Determination of Weighting Assessment on DREAD Model using Profile Matching

Didit Suprihanto[1]
Department of Electrical Engineering,
Universitas Mulawarman,
Kalimantan Timur, Indonesia 75123
Department of Computer Sciences & Electronics,
Universitas Gadjah Mada,
Sekip Utara, Bulaksumur, Yogyakarta, Indonesia 55281

Retantyo Wardoyo[2], Khabib Mustofa[3]
Department of Computer Sciences & Electronics,
Universitas Gadjah Mada,
Sekip Utara, Bulaksumur, Yogyakarta, Indonesia 55281

***Abstract*—Web application creators often get lack understanding of security threats that can occur in applications that are made, while security threats can create new problems that are more complex. These security threats will pose risks and can even result in large losses. Determining the risk ratings on a *web* application software development team is still experiencing problem or debate. The problem which occurs is that not all of the team members agree on the risk rating assessment process. This problem is caused by the differences in opinions and assumptions of the team members about threats and the fact that the assessor has different types of expertise, DREAD model places each expert in the same position. It means that there are no differences in weight at the time of assessment. DREAD stands for five aspects which are related to security threats in *web* applications. They are D (*Potential Damage*), R (*Reproducibility*), E (*Exploitability*), A (*Affected User*), and D (*Discoverability*). The proposal gives weight to the assessor by using profile matching method to produce an assessment involving assessors with different types of expertise, weighting on each assessor is according to their relevance to the assessed aspects, and rating on the type of expertise is according to the aspects assessed for the DREAD model. The result of the study shows that the proposed method can produce the weight closeness of the assessment to the target.**

***Keywords*—DREAD; risk; assessment; profile matching**

I. Introduction

The application which is used by agencies and companies is currently experiencing rapid progress. Applications by using the *web* are developed from small to large companies. At present, almost all agencies/companies use *web* technology to complete the work's needs. Web technology can be developed according to user needs and become more modern at a lower cost to make it more efficient. The development of *web* technology can overcome various problems such as interoperability problems, it also can be used in several different platforms, and can connect multiple databases with different DBMS. Although *web* application is so important, *web* applications also have a risk to security threats [1].

Web application makers often get lack understanding of security threats that can occur in the application that is made, while security threats can create new problems that are more complex. Security threats that can be categorized as input validation, authorization, authentication, cryptography, exception management, configuration management, session management, sensitive data, parameter manipulation, audit, and logging. These security threats will pose risks and can cause many problems, and can even lead to large losses. In identifying the risks, there are several factors needed to consider, such as the extent to which these risks are exploited and how much damage will occur. [2]

The determination of risk ratings on a web application software development team is still experiencing problems or debates. The problem that occurs is that the team members do not all agree on the risk rating assessment process. This problem is caused by the fact that team members have different opinions and assumptions about threats [3]. These problems are in line with [4] the similarity of the experts which can be used in group decision making that can provide comprehensive information from all experts who have different and subjective.opinion.

Weighting is part of the way for decision making in a process to produce alternative decisions through assessment of parameters, criteria, and scoring [5]. Weights can be given to attributes such as parameters, criteria, experts or decision-making actors [6]. The weighting process can be done in 2 (two) ways. They are the process of weighting directly and indirectly. Direct weighting gives direct weight or percentage value based on knowledge about the importance of parameters and criteria used. Meanwhile, indirect weighting generally uses analytical methods with computation to produce weight values [7].

Based on the results of a preliminary study, it is known that the application of the DREAD model still has weaknesses. The DREAD model can be applied to assessments by several assessors with the same or different types of expertise. The problem is that in the event which the assessor has a different type of expertise, DREAD model places each expert in the same position, and it means that there is no difference on weight at the time of assessment weighting. The weighting model proposed in this study uses *profile matching* to get ranking from the assessor.

II. DREAD Model

DREAD model is a model which is developed by Microsoft, and it is used to calculate risk and generate risk

ranking information for a threat that occurs. DREAD stands for five aspects related to security threats in web applications, namely D (*Damage Potential*), R (*Reproducibility*), E (*Exploitability*), A (*Affected User*), and D (*Discoverability*).

Some points that need to be considered which are related to the extension of DREAD and asking the following questions are such as [3]:

1) Damage potential: How great is the damage if the vulnerability is exploited?

2) Reproducibility: How easy is it to reproduce the attack?

3) Exploitability: How easy is it to launch an attack?

4) Affected users: As a rough percentage, how many users are affected?

5) Discoverability: How easy is it to find the vulnerability?

Determination of the level of risk in the DREAD model can be calculated by the formula:

$$Risk\_Level = \frac{(D + R + E + A + D)}{5}$$

Therefore, the value of D, R, E, A, and D is maximum three the level of threat using the rating, can be seen in TABLE I.

TABLE I. RATING OF RISK ASSESSMENT

No	Range Assessment	Rating	Risk Description
1	5 to 7	3	Low
2	8 to 11	2	Medium
3	12 to 15	1	High

Source: *Improving Web Application Security* [3]

Generally, the DREAD model consists of three important stages, and they are such as identification of threats, documentation of threats, and determination of threat levels [3].

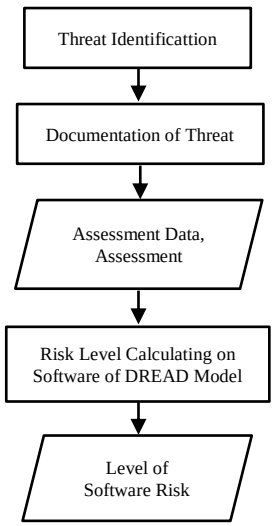


Fig. 1. DREAD model [3]

The examples of applying DREAD model is carried out by [1] in GWIS (*Geospatial Weather Information System*) system. The DREAD model has also been developed and implemented into a fuzzy concept for risk rating determination, namely by transforming ordinal ranks on several security parameters into numerical value ratings [8].

III. PROFILE MATCHING

Profile Matching is a decision-making mechanism to assume that there is an ideal level of predictor variables that must be done by parameters, not in static criteria [9]. In the profile matching process, the outline of the process of comparing individual competencies into aspects that can be known for differences in competencies is called gap [10] [11]. The smaller of the gap produces a large value weight, and it means that it will get a better chance to occupy the top position. In analyzing the data according to specific targets included; the method of matching profiles performs the method, in which the process is first to determine the competencies needed by the data. In a profile matching process, it describes the process of comparison between individual competencies and aspects that can be identified for both differences.

Profile Matching algorithm is divided into several steps:

- Weighting Aspects and Sub Aspects
- Determine the goal
- Weighting the gap
- Rating using the weight of aspect and score of the gap

A gap is a difference between the aspect value and the target value. Gaps can be obtained by doing this formula.

$$\text{Gap} = \text{Aspect Value} - \text{Target Value} \quad (1)$$

Scoring the gap = to score the gap, so that gap = 0 will weight 3, a maximum gap will have a score of 1.

IV. RESEARCH METHODOLOGY

This study takes a sample in one of the Universities in Samarinda, East Kalimantan. The steps in the study are such as:

1) Identify how many assessors who conduct assessments (n = number of assessors)

2) Identifying the type of expertise

3) Collection of assessment data based on expert/assessor analysis. The data used is academic management data in each university that is sampled with adjusted rules with ten threat categories.

4) Determining the weight of each assessor by using the stages of the profile matching method.

5) The next stage is analysis according to data obtained from experts/assessors and obtained data comparison between one expert and another expert based on established rules.

V. Proposed Determination of Assessment

In this study, the assessment is developed from the DREAD model, so that each assessor with different types of expertise will get an assessment weight that is adjusted to the aspect which is assessed. In the developed model, the assessor with the most relevant type of expertise with the aspect assessed will be given the highest weight. Otherwise, the assessor with the type of expertise that is least relevant to the aspect evaluated will be given the lowest weight. Meanwhile, the assessor with other kinds of knowledge is given appropriate weights on the level of relevance to the assessed aspect. The aspects assessed in the DREAD model which is developed include ten categories in which each category consists of predetermined variables, as a whole as many as 37 variables. For each variable is given in the form of rating categories such as high, medium, or low.

The proposal for determining the weight of each assessor which is carried out in the research is described in the form of these following categories, such as:

1) The same weight of assessor is formulated:

$$Wi = {}^{1}/_{n} \quad (4)$$

Description:

Wi = The weight of assessor -i, in which i= 1,2,.., n

n = number of assessors

2) Different weight of assessor is formulated:

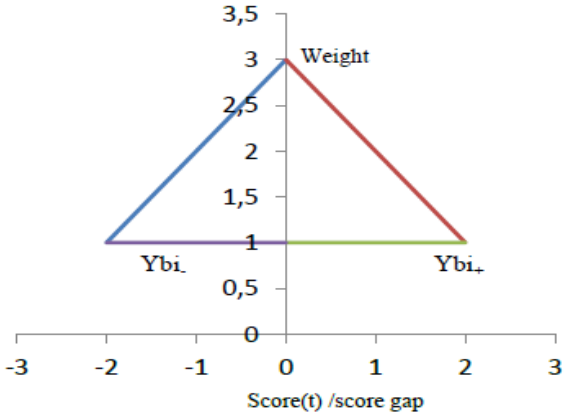
$$Wi = W_i' \quad (5)$$

Description:

Wi = The weight of assessor -i, in which i= 1,2,.., n

$W_1', W_2', W_3', \dots, W_n'$ = Weight of 1,2,3,.., n

Gap assessment can be calculated by using the formula below with the formula of graph 1.



Graph 1. Determination of weight

Determining the score (t) at min x <= t <=0 is determined by the formula:

$$score(t) = \frac{(t - \min x)}{(-(\min x))}.(Ymaks - Ybi_{-}) + Ybi_{-} \quad (6)$$

While, the determination of the score (t) at 0 <= t <= max x can be formulated as:

$$score(t) = \frac{(t)}{(max\ x)}.(Ybi_{+} - Ymaks) + Ymaks \quad (7)$$

Description:

score (t) = weight/ score

t = value at gap / difference

min x = the smallest value in the gap (negative / x negative difference)

max x = the biggest value on the gap (positive / x positive difference)

Ymaks = the highest value on the assessment score

Ybi_{+} = lower limit Y on t positive

Ybi_{-} = lower limit Y at t negative

Each assessor (Ni) calculated the number of DREAD which is calculated in the form of:

$$DTot_i = D_i + R_i + E_i + A_i + D_i \quad (8)$$

Description:

$DTot_i$ = Sum of DREAD with index i and i= 1,2,.., n

D_i, R_i, E_i, A_i, D_i = the value on D,R,E,A,D with index i and i= 1,2,3,.., n

The score of each assessor is divided into 2 (two), such as:

3) Scores with the same weight are formulated:

$$WSi = \frac{1}{n}.DTot_i \quad (9)$$

Description:

WS_i = score with the same weight from each assessor

4) Scores with the different weight are formulated:

$$WDi = W_i'.DTot_i \quad (10)$$

Description:

WD_i = Scores with different weights are formulated

VI. Result and Discussion

The results of the study are presented continually in TABLE II to TABLE V as follows:

TABLE II. The Expert who Assessed

No	Code	Expertise
1	P1	Networking
2	P2	Hardware
3	P3	Programmer
4	P4	Database
5	P5	Database

In this study, the assessors or experts who assessed are 5 people. The experts who assess the academic information system are according to their respective expertise. Appraisal expertise can be seen in TABLE II which is consisting of experts given P1 to P5 codes. In this study, two experts are the same in code P4 and P5, and they are experts in the field of the database. The similarity of some assessment expertise proves that the assessment of the academic information system in determining the expert as an assessor is objective, and in which it means that the number of experts obtained can be an assessor in this study.

Based on expert judgment, a calculation with the profile matching method obtained results from the weight of each expert which is presented in TABLE III.

TABLE III. EXPERT WEIGHTS BASED ON CATEGORY

No	Category	Expert				
		P1	P2	P3	P4	P5
1	Input validation	21.3%	19.1%	23.4%	19.1%	17.0%
2	Authentication	19.4%	17.7%	19.4%	21.0%	22.6%
3	Authorization	22.9%	20.8%	16.7%	18.8%	20.8%
4	Configuration management	25.5%	19.1%	21.3%	14.9%	19.1%
5	Sensitive data	20.6%	14.7%	17.6%	20.6%	26.5%
6	Session management	18.5%	21.5%	24.6%	18.5%	16.9%
7	Cryptography	21.9%	18.8%	15.6%	25.0%	18.8%
8	Parameter manipulation	22.7%	13.6%	22.7%	22.7%	18.2%
9	Exception management	21.6%	18.9%	16.2%	18.9%	24.3%
10	Auditing and logging	21.1%	15.8%	21.1%	26.3%	15.8%

Based on TABLE III, it can be explained that the highest weight of proximity between each category varies in each expert. The highest weight obtained in all categories in each expert in the range of 22% to 26%, while the lowest weight in the range of 13% to 17%. The highest expert weight of each category is presented in TABLE IV:

TABLE IV. THE HIGHEST EXPERT WEIGHT OF EACH CATEGORY

No	Category	Expert	Weight
1	Input validation	P3	23.4%
2	Authentication	P5	22.6%
3	Authorization	P1	22.9%
4	Configuration management	P1	25.5%
5	Sensitive data	P5	26.5%
6	Session management	P3	24.6%
7	Cryptography	P4	25.0%
8	Parameter manipulation	P1, P3, P4	22.7%
9	Exception management	P5	24.3%
10	Auditing and logging	P4	26.3%

From TABLE IV, it can be concluded that the highest weight of the expert judgment on the sequential target is such as: in the input validation category, the highest weight is located in the programming, database authentication, network expert authorization, network expert configuration management, sensitive database expert, session management programming expert, cryptography database expert. On the parameters, the highest manipulation weight is owned by network experts, programmers and it means that the closeness of the assessment of 3 experts on the target has the same weight value of 22.7%, for the highest category of exception management weight in database experts while in the Auditing and logging category lies in the database expert.

The expert weight which is obtained in each category in TABLE III is used in the calculation into the DREAD model. The calculation result that is according to the expert weights obtained result which is presented in TABLE V:

TABLE V. THE RESULT OF DREAD VALUE ACCORDING TO EXPERT WEIGHT

No	Category	Dp	R	E	A	D	SUM	Level Risk
1	Input validation	2.55	2.36	2.62	2.23	2.43	12.19	High
2	Authentication	2.23	2.58	3.00	2.58	1.63	12.02	High
3	Authorization	1.83	2.60	2.25	1.88	2.38	10.94	Medium
4	Configuration management	1.66	2.02	2.02	1.85	2.11	9.66	Medium
5	Sensitive data	2.00	2.41	2.62	2.59	2.82	12.44	High
6	Session management	2.29	2.40	2.00	2.40	1.58	10.68	Medium
7	Cryptography	1.75	1.75	2.59	1.84	1.56	9.50	Medium
8	Parameter manipulation	1.36	1.36	1.64	2.05	2.00	8.41	Medium
9	Exception management	2.43	2.41	1.65	2.00	2.57	11.05	High
10	Auditing and logging	1.68	2.47	1.16	2.00	2.16	9.47	Medium
						Avg	10.64	Medium

From TABLE V, it can be explained that high risk lies in the category of input validation, authentication, sensitive data and exception management with successive values of 12.19, 12.02, 12.44 and 11.05 while for other categories the level of risk is in the medium category. For the average value of all categories in the assessment of web applications or software, this is 10.64 including moderate risk.

VII. CONCLUSION

Based on the result of the trials which have been done, the highest rank in each category can be occupied by more than one expert, this indicated that the proximity of the expert judgement to the target is equal. Profile matching method can be used as an alternative to finding out the weight of the assessor in the assessment of DREAD model.

Meanwhile, the DREAD value after being calculated with the appraisal weight to reach the highest value or high risk contained in the input validation category with a value of 12.19, authentication with a value of 12.02, sensitive data with

a value of 12.44 and exception management with a value of 11.05. For the overall assessment with the DREAD model is known that web applications or software are in moderate risk with a value of 10.58. so it can be said that the application that is applied can still be used with the main priority of improvement or full attention in the category of input validation, authentication, sensitive data, exception management.

ACKNOWLEDGMENTS

The author would like to thank the Director of Research and Community Service (DPRM) for helping with funding in this research, through the funding of the 2018 Doctoral Dissertation Research scheme.

REFERENCES

[1] K. R. Mohan Rao, and D. Pant, 2010, "A threat risk modeling framework for Geospatial Weather Information System (GWIS): a DREAD based study," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 1, No. 3, September 2010

[2] D. Suprihanto and R. Wardoyo, 2017, "Analysis of Computational Time on DREAD Model", International Journal of Computer Engineering In Research Trends, Volume 4, Issue 2, pp. 53-56.

[3] J.D Meier, A. Mackman, S. Vasireddy, M. Dunner, S. Escamilla, and A. Murukan, "Improving Web Application Security: Threats and Countermeasures," Microsoft Corporation. 2003.

[4] W. Lu, C. Liang, and Y. Ding, "Experts Based on Evidence Similarity in Group Decision-making," in 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp.1–4, 2008.

[5] R.R. Yager, "Uncertainty modeling and decision support," *Reliability Engineering & System Safety*, 85(1-3), pp.341–354, 2004.

[6] L. Garc, "Weighting Individual Opinions in Group Decision Making," pp.92–103, 2007.

[7] Z. Wang, "An Adjustment Method of Experts Weights in Group Decision," pp.1–5, 2010.

[8] A.A Singh and K.S Singh, "Network Threat Ratings in Conventional DREAD Model Using Fuzzy Logic," IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012 ISSN (Online): 1694-0814

[9] Z. Tharo, and A.P.U Siahaan, "Profile Matching in Solving Rank Problem," *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE).Volume 11, Issue 5, Ver. I (Sep.-Oct .2016), PP 73-76, e-ISSN: 2278-2834,p- ISSN: 2278-8735*

[10] D. J. Power, "Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation," Journal of Machine Learning Technologies, pp. 37-63, 2011.

[11] E. Turban, "Decision Support Systems and Intelligent Systems," New Jersey: Pearson Education, 2005.