Perspectives

Perspectives of Threat Modeling of a Secure Cloud Picture Archiving and Communication System

Jinmisayo A. Awokola
Department of Computer Science and Engineering,
Ladoke Akintola University of Technology,
Ogbomoso, Nigeria
rhgonline@gmail.com

Ozichi N. Emuoyibofarhe
Department of Computer Science,
Bowen University,
Iwo, Nigeria
eozichi@yahoo.com

Adebayo Omotosho
Landmark University,
Omu-Aran,
Nigeria
bayotosho@gmail.com

Justice O. Emuoyibofarhe
Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
eojustice@gmail.com

Jacob O. Mebawondu
Department of Computer Science,
The Federal Polytechnic,
Nasarawa, Nigeria
mebawondu1010@gmail.com

Abstract—**The Picture Archiving and Communication System (PACS) used in electronic health, is computationally enhanced by the migration into the cloud, which reduces the cost of storage space and equipment. However, cloud-PACS technology is susceptible to threats and vulnerabilities. This paper implements a threat modeling approach on a cloud-PACS framework, using Microsoft Threat Modelling Tools. Security requirements and mitigation strategies were formulated for the implementation of the framework, in order to improve cloud PACS security.**

Keywords-Picture Archiving and Communication (PAC); e-health; modeling; threat; cloud

I. INTRODUCTION

Picture Archiving and Communication System (PACS) has been deployed in health informatics due to the need to retrieve, capture and archive images, from different image modalities [1]. However, the rapid increase in volume and required speed of medical images has necessitated the need for acquiring high-performance, grid-based hardware and software, increasing PACS' management cost. Cloud computing technology has been proposed to provide a cost-effective approach for storage [3]. However, this resulted in several security vulnerabilities and loopholes. This, therefore, motivated the need for studies focusing on the development and implementation of different cloud-based security frameworks, in order to bridge the gap [4]. Threat modeling is a quintessential software engineering methodology for security-compromisable systems [5]. It integrates goal and risk modeling methodologies, for any technology of interest [6]. This makes it possible to specify threat requirements, prior to the development of a security framework. However, the majority of existing studies did not focus on this aspect during the security framework development of cloud PACS. Therefore, there is a need to adapt threat modeling techniques, in order to ensure a secured cloud PACS. Threat modeling parameters are based on different cyber-security indices. In the threat framework presented in [7], the essential parameters for simulation are strength, threat capability, contact frequency, and vulnerability. The strength of a hypothetical security-compromisable system describes the level at which it can resist a malicious attack, whereas the threat capability denotes the level of the hacking that can deplete the strength of the system. Contact frequency describes the rate at which the hacker interfaces with the system, while vulnerability denotes the rate of successful attacks initiated by an alleged intruder. Threat modeling has been applied in sensitive utility areas, such as the Smart Electricity Metering System (SEMS), because of some inherent security issues [8]. SEMS is the current trend because it provides a cost-effective approach to billing and utilization of energy. However, different threat modeling methodologies, such as STRIDE and DREAD, were employed for the essential threat requirement elicitation and identification. STRIDE acronym represents Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege, whereas DREAD denotes Damage, Reproducibility, Exploitability, Affected users and Discoverability [9]. Based on the identified threats, a security software imitating SEMS was developed, as a proof of concept. Consequently, adoption of SEMS will be higher if security is guaranteed optimally. Additionally, it has been shown that threat modeling is very applicable to mobile and desktop e-health systems, due to the confidentiality requirements [10]. However, there is a lack of threat modeling studies on cloud PACS, although similar confidentiality requirements also exist.

Corresponding author: Adebayo Omotosho

II. METHODOLOGY

A cloud-based PACS framework was designed, with features that allow images to be captured and stored in cloud storage platforms. The proposed framework is fully described in [11]. The framework, embedding security features, takes care of medical images and their transmission through internet, until they are finally rested in the cloud, allowing access to every authorized user. Microsoft Threat Modelling Tool was used in order to analyze the cloud-PACS framework and identify points of vulnerabilities that could compromise the system, in terms of entry and exit points. All possible external dependencies, such as trust levels as well as entry and exit points to the system were identified. Possible threats were identified and analyzed using STRIDE. Also, threats were ranked using the DREAD model classifier, by scaling its individual components from 1 to 10, which were summed up and divided by 5 in order to obtain a final threat value. Threat values were ranked as Low (1–3), Medium (4–6) and High (7–10). Threats ranked as High were given utmost attention. At the end, possible mitigation strategies were proposed towards the final implementation, so that the resulting system would be able to achieve an optimum security level.

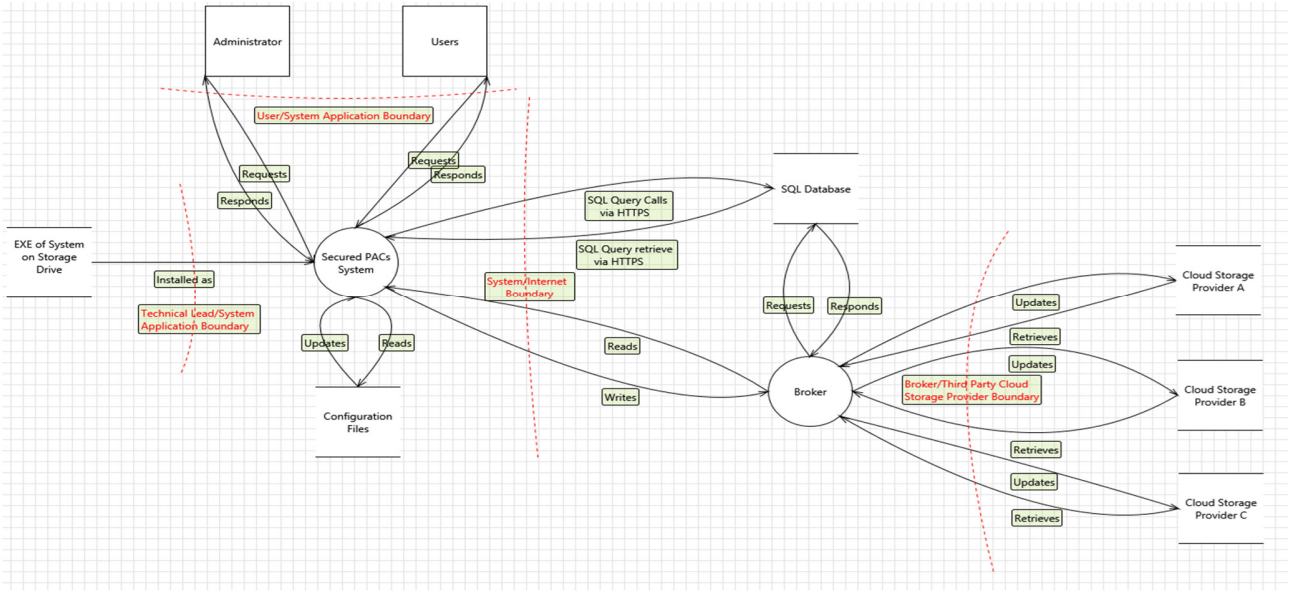

Fig. 1. Dataflow diagram for the Cloud PACS Framework

TABLE I. SYSTEM'S THREAT ANALYSIS BASED ON THE STRIDE APPROACH

System's threats identification			
Id	**Threat type**	**Susceptible asset(s)**	**Threats**
1.	Spoofing	Administrator/Technical lead/Users' login details, Technical lead's credentials, Personal, Meta and Pixel Data	1. Attacker aims to log into the PACS or server-based components with valid user's privileges 2. Attacker aims to retrieve meta and pixel data from the cloud storage provider.
2.	Tampering	The PAC System Users, Administrator and Technical Lead Credentials	3. Attacker aims to tamper configuration files rendering the PAC system unavailable. 4. Attacker aims to alter PACS' data in transit. 5. Attacker aims to modify user credentials so as to make user's authentication impossible.
3	Repudiation	Meta and Pixel Data	6. Attacker is a valid user who aims to perform unauthorized actions unnoticed. 7. Attacker aims to gain access to the PACS and/or its database so as to make illicit changes.
4.	Information Disclosure	Administrator/Technical lead/Users' login details, Technical Lead's credentials, Personal, Meta and Pixel Data	8. Attacker aims to intercept user's credentials and personal details, transmitted through Internet. 9. Attacker aims to intercept meta and pixel data as they travel through the cloud storage provider's infrastructure, the web server and the PACS.
5.	Denial of Service	The PAC system The Internet Server-Based Database. The Internet Server-Based Broker.	10. Attacker aims to tamper system's files in order to reduce functionality. 11. Attacker aims to tamper system's database files in order to reduce functionality of the PAC application, such as authentication. This can also lead to a failed interaction with the broker.
6.	Elevation of Privileges	The PAC System	12. Attacker aims to gain unauthorized privileges in order to compromise the PAC system. Attacker could be a valid user.

TABLE II. SYSTEM'S THREAT RANKING BASED ON THE DREAD APPROACH

Identified Threats	D	R	E	A	D	Total	Threat Rating
Attacker aims to log into the PACS or server-based components with valid users' privileges.	6	6	4	9	9	6.8	**Medium**
Attacker aims to retrieve meta and pixel data from the cloud storage provider.	10	3	9	10	9	8.2	**High**
Attacker aims to tamper configuration files making the system unavailable.	2	4	5	1	6	3.6	**Low**
Attacker attempts to alter PACS' data in transit.	7	2	9	3	4	5	**Medium**
Attacker aims to modify user's credentials so as to make user's authentication impossible.	7	4	8	9	3	6.2	**Medium**
Attacker is a valid user who aims to perform unauthorized actions unnoticed.	6	4	9	4	6	5.8	**Medium**
Attacker aims to gain access to the PACS and/or its database so as to make illicit changes.	8	5	8	7	7	7	**High**
Attacker aims to intercept user's credentials and personal details transmitted through Internet.	6	3	8	6	7	6	**Medium**
Attacker aims to intercept meta and pixel data as they travel through cloud storage provider's infrastructure, the web server and the PACS.	6	3	8	6	7	6	**Medium**
Attacker aims to tamper system's files in order to reduce PACS' functionality, such as authentication. This can also lead to a failed interaction with the broker.	6	4	9	6	7	6.4	**Medium**
Attacker aims to gain unauthorized privileges in order to compromise PACS. The attacker could be a valid user.	10	7	6	6	9	7.6	**High**

TABLE III. SYSTEM'S THREAT MITIGATION STRATEGIES TABLE

Identified threats	Threat mitigation strategies
Attacker aims to log into the secured PACs system or server-based components with valid user's privileges.	All system's users are authenticated with Internet database server for the validity of their credentials.
An attacker aims to retrieve meta and pixel data from the cloud storage provider.	1. Meta and pixel data are distributed, so they are not useful if found in parts. 2. Retrieved metadata are obfuscated and can only be deobfuscated by valid users.
Attacker aims to tamper configuration files rendering the PAC system unavailable	Directory of the configuration files is accessible and modifiable only by the system's administrator.
Attacker attempts aims to alter PACS' data in transit.	Communication is made through encrypted TLP/SSL Internet protocol which is relatively tamper-resistant.
Attacker aims to modify user's credentials, so as to make future authentication impossible.	User's authentication and authorization are checked before any changes can be made.
Attacker is a valid user who aims to perform unauthorized actions unnoticed.	Every action inside the system is logged.
Attacker aims to gain access to the PACS and/or its database so as to make illicit changes.	User's authentication and authorization is checked before any change occures.
Attacker aims to intercept users's credentials and personal details transmitted through Internet.	Communication is made through the encrypted TLP/SSL Internet protocol which is relatively tamper-resistant.
Attacker aims to intercept meta and pixel data as they travel through the cloud storage provider's infrastructure, the web server and the PACS.	Communication is made through the encrypted TLP/SSL Internet protocol which is relatively tamper-resistant.
Attacker aims to tamper system's files in order to reduce PACS' functionality, such as authentication. This can also lead to a failed interaction with the broker.	1. Database is located in a firewall secured Internet server. 2. Parameters inserted into forms are validated before processing, so as to avoid vulnerabilities like SQL injection.
Attacker aims to gain unauthorized privileges in order to compromise PACS. The attacker could be a valid user.	Authorization check before making privileges accessible to users.

III. RESULTS AND DISCUSSION

Table I shows the identified threats for a typical cloud-PACS system prototype using the STRIDE approach. Assets at risk such as PACS, database hosted on an Internet Server, broker, system user's details, meta, pixel, and personal data, in a cloud-PACS system, are the major concerns of interest during the threat modeling pipeline. Table II shows the threat ranking, performed by the DREAD classifier approach. Threats identified by STRIDE methodology, were inputs into the DREAD threat classifier. Risks ranked as "High" were given the highest attention during the implementation of the cloud-PACS security framework, followed by the "Medium" and "Low" respectively. Table III shows different threat mitigation strategies to deploy during the implementation of the proposed cloud-PACS framework. The proposed framework is designed based on a security manager middleware, which comprises of components such as the obfuscator, cloud service broker, firewall, gateway, account and preference manager. Figure 1 shows the detailed data flow diagram of the proposed framework, showing interaction details within the system, based on the threat modeling approach.

IV. CONCLUSION

Security is an essential factor in modern computer systems used in banking, health, schools and so on. It ensures that only authenticated and authorized individuals can use a system and term generally encompasses authentication, confidentiality, and integrity [12-14]. Cloud-based systems can easily be compromised by malicious insiders or users, if the system cannot maintain continuously a certain level of integrity. This work used a threat modelling approach to identify possible threats to a Cloud PACS, as well as elicit threat mitigation strategies for identified and classified threat rankings using STRIDE and DREAD approaches. Results from this threat modeling study will improve cloud-PACS' usability and security, and ultimately enhancing its adoption.

REFERENCES

[1] K. A. Kurlakose, Infrastructure for secure medical image sharing between distributed PACS and DI-r systems, Msc Thesis, University of Ontario, 2013

[2] R. K. Grace, R. Manimegalai, S. S. Kumar, "Medical image retrieval system in grid using hadoop framework", International Conference on Computational Science and Computational Intelligence, Las Vegas, USA, March 9-12, 2014

[3] C. Stergiou, K. E. Psannis, B. G. Kim, B. Gupta, "Secure integration of IoT and cloud computing", Future Generation Computer Systems, Vol. 78, No. 3, pp. 964-975, 2018

[4] S. K. Vuppala, M. S. Dinesh, S. Viswanathan, G. Ramachandran, N. Bussa, M. Geetha, "Cloud-based big data platform for image analytics", IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, November 1–3, 2017

[5] P. H. Meland, E. Paja, E. A. Gjaere, S. Paul, F. Dalpiaz, P. Giorgini, "Threat analysis in goal-oriented security requirements modelling", International Journal of Secure Systems and Software Engineering, Vol. 5, No. 2, pp. 1-19, 2018

[6] L. Sion, K. Yskout, D. Van Landuyt, W. Joosen, "Poster: Knowledge-enriched security and privacy threat modelling", 40th International Conference on Software Engineering: Companion, Gothenburg, Sweden, May 27-June 03, 2018

[7] J. Freund, J. Jones, Measuring and managing information risk: a FAIR approach, Butterworth-Heinemann, 2018

[8] S. Cleemput, Secure and privacy-friendly smart electricity metering, PhD Thesis, Arenberg Doctoral School, 2018

[9] Microsoft, "Microsoft Threat Modelling Tool 2016", available at: www.aka.ms/tmt2016

[10] M. Cagnazzo, M. Hertlein, T. Holz, N. Pohlmann, "Threat modelling for mobile health systems", IEEE Communications and Networking Conference, Barcelona, Spain, April 15–18, 2018

[11] A. Omotosho, J. A. Awokola, O. J. Emuoyibofarhe, C. Meinel, "A secure cloud-based picture archiving and communication system for developing countries", Journal of Theoretical and Applied Information Technology, Vol. 97, No. 7, pp. 1902-1913 2019

[12] A. Omotosho, J. Emuoyibofarhe, "A criticism of the current security, privacy and accountability issues in electronic health records", International Journal of Applied Information Systems, Vol. 7, No. 8, pp. 11–18, 2014

[13] A. Omotosho, J. Emuoyibofarhe, C. Meinel, "Ensuring patients' privacy in a cryptographic-based-electronic health record using bio-cryptography", International Journal of Electronic Healthcare, Vol. 9, No. 4, pp. 227-254, 2017

[14] A. Omotosho, J. Emuoyibofarhe, A. Oke, "Securing private keys in electronic health records using session-based hierarchical key encryption", Journal of Applied Security Research, Vol. 12, No. 4, pp. 463-477, 2017