack was successful, and we were able to access sensitive data and modify the data in the database. The following scripts have been used for the brute force attack,

```
---------------------------------------------
#nmap -sV 127.0.0.1
#cd cd/var/tmp
#grep -v "^#" /usr/share/hasan/password.lst | head > pw.txt
#echo auserpassword >> pw.txt
#cat pw.txt
#cd
#msfconsole
msf> search mysql
msf> use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_inour) > set PASS_FILE /var/tmp/pw.txt
msf auxiliary(mysql_inour) > set RHOST 127.0.0.1
msf auxiliary(mysql_inour) > set USERNAME auser
msf auxiliary(mysql_inour) > exploit
---------------------------------------------
```

Ethical Hacking Senario 2 – SQL Injection. We launched automatic SQL injection attack [13] and used "sqlmap" to detect and exploit databases vulnerabilities. The attack was successful and we were able to extract entities from the database and obtained sensitive data. The following scripts have been used for the SQL injection attack,

```
---------------------------------------------
#systemtl start apcache2
#cd /usr/share/sqlmap
#python sqlmap.py -u "http://127.0.0.1/index.php" --data 'username=test&password=test#login=login' –dump
---------------------------------------------
```

D. *Cyber Defense Strategies*

Figure 3 provides the security defence strategies that are specifically tailored for IMDS. These include but are not limited to the ECGs record encryption, strong login password, login encryption, strict access control and regular ECGs record backup.

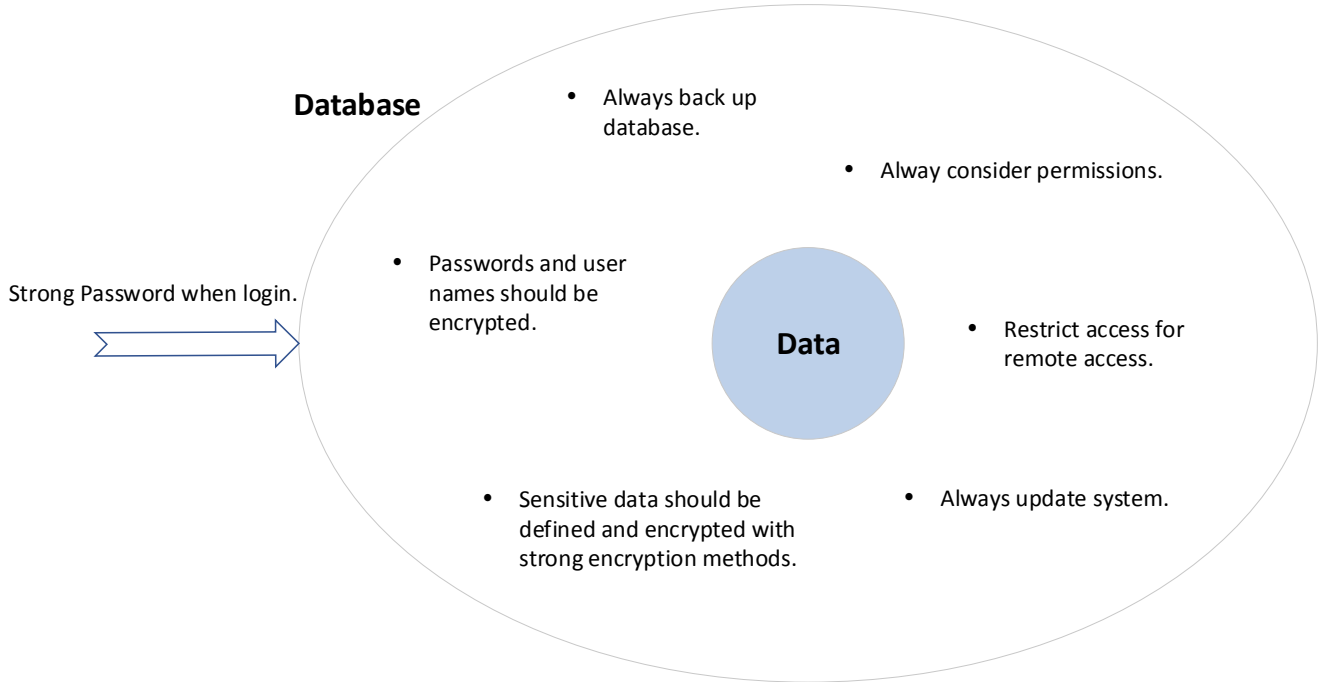

Figure 3 Cyber Defense Strategies

In this case, we applied encryption methods on sensitive data, i.e. the ECGs records. Table 1 listed the encryption methods that were applied on our database. MD5 [14] was used to encrypt login details against brute force attack. Besides, with strong password setting requirement, it becomes harder for the attacker to obtain login details. AES [14] method was used to encrypt ECGs records.

Table 1 Encryption methods and example code from our database.

MD5	INSERT INTO users (username, password) VALUES ('auser' ,'".md5('auserpassword')."');
AES	INSERT INTO `ecg_record_data` (`id`, `record_id`, `y-axis`) VALUES (AES_ENCRYPT ((1, 1, '-127 -162 -197 -229 -245 -254 -261 ….))

III. Results

A. The Ethical Hacking Results

Figure 4 shows the comparison results before and after Ethical Hacking Scenario 1 Brute Force. The ECGs has been modified and this affects the diagnosis of the heart diseases. In Figure 4, first record is original record and after ethical hacking methods second half of data was changed and this is shown in second diagram.

Figure 5 shows the comparison results before and after Ethical Hacking Scenario 2 – *SQL Injection*. The ECGs have been modified and this can affect the diagnosis of the heart diseases. In Figure 5, first record is original record and after ethical hacking methods data was changed and this is shown in second diagram.

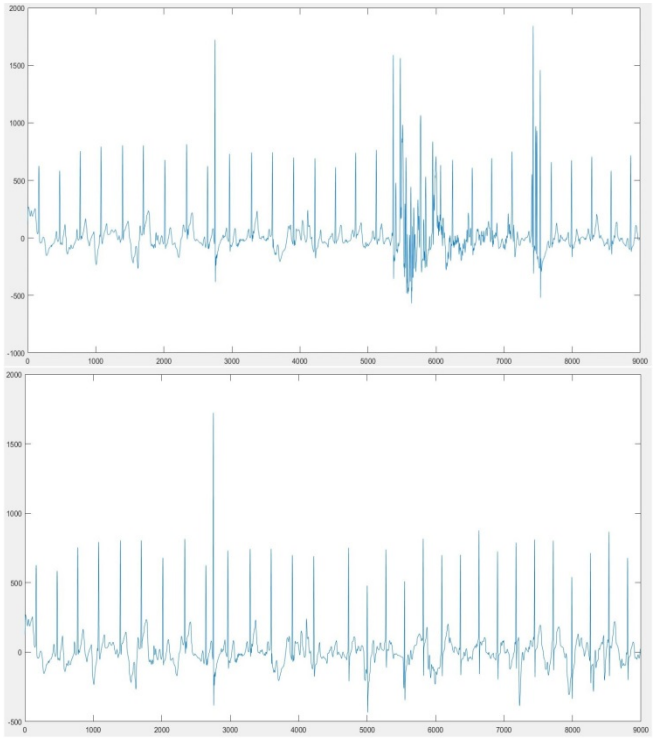

Figure 4: Comparison of ECGs before and after Hacking Scenario 1 - *Brute Force*

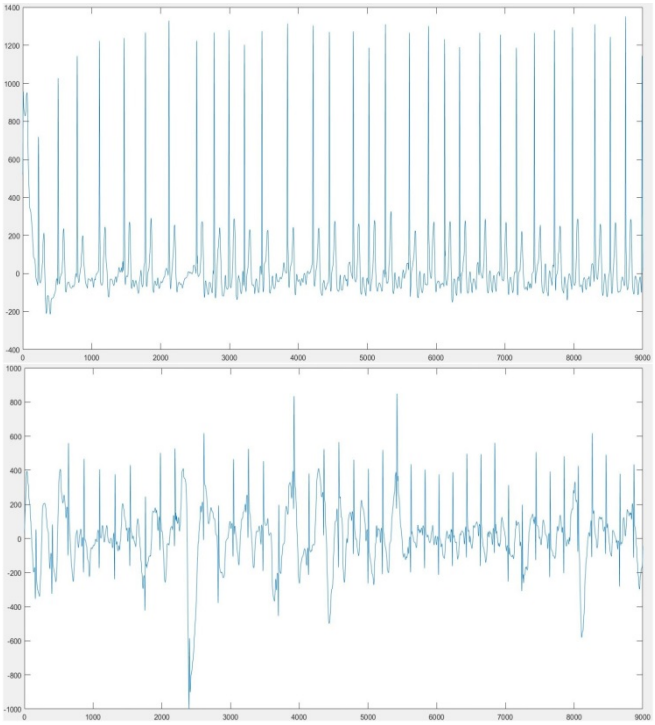

Figure 5: Comparison of ECGs before and after Ethical Hacking Scenario 2 – *SQL Injection*

B. After Applying Cyber Defense Strategies

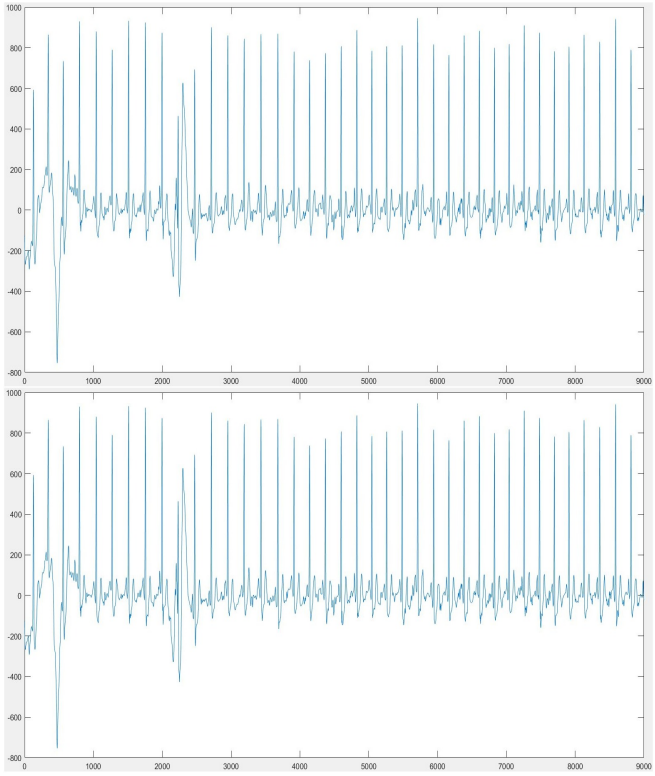

Figure 6: comparison hacking results before and after applying cyber security strategy

Figure 6 shows the comparison hacking results before and after applying cyber security strategy. After applying the MD5 and AES, the two hacking scenarios failed, meaning our cyber security strategies are effective in counteracting Brute Force and SQL Injection attacks.

IV. Discussion and Conclusion

In the present study, we (1) demonstrated how the IMDS diagnosis results can be compromised, (2) presented a set of cyber security strategies specifically tailored to IMDS to prevent such compromise and (3) evaluated our proposed strategies by comparing the results before and after applying the strategies.

This study provides novel insights into the protection of IMDS and concluded that our tailored cyber defense strategies can protect IMDS from being compromised by brute force and SQL injection attacks. From a security defense perspective, future work will consider applying advanced pentration testing methods towards IMDS and their associated defense strategies. From a medical diagnostics perspective, future work will consider using a more mature IMDS, such as the arrhythmia detection and classification in ambulatory ECGs proposed by Andrew Y. Ng [15]. Future work will also focus on expanding the data set to include data collected from different medical devices such as MCG and MRI.

Acknowledgment

The authors thank Prof. Henggui Zhang and Prof. Kuanquan Wang for useful discussions.

References

[1] Ronquillo, Jay G., et al. "Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information." JAMIA Open 1.1 (2018): 15-19.

[2] Ransford, Benjamin, et al. "Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance." (2012).

[3] Wirth, Axel. "Cybercrimes pose growing threat to medical devices." Biomedical instrumentation & technology 45.1 (2011): 26-34.

[4] Zhang, Meng, Anand Raghunathan, and Niraj K. Jha. "Trustworthiness of medical devices and body area networks." Proceedings of the IEEE 102.8 (2014): 1174-1188

[5] McMahon, Emma, et al. "Assessing medical device vulnerabilities on the Internet of Things." 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, 2017

[6] Khera, Mandeep. "Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications." Journal of diabetes science and technology 11.2 (2017): 207-212.

[7] Zheng, Guanglou, et al. "Ideas and challenges for securing wireless implantable medical devices: A review." IEEE Sensors Journal 17.3 (2017): 562-576.

[8] Sametinger, Johannes, et al. "Security challenges for medical devices." Commun. ACM 58.4 (2015): 74-82.

[9] Sandler, Karen, et al. "Killed by code: Software transparency in implantable medical devices." Software Freedom Law Center (2010): 308-319.

[10] Kobes, Shelby David. "Security implications of implantable medical devices." (2014).

[11] Scarfone, Karen, et al. "Technical guide to information security testing and assessment." NIST Special Publication 800.115 (2008): 2-25.

[12] Heule, Marijn JH, and Oliver Kullmann. "The science of brute force." The Best Writing on Mathematics 2018 7 (2018): 46.

[13] Alwan, Zainab S., and Manal F. Younis. "Detection and Prevention of SQL Injection Attack: A Survey." vol 6 (2017): 5-17.

[14] Kumari, Shruti, and Gautam Kumar. "Comparison of AES and DES Algorithm." IITM Journal of Management and IT 6.1 (2015): 144-146.

[15] Awni Y. Hannun, Pranav Rajpurkar, Masoumeh Haghpanahi, Geoffrey H. Tison, Codie Bourn, Mintu P. Turakhia, andAndrew Y. Ng. "Cardiologist-level arrhythmia detection and classification in ambulatory electrocardiograms using a deep neural network." Nature Medicine 25 (2019): 65-69