Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 170 (2020) 923–928

Procedia Computer Science

www.elsevier.com/locate/procedia

The 10th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS 2020)
April 6-9, 2020, Warsaw, Poland

Classification of Logical Vulnerability Based on Group Attacking Method

Faisal Nabi* , Jianming Yong , Xiaohui Tao

University of Soutern Queensland, QLD4350, Australia

Abstract

New advancement in the field of e-commerce software technology has also brought many benefits, at the same time developing process always face different sort of problems from design phase to implement phase. Software faults and defects increases the issues of reliability and security, that's reason why a solution of this problem is required to fortify these issues. The paper addresses the problem associated with lack of clear component-based web application related classification of logical vulnerabilities through identifying Attack Group Method by categorizing two different types of vulnerabilities in component-based web applications. A new classification scheme of logical group attack method is proposed and developed by using a Posteriori Empirically methodology.

Keywords: Security Dimensions, CBS Application, Group Attack Method, Application logic, Attack Classification

* Corresponding author. Tel.: 61+0405265929; fax: +0-000-000-0000 .
E-mail address: faisal.nabi@yahoo.com

10.1016/j.procs.2020.03.109

1. Introduction

The growing complexity of modern e-commerce software based on component architecture is creating many benefits for e-commerce industry. However, at the same time critical process of different available commercial of the shelf components may cause of software application logic faults and defects during the plug and play phase of application new functionality development that increases the issues of reliability and security [3]. Therefore, an approach is required to classify the issues on the base of component-based software faults and flaws categorization scheme, which then classify each attack into group attack ID through attack method. The characterization of the attack method is based on vulnerability that may cause of fault logic into an application design. The design faults or flaws are system design phase issues those cannot be mitigate through modification of few lines of component code or interface connection code [10].The security of such problems are discussed through security dimension which reflects the system aspects and attributes. This may be affected by risk of loss in the event of cyber-attack through group attacking method. The security dimensions are divided into categories of problem where attacking method that may cause of logical vulnerability into a system. This help to the developers understand the design issues of security related system attributes. The security dimension is based on further attributes of the security system, such as security group knowledge, attack group knowledge, vulnerability category and attack boundary, and group attack method in system. These all attributes perform a major role in identifying and classifying the logical vulnerabilities based on group attack method. A group attack method explains the type of vulnerability and its attacking parameters that trigger an infected component in the case of particular event within the system. This process exploits the system security dimension. Therefore, such a scheme is needed to be developed that could characterize the two different vulnerabilities, logical and technical into groups and classification.

1.1. Objective

The research focuses the progress towards the highlighting different security dimensions of categorized vulnerability into classification of each attack with parameter that cause of triggering an exploitable event within the system. This will help to understand the further attributes of security dimension related to a system.

1.2 **Method**

Our research methodology focuses on a classification that separates or orders of main objects and specimens related to classes. The classifications can be derived by a priori or a Posteriori Empirically by considering the CVE vulnerability database for security breach cases [11].

2. Related work

Samaila te al .2017, classified the vulnerability into three units by intersection each of these three units: First Units is (i) a system's weakness that cause of a flaw, Second Units is (ii) Attacker approach of attack the flaw, and Third Units is (iii) Being able to exploit the Flaw by an attacker [1] but did not proposed any classification based on these three units or categorized them into attack cause.

Krsula, 1998, defined the classification of software vulnerabilities related issues which is based on fault that is in case of faults specification, development / configuration related to software. For example execution can violate clearly defined security policy [2]. This can be mitigated through the elimination of these problem in a numerous ways, such as software patches and re-configuring the devices [5]. Krsula; s classification is more likely about environmental fault which describes given below exampled figure of taxonomy of software. However, the shortcoming of his research is, proposed scheme limitation to the software fault related environmental condition.Joshi and Singh (2014) has proposed the classification five dimensional vector of vulnerability and defined the defense, method and its impact related to target attack [3]. However , his work most likely cover the network vulnerabilities , which shortfalls about design flaw in architecture of software base application in case of component-based development. Software vulnerability occurs due to the existence of software bugs, faults and errors which cause an unchecked buffer or race condition [4]. By the date now, there have been many different classification schemes [12, 13, 14, 15, 16] proposed targeting various parameters related to technology can affect the software production process specially in the phase of (SDLC), revelation process and attack pattern [6].

Modern classification of vulnerability models mostly targets the vent of software vulnerability, that is a single cause specially concentrate on domain specific application. It is also possible that a single vulnerability may not cause of a single reason [8]. Many different reasons can cause of a single vulnerability in a system [9]. Therefore, a single cause can be reason of different vulnerabilities in different sort of applications based on class of domain. So it is very much clear that such presentation does not classify the classification models in a holistic way or presentation. Moreover, present schemes do not provide any detail about logical vulnerability-based attack classification and group attack method. This paper covers the research gap between present classifications as stated in related work and the approach adopted in this paper "Classification of logical vulnerability "and group attack method.

3. Proposed Vulnerability Classification Model

The security dimensions are considered as aspects of system and attributes or related process that leaves its effects on security group to know system and delivers the changes to the system. This is based on understanding of the class of vulnerability and its category. The security dimensions directly impact on security group knowledge to evaluate the ussies related to the security in network or system. This can be both logically and technically, each aspect of both can be categorized and a classification is given before mitigating the security issues.

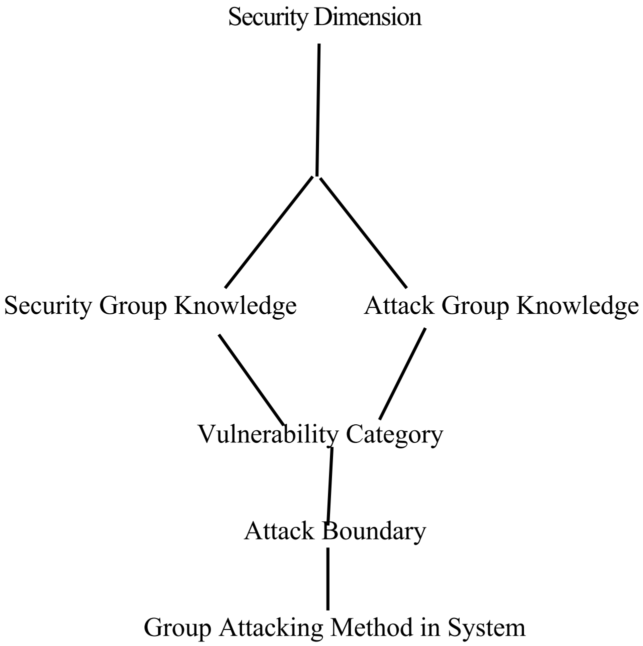

Fig. 1. The proposed vulnerability classification model

The attack group knowledge also refers to attack pattern that depends on rigorous methods of exploitation by attacker. This dimension of security based on process or set of system attributes that may be exploited in an action by attacker with means of gaining access to the system related information. The next fourth element of security dimension is vulnerability category .In this stage having evaluated by the first two process of security group and attack group knowledge gained, a vulnerability is classified and the categorized into its class of group based on exploitation technique and parameters. Once a vulnerability is categorized its attack boundary profile that is designed keeping in view the level of impact on the system in case of exploit the security function. This helps to understand the level and scale of infection or impact onto the system that became target of attack propagation. An attack boundary is basically defined through a set of systems under attack that is controlled as a single administrative control. At this level boundaries are various, and vulnerabilities can become obvious as data object is input boundary race condition.

The group attacking method consist on attack ID, classification and attack group that simplifies the vulnerability and attacking technique, whereas group classifies the attack dimension fall under the category. The purpose of this model is to simplify the attack dimensions and way of attack fall under the category, where each vulnerability is subdivided into attack class and method, as defined in the model. Presentation of model is depicted through the table of Grouping Attack Method ID & Logical Vulnerability Classification.

Table 1. Group attacking method ID and Vulnerability Classification.

SN	Attack Classification	Attack method & Parameter	Attack Group & pattern	Category
1	Application Logic attack	Logic Design Fault	Exploitation of Functionality	Web Application
2	Application Logic attack	logic diversion error	Anti-Automation	Web application
3	Application logic attack	control flow error	web function exploit	Web application
4	Application Logic attack	programme logic flaw	Subversion of Logic	Web application
5	Application Logic attack	functional flow Fault	exploit the sequences of logic order	Web application
6	Application Logic attack	Design logic flaw	web Copy Cat	Web application

The logical attacks are different types of attacks with different attack methods because logical attack has to exploit the functionality that is specific to the application and its logic .This is what, defined in the above mentioned table of Grouping Attack Method ID & Logical Vulnerability Classification.

As mentioned above the main scope of this study is to focus on "application logic based vulnerabilities" problem that is because of a design flaw or fault that mismatch between design & architecture while developing component –based software application. We have classified the six vulnerabilities in the application logic and then developed the attack group and vulnerability classification to be categorized by proposed model of classification and security dimension in the light of vulnerability model that is cause of design flaw in application logic and functionality.

3.1 **Classification of Logical Vulnerability VS Technical Vulnerability**

In the light of our research, the proposed model would turn into be a classification & characterization of two distinctive categories of vulnerability issues /problems "Technical vs Logical Vulnerabilities". These vulnerabilities are classified based on the attack method as mentioned in the above table of vulnerability, this classification relates to attack pattern technique. Therefore, keeping in view the proposed model of classification falls under the two categories of vulnerabilities, which have been drawn into classification tree model dividing into sub-class of attack at the application layer of ecommerce component-based software application. This depicts the detailed classification, having characterized each vulnerability by their unique signature of indemnity in the proposed scheme.

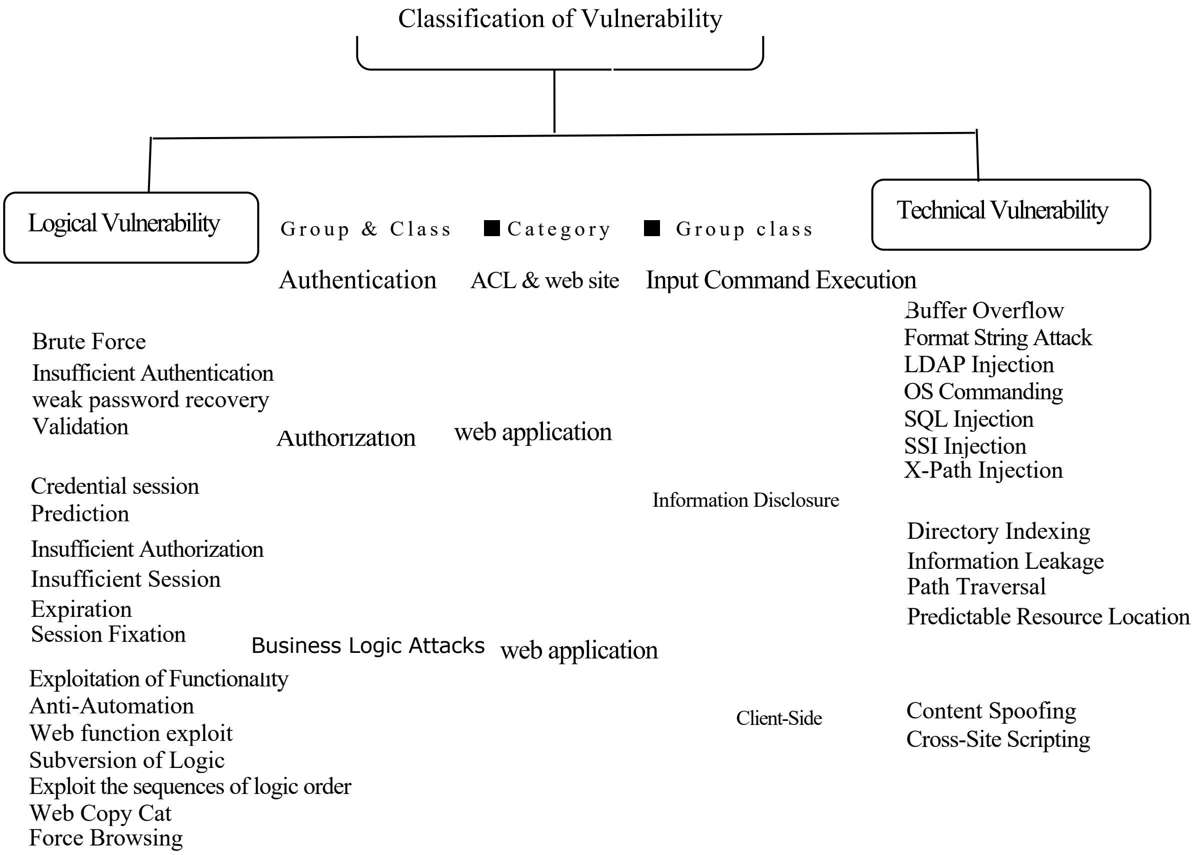

Fig. 2. Classification of Vulnerability Scheme

The proposed contribution of the classification is characterized by attack pattern and target agent in each kind of attack as mentioned in given classification scheme of application logic-based attack pattern method, vulnerability class and event triggering logical element. This is further put into attack pattern technique to classify each vulnerability in the light of attack method, such classifications are characterized in groups of attacking parameters which defines nature of vulnerability. Therefore, in the light of our detailed classification and characterizing of vulnerabilities into groups and their attacking methods, as it is defined in the above-mentioned table. It is derived that logical vulnerabilities are such vulnerabilities which cannot be mitigated through traditional approaches such as web scanning tool and vulnerabilities detection tool those are based on static analysis because web scanners only detect the implementation bugs, programming error conditions, and fault. Whereas logical vulnerabilities are based on design phased flaw of software-based application [17].Therefore, our proposed scheme is based on classification and categorization of each logical vulnerability based on attack method, which is explained through the parameters of attack logic in above presented table. The classification with defined detailed information about each attack and related attack pattern will be helpful for the developers, having knowledge of the different attacks with technique to design new applications based on the idea of security by design technique.

4. Conclusion

The idea of security development process is based on a proper classification of the vulnerability. It is very useful to have knowledge about the attack and its parameters, target agent, method .Since with the passage of time new technologies emerges, and the more security attacks occur software application server side , in this scenario researcher has made an effort to classify the logical vulnerabilities those are never given consideration by the research community. The proposed vulnerability classification model contributed the new classification related to group attacking method ID and vulnerability classification , which is never been done this before. The proposed model will cover the gap between previously design taxonomies based on different areas of system domain and security classifications of vulnerabilities. This will be very useful for developers to understand the two different sort of vulnerabilities, specially logical vulnerabilities, while designing applications or security by design based idea adoption by them. This model will cover the gap of logical vulnerabilities and related attack patterns, technique, method. This is a significant improvement to taxonomies a class of vulnerability that is not given much consideration by the academia.

References

[1] Samaila, M. G., Neto, M., Fernandes, D. A. B., Freire, M. M., & Inácio, P. R. M. (2017). Security Challenges of the Internet of Things. Pp. 53–82, In J. Batalla, G. Mastorakis, C. Mavromoustakis, & E. Pallis (Eds.), Beyond the Internet of Things. Internet of Things (Technology, Communications and Computing) Cham: Springer. doi:10.1007/978-3-319- 50758-3_3

[2] Krsul, I. V. (1998). Software vulnerability analysis (Doctoral dissertation). Retrieved from https://dl.acm.org/citation. cfm?id=927682

[3] Joshi, C., & Singh, U. K. (2014). Admit-A five dimensional approach towards standardization of network and computer attack taxonomies. International Journal of Computer Applications, 100, 5. doi:10.5120/17524-8091.

[4] Li, X., Chang, X., Board, J. A., & Trivedi, K. S. (2017). A novel approach for software vulnerability classification. In Reliability and Maintainability Symposium (RAMS), 2017 Annual (1– 7). IEEE. doi: 10.1109/RAM.2017.7889792

[5] Antoon, R. U. F. I. (2006). Network Security 1 and 2 Companion Guide. (Cisco Networking Academy).

[6] Fournaris, A. P., PoceroFraile, L., & Koufopavlou, O. (2017). Exploiting hardware vulnerabilities to attack embedded system devices: A survey of potent microarchitectural attacks. Electronics, 6(3), 52. doi:10.3390/electronics6030052 .

[7] Garg, S., & Baliyan, N. (2019a). A novel parallel classifier scheme for vulnerability detection in android. Computers and Electrical Engineering, (Final revision submitted) doi:10.1016/j. compeleceng.2019.04.019.

[8] Homaei, H., & Shahriari, H. R. (2017). Seven years of software vulnerabilities: The ebb and flow. IEEE Security & Privacy, (1), 58–65. doi:10.1109/MSP.2017.15

[9] Sharma, C., & Jain, S. C. (2014, August). Analysis and classification of SQL injection vulnerabilities and attacks on web 18 S. GARG ET AL. applications. International Conference on Advances in Engineering and Technology Research (ICAETR), 2014 (1–6). IEEE. doi: 10.1109/ICAETR.2014.7012815

[10] Faisal Nabi, A Process of Security Assurance Properties. Unification for Application Logic, International Journal of Electronics and Information Engineering, Vol.6, No.1, PP.40-48, Mar. 2017.

[11] Jens L. Eftang a, Martin A. Grepl b, Anthony T. Patera, A posteriori error bounds for the empirical interpolation method, C. R. Acad. Sci. Paris, Ser. I 348 (2010) 575–579 http://www.sciencedirect.com/ .

[12] Hansman, S., Hunt R., "A taxonomy of network and computer attacks". Computer and Security, vol. 24, issue 1, Feb 2005, PP. 31-43.

[13] Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. "AVOIDIT: A Cyber Attack Taxonomy", University of Memphis, Technical Report CS-09-003, 2009. [Online]. Available:

[14] T. Aslam, "Use of a taxonomy of Security Faults," Technical Report 96-05, COAST Laboratory, Department of Computer Science, Purdue University, March 1996.

[15] Scott D., Angelos S," Towards a Cyber Conflict Taxonomy", 5th International Conference on Cyber Conflict K. Podins, J. Stinissen, M. Maybaum (Eds.), 2013.

[16] Lough, Daniel. "A Taxonomy of Computer Attacks with Applications to Wireless Networks," PhD thesis, Virginia Polytechnic Institute and State University, 2001.

[17] Marco Vieira, Nuno Antunes, and Henrique Madeira, Using Web Security Scanners to Detect Vulnerabilities in Web Services, 2009 IEEE/IFIP International Conference on Dependable Systems & Networks, https://ieeexplore.ieee.org/abstract/document/5270294.