Evaluation on accuracy of new vulnerability classification pattern algorithm in public data set

Nor Hafeizah Hassan[1,*], Nurul A. Emran[1], Noraswaliza Abdullah Jumaidin[1]

[1] Advanced Computing Technologies Centre (C-ACT), Faculty Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

[*]Corresponding e-mail: nor_hafeizah@utem.edu.my

Keywords: Security relationship, software modeling, vulnerability pattern

ABSTRACT – Software developers are facing difficulties in understanding the possible vulnerabilities from early stage of software development. This makes it hard to plan for the mitigation process and testing process. In particular, identification and classification algorithm of software vulnerabilities are under study. To evaluate the accuracy of classification pattern algorithm, an experiment is conducted using public data set, where the precision and recall rate were used. The results show significant accuracy when execution is conducted randomly on two different data sets. This study shall help the developers to identify the possible vulnerability at early stage of their development.

1. INTRODUCTION

A good modeling process will have mechanism for preventing, detecting and correcting errors at each step of software development process [1]. Models for security analysis must describe how and when security breaches occur; they must describe the impact on the system when they do, as well as the mechanisms, effects, and costs of system recovery, system maintenance, and defenses [2]. Some models have been introduced to elicitate security requirements such as UML-Based modeling for security, attack trees and misuse case. However, some limitations occur within them. This study proposed a new vulnerability classification pattern algorithm to elicit the security relationship.

A comparison of security model had been made by [3]. They compared eleven secure systems design methodologies from year range 1996 to 2004. The comparison was made using specification techniques introduced by [4]. They highlighted the needs for a standardized methodological approach that taking into account security aspects from the earliest stages of development till the completion.

1.1 Example on security-based modeling

Analyses on the mentioned security elicitation models were made. Due to works by [4], two (2) are discussed here. Their disadvantages were considered and improvements are proposed in the new notation.

i. Attack trees

An attack trees represent step by step realization of the attack. It is not only representing the attacks but also represent the countermeasures as a tree structure. The attacks consist of attack goals and attack paths as mentioned in Figure 1.

ii. Misuse Case

A misuse case as shown in Figure 2, describes potential system behaviors that a system's stakeholders deem unacceptable. In a misuse case, at least one threat (or, in more common parlance, attacker) serves as an actor. A misuse case do not indicate how the attacker will achieve his objective of the attack.

Figure 1 A sample of attack trees diagram

Figure 2 A sample of a misuse case diagram

1.2 Derivation of vulnerability classification pattern

A historical preliminary data sources were used to derive this data set as explain in the previous paper [5]. For this experiment, the confirmed case was extracted. Upon examined random extracted data, the labeling and the associates word of the data is given which summarized as object and relationship. The aim of the analysis is to predict the value of the pattern based on several input of classifiers, which, in this research are the four classifiers SourceRoot, SourceLocation, TargetVector and TargetImpact as discussed in [5].

2. METHODOLOGY

Figure 3 shows the methodology of this research. The input to this research includes an experimental approach on public dataset which consist of the mix-dataset and another public vendor-based dataset. Vulnerability classification conceptual models are used as reference and later the vulnerability classification pattern is produced and evaluate. Later, the outputs of

the activities are the results discussion of experimental result and validation result. The vendors-based execute the vulnerability classification pattern algorithm result when the algorithm is applied on the selective vendors. The experts view is to show the correctness and eliminate the ambiguity of classification rules and to prove the whole framework process. The methodology process is illustrated in Figure 3.

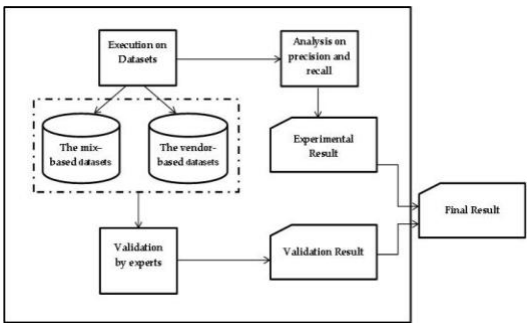

Figure 3 The methodology of this research

3. RESULT AND DISCUSSION

Table 1 and Table 2 depict the results of the experimental execution. Table 1 shows the mix-based dataset and Table 2 shows the vendor-based data set results. The accuracy of the model is measured using two metrics: precision and recall rate.

Precision is the degree of confidence that the returned patterns are accurate when the vulnerability classification pattern algorithm is applied on the data set. Recall is the degree of the ability to return the patterns when the vulnerability classification pattern algorithm is applied on the data set. As given in the definition, between the two rates, the precision rate suggests a better understanding of accuracy in the model. The discussion of precision and recall rate starts with the first data set DS1. The data has been analyzed and the summary is given in Table 1.

Table 1 DS1 – Mixed-based data set extracted using vulnerability classification pattern

Actual Pattern	True Selected Pattern							Total	Accuracy (P rate)
	Repudiation	EoP	Not Classified	Ddos	Tampering	Information	Spoofing		
Repudiation	100	3	0	0	2	0	0	105	0.95
EoP	3	116	1	0	1	2	0	123	0.94
Not Classified	0	1	67	0	1	0	1	70	0.96
Ddos	0	0	1	93	2	0	0	96	0.97
Tampering	1	0	1	1	53	1	1	58	0.91
Information	1	2	0	0	1	34	0	38	0.89
Spoofing	0	0	2	0	0	0	8	10	0.80
Total	105	122	72	94	60	37	10	500	**Ave 0.92**
R rate	0.95	0.95	0.93	0.99	0.88	0.92	0.80		**Ave 0.92**

Table 1 shows the precision and recall rate for DS1 data set from the 500 samples of incidents that range from year 1999 to 2004. The left column is the number of actual pattern classes from the data. The middle column is the number of true selected pattern that gained. And the right most columns are the total counts of the predicted pattern and their precision rate, or accuracy. The last rows are the total counts of the recalled patterns and their recall rates. The last cell diagonally at bottom right denotes the sample size from either the total from row of precision or recall. The bold values are the average rate for the precision and recall rates. In this data set, the average rate for precision and recall are both 0.92. In Table 2, DS2 represent the vendor-based data set from a vendor which emphasized on the applications and server incidents. The standard deviation (SD) for precision rate is 0.23 and recall rate is 0.24. The *p* value (p_value) for precision rate is 0.01 and the p_value for recall rate is 0.02.

Table 2 DS2 – Vendor-based data set extracted using vulnerability classification pattern

Actual Pattern	True Selected Pattern							Total	Accuracy (P rate)
	Spoofing	Tampering	Repudiation	Information	Ddos	EoP	Not Classified		
Spoofing	2	1	1	0	1	1	0	6	0.98
Tampering	0	7	0	0	0	3	0	10	1.00
Repudiation	1	0	6	0	0	1	0	8	0.94
Information	0	0	0	31	0	0	0	31	0.70
Ddos	1	0	0	0	46	2	0	49	0.75
EoP	2	4	1	0	0	384	0	391	1.00
Not Classified	0	0	0	0	0	0	5	5	0.33
Total	6	12	8	31	47	391	5	500	**0.81**
R rate	0.33	0.58	0.75	1.00	0.98	0.98	1.00		**0.80**

4. CONCLUSIONS

In conclusion, all data sets showed that there was an encouraging result in the analysis. The standard deviation is to measure the variability of each pattern in respective data sets. And the p value is to measure if there is any extreme difference between them. If the p value is equal or less than 0.05, than there is no difference between the average and the algorithm is acceptable.

ACKNOWLEDGEMENT

Authors are grateful to the Universiti Teknikal Malaysia Melaka (UTeM) for supporting this research.

REFERENCES

[1] Recker, J., Indulska, M., Green, P., Burton-Jones, A., Weber, R., Information systems as representations: A review of the theory and evidence, *J. of the Assoc. for Infor. Sys.*, vol. 20, no. 6, pp. 735-786, 2019.

[2] Nicol, D. M., Sanders, W. H., Trivedi, K. S., Model-based evaluation: from dependability to security, *IEEE Transactions*, vol. 1, no. 1, pp. 48-65, 2004.

[3] Villarroel, R., Fernández-Medina, E., Piattini, M., Secure information systems development - a survey and comparison, *Comp. & Security*, vol. 24, no. 4, pp. 308-321, 2005.

[4] Khwaja, A. A., Urban, J. E., A synthesis of evaluation criteria for software specifications and specification techniques, *Int. J. of Softw. Eng. and Knowl. Eng.*, vol. 12, pp. 581-599, 2002.

[5] N.H. Hassan, S.R. Selamat and S. Sahib, Establishing the relationship in vulnerability classification for a secure software testing, *Int. Conf. on Adv. in Intel. Sys. in Bioinf., Chem-Informatics, Business Intelligence, Social Media and Cybernetics*, 2014.

[6] N. H. Hassan, N. Bahaman, B. Hussin, S. Sahib, *Int. J. of Adv. Comp. Sci. and App.*, vol. 9, no. 9, pp. 352-364, 2018.