Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)

doi:10.3233/APC210259

Threat Model for Secure Health Care Data Using EMR, EHR and Health Monitoring Devices

Ms. RA. Kamalaeswari [a,1], Dr. V. Ceronmani Sharmila [b]
[a]*PG Student, Department of Information Technology, Hindustan Institute of Technology and Science, Chennai, TN, India*
[b]*Professor and Head, Department of Information Technology, Chennai, TN, India*

Abstract. The main aim of this project is to propose a threat modeling framework that promotes the security of health care services. The threat model is used to analyze the cyber threats that makes the electronic health monitoring devices vulnerable to a cyber-attack. The model also helps in strengthening the security of the software-based web applications like EMR and EHR used in a health care organization. The information assets are identified and the threat agents are eliminated considering the software, web application and monitoring devices as attack surface. The major goal of this threat model is to analyze and establish the trust boundaries in the OpenEMR that render a secure data transmission. We use a STRIDE threat model and a DFD based approach using the OWASP threat modeling tool. The SIEM tools provide a continuous security methodology to document the process and result.

Keywords. Threat model, cyber-attack, EMR, EHR, information asset, threat agents, attack surface, OpenEMR, STRIDE, DFD, SIEM.

1. Introduction

Medicine may be defined as the most important part of the human life. Even though the field of medicine involves the interaction purely with the human body and organs, there are situation where we integrate the advancements of technology to interpret the working of human body. So, we use electronic health monitoring devices which provides the doctors with data regarding a particular organ or organs of the human body.

A Healthcare organization uses software and web application to collectively maintain the patient and hospital data. The commonly used software is EMR and EHR. The EHR run like any other software based on web application including both front-end and back-end.

[1]RA.Kamalaeswari, Department of Information Technology, Hindustan Institute of Technology and Science, TN, India; Email: kamaliraghu98@gmail.com.

Electronic medical records (EMRs) are an advanced form of the paper diagrams in the doctor's office. An EMR provides the hospital visit and treatment history of the patients in a single practice.[1] EMRs have benefits over paper storage. For instance, EMRs permit doctors to:

- Track information of all the patient history and conditions.
- Effectively recognize which patients are expected for screenings or tests
- Check how their patients are getting along on specific boundaries, for example, pulse readings or inoculations.

2. Working of the model

Professionals in medical field use EMRs for data storing, processing and retrieving due to their user-friendly nature and customization options. We in this project will use one of these widely used framework called as OpenEMR, which requires a web server and data base server to function in optimization. We store and manage clinic related sensitive information inside the EMRs [2]. Threat model is the security cycle by which we can recognize, sort, and investigate dangers. A threat model incorporates:

- A plan (graph) of the framework
- A procedure that incorporates a rundown of suspicions that can be checked. A portion of the mainstream systems are STRIDE, PASTA, TRIKE, and VAST.
- A rundown of threats and controls for alleviation.
- An approach to approve the model, vulnerabilities and check of accomplishment of the activities taken.

2.1. Methodology

STRIDE represents Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Escalation of Privilege. These are against security functionalities like Authentication, Integrity, Confidentiality, Non-Repudiation, Authorization and Availability of the data [8-10]. The three main goals of this threat model are to assess:

- Ability to understand the system proposed, which in our case is OpenEMR.
- Find the potential vulnerabilities.
- Prioritize these vulnerabilities and eliminate them respectively

The threat model is created by first defining a template workflow of the events in the proposed system. The threat stencils are determined and categorized. The threat is defined using properties as we identify and prioritize them. The workflow template as shown in Figure 1, is created which defines the critical information assets, data flow, user roles, user privileges, escalated privileges, attack surface and trust boundaries.

Figure 1. Open EMR login through local host and database.

2.2. Process and threat flow

The OpenEMR consists of various modules which help in executing each functionality according to the patient and clinic needs is shown in Figure 2. The addition of patients, billing, payments, electronic health reports, lab documents, procedure recordings, care coordination, patient validation, prescription of medicine and symptoms are all stored in the database. The clinical plans, rules and drug inventory are monitored using the interface. All the data specified are critical assets of the system and define the data flow within the system. The database and the user credentials are vulnerable attack surfaces.

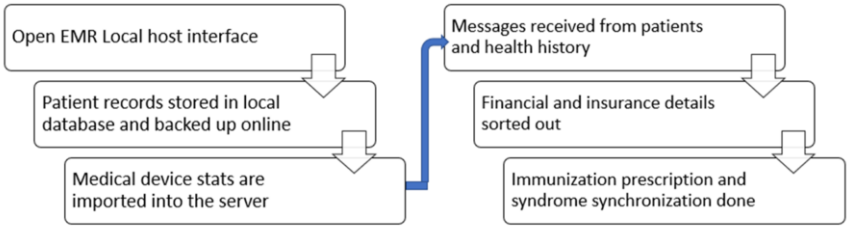

Figure 2. Open Emr process flow

The critical information assets of the system proposed can be physical and logical. The hospital data contains most of the physical information about the patient which is highly confidential. The health data about a person can be used against them in various ways. In order to avoid all the potential threat factors from inside the organization we must identify the bad actors and the attack surface is given in Table 1. The bad actors contribute to most of the insider threats.

Table 1. Threat properties

Attack surfaces	**Insider threats**
Local host	Database flaws
Database	Pharmacist
Patient records	Doctor
Billing checkouts	Lab technician

Lab Documents	Patient
Electronic device	Billing accountant
Electronic Reports	External drug vendor

3. Related works

The medical care industry is highly considered by hackers more so than some other area at recent times. The internet that is being utilized in the medical services is one of the primary stores to acquire data from. Many researches have been made regarding the working and security of these EMRs. We have considered few of those studies as references in our project. The threat model is given in Figure 3.

a) The workflow of the data processing, mining inside an open source EMR is described in depth in this work. Various data algorithms are used in fetching the correct data regarding the patient medical treatment history. Conformance checking is the methodology used here. The building of user roles inside the software is determined and hence the understanding of the work done here can be used to prevent the escalation of privilege and access control issues.[3]

b) The second work showcased deploys more security in the EMR by deploying block chain technology. The authentication and integrity of the data is hence preserved. The security and transparency amongst the network nodes are also regulated for clear communications. The data stored is hashed and encrypted in order for more security. A reminder system is added in the set up to manage the time schedule of the patients.[4]

c)This thesis is part of the Arizona Center for Accelerated Biomedical Innovation's ongoing health analytics research and development programme. They use big data technology to improve the experience of both patient and doctor when it comes to EHR. The video and audio of patient visit along with the clinical measurements are recorded with the patient's consent. Even though this provides a better and clear methodology, this contains all the highly sensitive data but also most vulnerable to cyber threats.[5]

d) In this thesis the management of a secure hospital cyber space by the Dubai hospitals are analyzed and defined. The users present inside the hospital environment and their perception of the data security is questioned and researched. This was implied as a overall case study of data privacy inside the hospital and how the patient information is vulnerable to an unintentional insider attack.[6]

e) According to General data protection regulation all the highly sensitive and personal data of both patient and doctor must be secured. This work implies various cryptographic and data analysis algorithms to generate private keys and protecting the data. The cryptographic keys are also used for storage and transmission of data.[7]

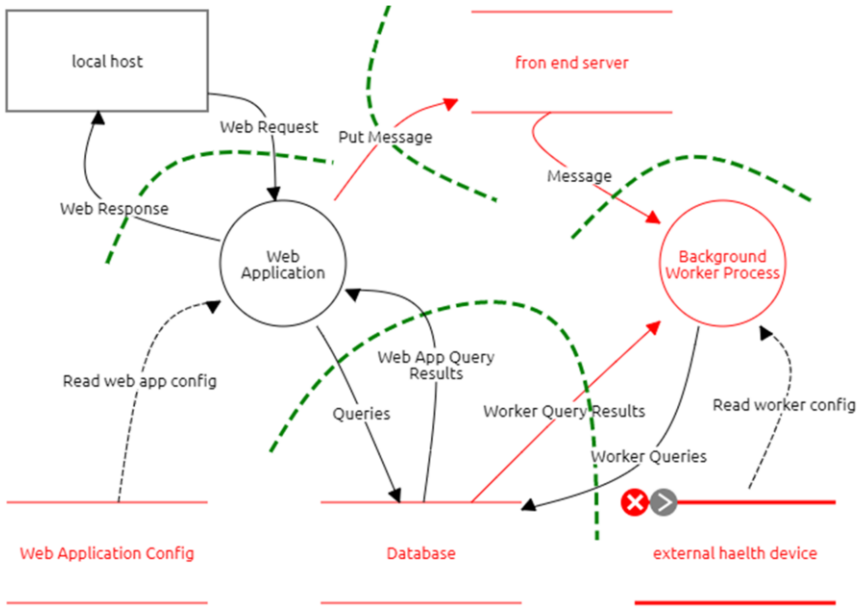

Figure 3. Threat model

4. Conclusion

The medical care industry is highly considered by hackers more so than some other area at recent times. The internet that is being utilized in the medical services is one of the primary stores to acquire data from. Many researches have been made regarding the working and security of these EMRs. We have considered few of those studies as references in our project.

References

[1] Akowuah, F., Lake, J., Yuan, X., Nuakoh, E., & Yu, H. (2015). Testing the security vulnerabilities of OpenEMR 4.1.1: A case study. *Journal of Computing Sciences in Colleges*, *30*(3), 26–35.

[2] Agbele, K. K., Oriogun, P. K., Seluwa, A. G., & Aruleba, K. D. (2016). Towards a model for enhancing ICT4 development and information security in healthcare system. In *International Symposium on Technology and Society, Proceedings* (Vol. 2016-March). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ISTAS.2015.7439404

[3] Asare, E., Wang, L., & Fang, X. (2020). Conformance Checking: Workflow of Hospitals and Workflow of Open-Source EMRs. *IEEE Access*, *8*, 139546–139566. https://doi.org/10.1109/ACCESS.2020.3012147

[4] Sheela, K., & Priya, C. (2020). Enabling the efficiency of Blockchain Technology in Tele-Healthcare with Enhanced EMR. In *2020 International Conference on Computer Science, Engineering and Applications, ICCSEA 2020*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCSEA49143.2020.9132922

[5] Rahman, A., Mitra, A., Rahman, F., & Slepian, M. J. (2019). Smart EHR-A Big-Data Approach to Automated Collection and Processing of Multi-Modal Health Signals in a Doctor-patient Encounter. In *Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019* (pp. 6198–6200). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/BigData47090.2019.9006574

[6] Bakkar, M., & Alazab, A. (2019). Information security: Definitions, threats and management in dubai hospitals context. In *Proceedings - 2019 Cybersecurity and Cyberforensics Conference, CCC 2019*

(pp. 152–159). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CCC.2019.00010

[7] Park, H. A. (2019). Secure electronic medical record (EMR) system. In *Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019* (pp. 955–960). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CSCI49370.2019.0018

[8] R. G. Babu, A. Nedumaran and A. Sisay, "Machine Learning in IoT Security Performance Analysis of Outage Probability of link selection for Cognitive Networks," *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2019, pp. 15-19, https://doi.org/10.1109/I-SMAC47947.2019.9032669

[9] Markkandan, S., Malarvizhi, C., Raja, L., Kalloor, J., Karthi, J., & Atla, R. (2021), "Highly compact sized circular microstrip patch antenna with partial ground for biomedical applications", Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.04.480

[10] R. G. Babu, V. V. Nathan, J. Bino, C. Amali and S. Ganesh, "IoT Security Enhancement with Automated Identification Device using IOT SENTINEL," 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2021, pp. 518-523, https://doi.org/10.1109/Confluence51648.2021.9377165