Implementation of Square Methods in Analyzing the Security of an Application System

Suhaemi[1], H Permana[1], A Sunarto[1], D Murtiningsih[2], D Napitupulu[1,3], R Rahim[4]
{suhaemi.emi@gmail.com, hadipermana@gmail.com, arriyadi.chrisanty@gmail.com, dewi.murtiningsih@budiluhur.ac.id, darwan.na70@gmail.com, usurobbi85@zoho.com }

[1]Pasca Sarjana, Universitas Budi Luhur, Jl. Ciledug Raya, Jakarta, Indonesia
[2]Fakultas Ekonomi dan Bisnis, Universitas Budi Luhur, Jl. Ciledug Raya, Jakarta, Indonesia
[3]Research Center for Quality System & Testing Technology, Indonesian Institute of Sciences, Tangsel, Indonesia
[4]School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia

Abstract: An application system connected to a computer network connection and connected to the internet should be concerned about its security issues. Security aspects of an application system such as secured confidentiality, integrity, and availability of data and information stored and processed in an application system is very important to maintain the smooth running of an information system. Therefore, an application system firstly should be analysed its security system for the application system could run well without any threats that interfere with the process of a system. In this review paper, the method used to analyze the security needs of an application system is using square method (System Quality Requirements Engineering). This method consists of nine stages developed for helping to analyze security needs.

Keywords: Square Method, Security, System, Application, Review.

1. Introduction

One Security in an application system is absolutely necessary to maintain stability and maintain data integrity in the system. Security problems that arise when an application is connected to a computer network and connected to the internet then, which must be considered first is its security. SQUARE is one method of analysis of information security requirements that can be used to determine security needs in an application system. Many methods can be used to help analyze these security needs, one of which is the Square methodology. The square methodology was studied and developed by the Carnegie Mellon Software Engineering Institute.

When studying software engineering requirements documents often find a separate section of generic generated security requirements. Tendency requirements that are documented are common such as password protection, firewalls, virus detection and the like. Eligibility and analysis requirements that are needed to get a better set of security needs are very rare. Even when it exists, the ten requirements are developed separately from the rest of the engineering activities and are not integrated with the main activities of the engineering process. As a result, security requirements specific to those providing service and asset protection are often ignored. According to Curtis Coleman, the high vulnerability to a large company that has a wide network is the application. Security is mostly focused on antivirus and network security, but a very important part of business transactions is the application and the main data (Sandy, M., 2016). The abundance of application developers who ignore the

ICASI 2019, July 18-19, Banda Aceh, Indonesia

DOI 10.4108/eai.18-7-2019.2288579

importance of security analysis needs before doing software engineering becomes ironic in this era of technology so rapidly (Fahmi, I.et al, 2016).

The development of information technology at the present time has increased so fast, along with the development of many emerging applications, gadgets and latest framework that supports the progress of information technology (Napitupulu, 2016; Rachman, T., and Napitupulu, 2018). But on the one hand with the development of information technology there are good and bad things, if viewed from the good side of information technology has a lot of help the company's performance, and on the bad side of information technology many are abused (Napitupulu, et al., 2018; Sensuse, et al., 2017). Some cases that occur due to advances in information technology that is able to hack the site, steal permissions legal users, stealing data and information of an important nature, deface or change the look of the official website in order to commit fraud that may result in the loss of some parties. One of the advances in information technology in terms of internet network is wireless, or often also called Wi-Fi. As we know wireless is a medium / means to connect the internet without using a cable, a lot of companies, universities and government agencies at this time using wireless hotspot for internet network, but cannot be denied a lot of abuse on wireless network spot systems such as theft of information and data and hacking process through wireless technology. Actions by illegal users in wireless networks usually steal legal user login data by using special tools, randomizing user login and even logging into wireless network. Some of the attacks that can occur on the system:

- Denial of Service (DoS), the type of attack on a computer or server in the Internet network by spending resources owned by the computer until the computer cannot perform its function properly so that indirectly prevent other users to gain access to services of the computer being attacked.
- Distributed DoS (DDoS), a type of Denial of Service attack that uses multiple attack hosts (either using a dedicated computer to attack or a "forced" computer into a zombie) to attack a target host within a network.
- SQL Injection Attack, in this attack the object being attacked is a web page that uses Structured Query Language (SQL) to query and manipulate the database.
- Password Attack, an attack to crack a password.
- Key logger, software for recording keyboard keystrokes

2. Research Methodology

Based on literature studies conducted on the security system especially square method. There are 5 (five) literature found related to stages of square implementation, namely; (1) (Sandy et al., 2016) conducted the research to analyses the security needs of information using Square method. (Sandy et al., 2016) stated that there are nine step or process for obtaining the needs of secure information system, (2) (Fahmi, et al., 2016) case study research PT. Tawada Healthcare in order to obtain security requirement for network and application using Square method, (3) (Yopi, 2015) evaluated the security of wireless network hotspot. According to (Yopi, 2015), there are also nine stages of stages in Square method, started with agree on definitions until requirements inspection, (4) (Helmiawan, 2018) studied the security of e-learning system using Square method. (Helmiawan, 2018) found nine step for implementing Square method in e-learning system and (5) (Syahrial, 2013) paper analyzed the requirement of system security for hospital information system-open source based using Square method. Even all literature seemly had the same number of stages in implementing Square method, the stage was different one another. For instance, (Syahrial, 2013) stated the first stage of Square

method was definition related to describe about the existing information system, meanwhile (Helmiawan, 2018) started with elicitation of system requirement in implementing Square method. Therefore, we need synthesize process to integrate those different process or stages. The entire study in this paper was taken from Google Scholar or Google Cendekia database especially publication of the last five years.

3. Result & Discussions

This This SQUARE is a model developed to predict a process of engineering requirements, tailored specifically to identifying security requirements. SQUARE is a means to generate, categorize priority security requirements for information technology and application facilities and infrastructure. In analyzing the security requirements of this application system often used the Square Method, the synthesize process result of stages of Square method consists of 9 stages of the process to help analyze security needs which explained in these folllowing stages.

3.1 Stage 1: Agree on Definition

Describes the applications to be engineered and define and agree on the terms of information security for the applications to be analyzed. More infrmation will be explained in table 1 as follows:

Table 1. Agree on Definition.

Multiple definitions of attacks on the system: a. Denail of Service (DoS), the type of attack on a computer or server in the Internet network by spending resources (resources) owned by the computer until the computer cannot perform its function properly so that indirectly prevent other users to gain access to services of the computer being attacked. b. Distributed DoS (DDoS), a type of Denial of Service attack that uses multiple attack hosts (either using a dedicated computer to attack or a "forced" computer into a zombie) to attack a target host within a network. c. SQL Injection Attack, in this attack the object being attacked is a web page that uses Structured Query Language (SQL) to query and manipulate the database. d. Password Attack, an attack to crack a password. e. Key logger, software to record keyboard keystrokes.

3.2 Stage 2: Identify Security Goals

Analyze the objectives and system security requirements required by the company to ensure overall security of its availability, more information are explained in this following table 2.

Table 2. Goal Identification.

Purpose:	a. Control system configuration and usage. b. Ensure the confidentiality, accuracy, and integrity of the data system. c. Guarantee system availability if needed

3.3 Stage 3: Develop Artifacts

Describe in detail the architecture of the application system being engineered.

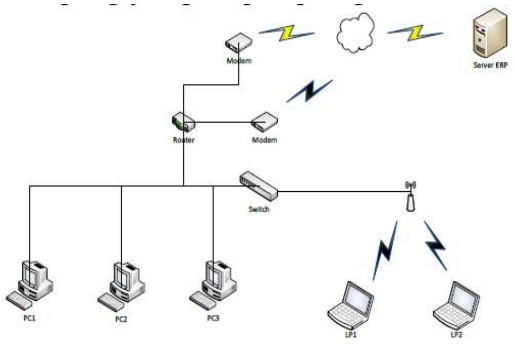

Fig. 1. Network Architecture.

3.4 Stage 4: Perform Risk Assessment

Conducting Risk Analysis Assessment qualitatively and gradually as following:

Table 3. Risk Assessment.

Possibility	Level
MC-01 Account Management Attacks	High
MC-02 Password Login Attack	Mid
MC-03 SQL Injection Attack	High
MC-04 Network Attack Wifi	High

3.5 Step 5: Select Elicitation Technique

Data collection related to the condition of the system thoroughly and comprehensively either through the method of observation use case analysis and literature study.

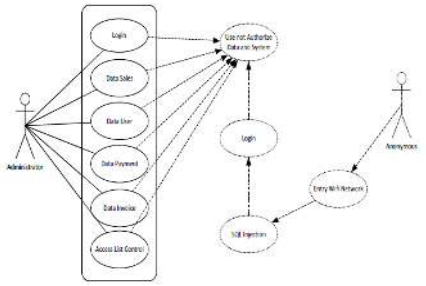

Fig. 2. Miss-Use case.

3.6 Stage 6: Elicit Security Requirement

Election elicitation techniques that is done by conducting interviews, questionnaires and observations related to the security opinion on the system. From the observation, use case analysis and literature study then made into the list of needs as described in this following table 4.

Table 4. Requirement Elicitation.

Requirement	Information
Architectural Recommendations (AR)	Firewall use

	Use of MAC Authentication Use of ACL Use of Encryption in the Information System
Policy Recommendations (PR)	Use of digital signatures for login system Use strong passwords Applications must be patched periodically Regular password change

3.7 Stage 7: Categorize Requirement

Make a detailed list of categorizations and recommendations on the architecture and policy requirements of implementing system security.

3.8 Stage 8: Prioritize Requirement

Create a list of architecture priorities and policy requirements for implementing system security.

Table 5. Requirement Priority

Threat *Likelihood*	D	R	E	A	D	Total	*Avarage*	Prioritas
MC 01	3	2	2	3	2	12	2.4	2
MC 02	2	1	2	3	2	10	2	4
MC 03	3	3	3	3	2	14	2.8	1
MC 04	2	2	2	3	3	12	2.4	3

3.9 Stage 9: Requirement Inspection

Creating a list of categories and providing detailed recommendations on the architecture and policy requirements of the security system implementation as well as the overall technical solutions that are then researched based on the priority level of the misuse case, which will provide all that is required in the implementation of the core components.

4. Conclusion

Based on the result of requirement engineering analysis, system improvement involving stakeholders has been able to meet the needs of users so that it can be used as a reference to design the improvement of this system in the future. Through this square method, it can be seen the part that has a security gap that can be entered by the user who is not responsible, so it can be anticipated.

Acknowledgements

We would like to thank the research institution that has supported the research activities was being carried out properly.

Reference

[1] Fahmi, I., Selviany, I., Indri, D., 2016. Analisa Kebutuhan Keamanan Sistem Jaringan

dan Aplikasi Dengan Metode Square Studi Kasus PT.Tawada Healthcare. *J. Sisfotek Glob.* 6(1).

[2] Helmiawan, M., 2018. Keamanan e-learning menggunakan metode square (studi kasus stmik sumedang. *Repos. STMIK Sumedang*.

[3] Napitupulu, D., Rahim, R., Abdullah, D., Setiawan, M I., Abdillah, L., Ahmar, A S., Simarmata, J., Hidayat, R., Nurdiyanto, H., Pranolo, A., 2018. Analysis of Student Satisfaction Toward Quality of Service Facility. *J. Phys. Conf. Ser* 954(1), 12019.

[4] Napitupulu, D., 2016. Evaluasi kualitas website uni- versitas xyz dengan pendekatan webqual [evalu- ation of xyz university website quality based on webqual approach]. *Bul. Pos dan Telekomun.* 14(1), 51–64.

[5] Rachman, T., and Napitupulu, D., 2018. User acceptance analysis of potato expert system application based on TAM approach. *Int. J. Adv. Sci. Eng. Inf. Technol* 8(1), 185–191.

[6] Sandy, M., and G.N., 2016. Analisis kebutuhan keamanan informasi menggunakan Metode square pada aplikasi remittance. *J. Ilm. Ilmu Komput.* 2(1).

[7] Sensuse, D I., and Napitupulu, D., 2017. The Study of User Acceptance Toward E-Learning System in Higher Education. *Int. J. Electr. Eng. Comput. Sci.* 7(2), 466–473.

[8] Syahrial, H., 2013. Analisis Kebutuhan Keamanan Sistem Dengan Menggunakan Metodologi SQUARE: Studi Kasus Pengembangan Sistem Informasi Rumah Sakit Berbasis Open Source ERP (Open Sikes)., in: *Seminar Nasional Teknologi Informasi & Komunikasi Terapan*. Universitas Budi Luhur.

[9] Yopi, A., 2015. Evaluasi keamanan jaringan wireless hotspot Menggunakan metode square (studi kasus warnet medianet sumedang). *Jur. Tek. Inform. Dosen STMIK Sumedang. Repos. STMIK Sumedang*.