FEMRA: Fuzzy Expert Model for Risk Assessment

Alireza Shameli Sendi[1], Masoume Jabbarifar[1], Mahdi Shajari[2] and Michel Dagenais[1]
[1]École Polytechnique de Montréal - Montreal, Canada
[2]Amirkabir University of Technology - Tehran, Iran
[1]e-mail: {alireza.shameli-sendi, masoume.jabbarifar, michel.dagenais}@polymtl.ca
[2] e-mail: mshajari@aut.ac.ir

Abstract—**Risk assessment is a major part of the ISMS Process. The Information Security Management System standards specify guidelines and a general framework for risk assessment. In many existing standards, such as NIST and ISO27001, risk assessment is described however, while these standards present some guidelines, there are no details on how to implement it in an organization. In a complex organization, risk assessment is a complicated process and involves a lot of assets. In this paper, we present the FEMRA model, which uses fuzzy expert systems to assess risk in organizations. The risk assessment varies considerably with the context, the metrics used as dependent variables, and the opinions of the persons involved. Fuzzy logic thus represents an excellent model for this application. Organizations can use FEMRA as a tool to improve the ISMS implementation. One of the interesting characteristics of FEMRA is that it can represent each risk with a numerical value. The managers can detect higher risks by comparing these values and develop a good strategy to reduce them.**

Keywords-risk assessment; asset; vulnerability; threat; fuzzy

I. Introduction

Today, many organizations and companies use information systems and network frameworks on a large scale, thus IT dependency is increasing daily. Security is one the most important issues for the stability and development of these systems. Therefore, most organizations invest in this area and are establishing Information Security Management System (ISMS). Although many organizations understand the importance of security, many don't understand how to implement an ISMS. The main process of an ISMS implementation is risk assessment [2].

Risk assessment provides organizations with an accurate evaluation of the risks to their assets. It can help them prioritize and develop a comprehensive strategy to reduce risks.

Information security risk assessment does not have an old history. There are some standards and methodologies for risk assessment, such as NIST and ISO27001, but while they explain general principles and guidelines, they do not give any implementation details. This may cause ambiguities to the users [3].

A practical model for information security risk assessment is presented in this paper; it can be used by various organizations. Considering the limitations of quantitative approaches, this model recommends a qualitative method based on expert opinions and fuzzy techniques for information security risk assessment. The relevant knowledge from human experts is stored as rule database in order to apply fuzzy logic and infer an overall numerical value [4].

Also, perfect asset identification is the main basis of vulnerability and threat identification, and eventually risk identification. In our model, a security cube for asset classification is proposed.

First, the coefficients of importance for the basic goals of information security (Confidentiality, Integrity and Availability) are determined. Confidentiality ensures that any authorized user can have access to only certain assets. Integrity verifies that any authorized user can modify assets in an acceptable manner. Availability means that the assets are always accessible by the authorized users. Then, vulnerabilities and threats related to assets are identified and their effects are determined. Finally, the effect of each risk is calculated quantitatively in each view of the security cube.

The paper is organized as follows: first, we will investigate earlier work and several existing methods for risk assessment will be introduced. Fuzzy modeling is illustrated in Section III. The proposed model will be discussed in Section IV. Experimental results are given in Section V. Finally, we will conclude and future work will be discussed.

II. Related Works

Information security risk assessment has a recent history and related standards and methodologies are in progress. Some of these articles are mentioned here.

Zhao *et al* [5] evaluated network security risk by using probabilities, impact severity, AHP techniques and Shannon entropy. Decisions were made using fuzzy logic through linguistic variables; entropy is also applied in measuring criterion weights.

Guan *et al* [6] assessed information security risks according to the likelihood and impact factors of each. In this method, risk factors are determined according to standard ISO17799 categorization. Then, it is assumed that determining the likelihood of each risk is similar to determining the weights in pairwise comparisons in the AHP method. Based on this view, the likelihood or weight of each risk factor is being determined using expert opinions. On the other hand, the vulnerability of each information asset for each risk factor is considered equal to its impact severity, which takes its relative value from experts through linguistic variables.

Wang and Elhag [7] proposed a fuzzy TOPSIS method based on alpha level sets and applied it in bridge risk assessment. In this example, the likelihood and impact of different threats are being determined in linguistic variable forms and then are applied in bridge risk assessment by multiplying their related fuzzy values. Likewise, four effective criterion on impact severity are introduced. Experts recommend their opinion in the form of these four criterion, with which the severity impact is then calculated.

Haslum *et al* [1] proposed a fuzzy model for online risk assessment in networks. The main contribution of their paper is the fuzzy logic controllers. They were developed to quantify the various risks based on a number of variables derived from the inputs from various components.

III. Fuzzy Modeling

Human experts rely on their experience and judgement to estimate the risk based on a number of dependent variables. Fuzzy logic aims to capture and automate this process. The knowledge from security and risk experts is embedded into rules for a fuzzy automatic inference system [1].

Figure 1 shows the fuzzy model. There are three steps in this model: fuzzification, inference engine and deffuzification. The input and output of the fuzzy model is a number. In the inference engine, we define the fuzzy rules.

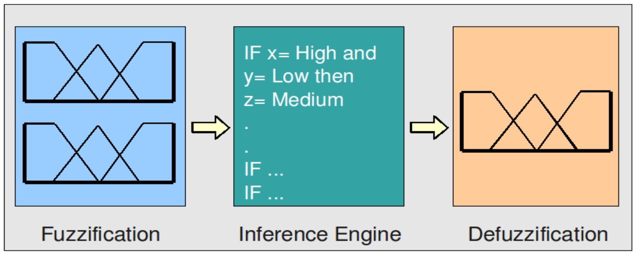

Figure 1. Fuzzy Model.

The first step in fuzzy logic processing involves a domain transformation called fuzzification. To transform crisp input into fuzzy input, membership functions must first be defined. The next step is to apply if-then rules. The final step is defuzzification. This step is used to convert the fuzzy output set to a crisp number. We define three membership functions for input and output: low, medium and high.

IV. Proposed Model

Figure 2 illustrates the dependencies among some of the most important notions in the risk assessment terminology. There are three steps in the risk assessment model:

- **Step 1:** The goal of the first step is to identify the assets and the potential threats applicable to the IT system. Three main bases of security known as the security golden triangle (Confidentiality, Integrity and Availability) are used to evaluate assets and calculate threat effects. Therefore, in this step, we have the CIA triad evaluated by expert people.
- **Step 2:** The goal of this step is to generate a list of asset vulnerabilities and risks. We can then calculate asset values, vulnerability effects and threat effects.
- **Step 3:** The goal of the final step is to calculate the effect of risks. To calculate these effects, we use the fuzzy model that will be explained.

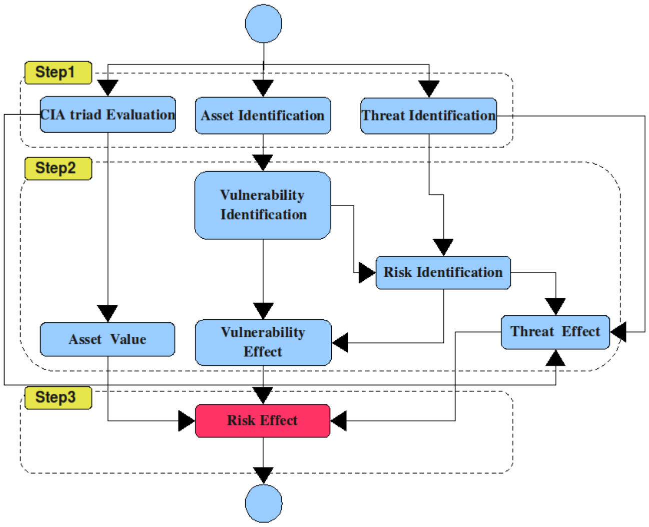

Figure 2. Risk Assessment Structure.

A. *Asset Classification and Identification*

Asset classification has a very important role in information security management. So far, some methods have been proposed to classify assets in organizations. Classifying assets properly will help us in obtaining an effective asset protection. In the proposed asset classification method, we have designed a security cube, which is a combination of valuable and important assets from a security perspective of the organization, and the Zachman model [8]. Figure 3 illustrates the security cube. Assets are classified according to three views:

- **Business View:** The business view consists of the three views of the Zachman framework (WHY - HOW - WHO) and includes value, policy, vision, mission, strategy, structure, process, partner, cooperator, internal rule, external rule, role and human. There are also some empty fields where some other parameters could be added, which illustrates the flexibility of the model.
- **Logical View:** The logical view is divided into three sections, which are software, data, and logical infrastructure of networks. The data section

corresponds to the WHAT view of the Zachman framework. The software section is divided into foreign, country and organization parts. Each part includes network tools, web applications, applications, programming, utilities, DBMS, OS and office. The data section is divided into personal and organizational parts, and each part comprises DB, file, paper and brain storage. The network section is divided into six parts, which are platform, application, strategy, protocol, communication and design.

- **Physical View:** The physical view consists of four sections: media, storage, where, hardware components. The WHERE section is used as the WHERE view of the Zachman framework.

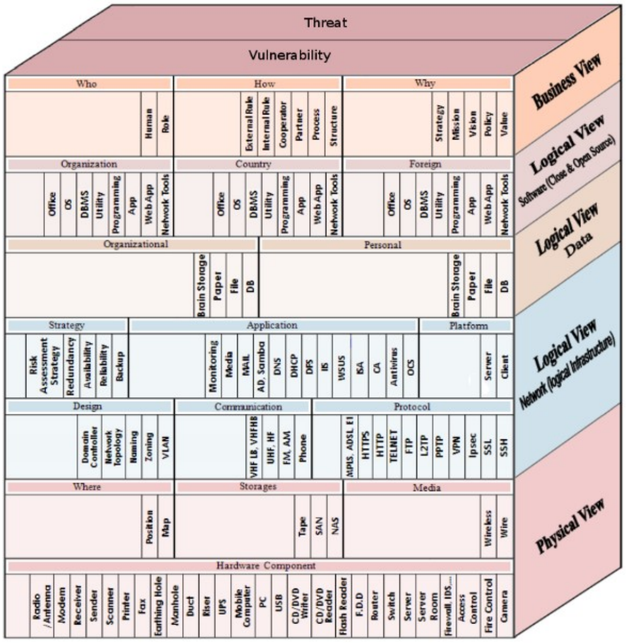

Figure 3. Security Cube.

Table I presents some examples of assets based on the security cube.

TABLE I. ASSETS

Id	Domain	Section (Sub)	Asset
A1	Business View	Who (Human)	John Smith
A2	Logical View (Software)	Organizational (App)	Human Resource Application
A3	Logical View (Data)	Organizational (DB)	SQL_Server_1
A4	Logical View (Network)	Application (DNS)	DNS_1
A5	Logical View (Network)	Design (VLAN)	VLAN_1
A6	Physical View	Hardware Component (Server Room)	Server_Room_1

B. *Threat Identification*

A threat is something which may happen. When a threat materializes, it may result in unwanted events which could damage the system or organization [2]. Threats can adversely affect assets. Table II shows some examples of threats.

TABLE II. THREATS

Id	Threat
T1	Cache poisoning attacks
T2	Data deletion
T3	SQL injection
T4	VLAN hopping attacks
T5	Earthquake
T6	Data theft
T7	Directory traversal
T8	Data discovery
T9	Physical theft

C. *CIA Triad Evaluation*

Evaluating the CIA triad is key to calculate the organization's risks, and we can determine which one of these three complimentary goals is more important to an organization. In this case study, we use *3* experts to evaluate the CIA triad. Obviously, a higher number of experts would give a better risk assessment.

TABLE III. CIA TRIAD EVALUATION

Expert	Confidentiality $\left(W_C\right)$	Integrity $\left(W_I\right)$	Availability $\left(W_A\right)$
E1	0.5	0.2	0.3
E2	0.4	0.3	0.3
E3	0.6	0.3	0.1

Finally, the base of the CIA triad could be calculated with the following formula:

$$W_C = \frac{\sum_{e=1}^{n} C_e}{n}, \quad W_I = \frac{\sum_{e=1}^{n} I_e}{n}, \quad W_A = \frac{\sum_{e=1}^{n} A_e}{n} \qquad (1)$$

D. *Vulnerability Identification*

A vulnerability is a flaw or weak point in system security procedures, design or implementation. It could be exploited by an attacker or may affect the security goals of the CIA triad. Vulnerability identification can be achieved by different means such as software tools in networks, questionnaire forms, etc. [9] Table IV presents some examples of asset vulnerabilities.

TABLE IV. ASSET VULNERABILITIES

Id	Asset	Vulnerability
V1	A1 (John Smith)	No knowledge of file encoding using public keys
V2	A2 (Human Resource Application)	Unchecked user input
V3	A3 (SQL_Server_1)	Not using a mixed authentication mode
V4	A4 (DNS_1)	Insufficient transaction ID space
V5	A5 (VLAN_1)	Not properly configured
V6	A6 (Server_Room_1)	Unsuitable location

E. *Risk Identification*

The objective of risk identification is to identify all possible risks to the assets. In the previous sections, we exposed all the vulnerabilities of each asset. We also exposed all threats to the organization's assets. In this section, we determine which threats are related to which vulnerability. The relationship between each vulnerability and threat is a risk. Table V illustrates some risks within an organization.

TABLE V. SOME RISKS IN AN ORGANIZATION

Asset Id	Vulnerability Id	Threat Id	Risk Id
A1	V1	T9	R1
A2	V2	T3	R2
A2	V2	T7	R3
A3	V3	T2	R4
A3	V3	T6	R5
A3	V3	T8	R6
A4	V4	T1	R7
A5	V5	T4	R8
A6	V6	T5	R9
A6	V6	T9	R10

F. *Asset Value*

The CIA triad should be used to calculate the value of each asset. As can be seen in Table VI, we use *3* experts to evaluate each asset. To get better results, we should get help from different experts for each group of assets in the security cube. For example, network experts should evaluate network assets such as servers, clients and firewalls, software experts should evaluate software assets such as web applications, and so on. Each expert assigns a value from 1 to 9 to each part of CIA triad based on Table VII.

TABLE VI. ASSET VALUE

Expert	Confidentiality (C)	Integrity (I)	Availability (A)
E1	9	6	1
E2	8	7	2
E3	7	7	1

For example, the *9* value in confidentiality means that this asset's privacy is very high and the *1* value in availability means that the availability of the asset is not important.

TABLE VII. RANGE

Level	Level	Effect
High	High	9
	Medium	8
	Low	7
Medium	High	6
	Medium	5
	Low	4
Low	High	3
	Medium	2
	Low	1

Finally, the asset's value could be calculated with formula 2. For this example, the result is 6.04 (based on Table III).

$$asset_{value} = \sum_{CIA=1}^{3} \left(\frac{\sum_{e=1}^{n} CIA_{e}}{n} \right) * W_{CIA} \qquad (2)$$

G. *Vulnerability Identification*

We represent vulnerability effects with a percentage, and for better accuracy, we get help from *n* experts. Table VIII shows *3* expert opinions for a given vulnerability. For example, the *90%* means a very high vulnerability percentage, which means that all threats related to this vulnerability have a high probability of occurring.

TABLE VIII. VULNERABILITY EFFECTS

Expert	Effect
E1	90 %
E2	70 %
E3	60 %

Finally, the vulnerability effect could be calculated with formula 3. For this example, the result is 73.33%.

$$Vulnerability_{effect} = \frac{\sum_{e=1}^{n} effect}{n} \qquad (3)$$

H. *Threat Effects*

We used the CIA triad to calculate threat effects. As you can see in Table IX, we use 3 experts to calculate those effects. For each threat, we should get help from relevant experts to get better results. The calculation method of threats is similar to the one for assets. Each expert assigns a value from 1 to 9 to each part of CIA triad based on Table VII. For example, a value of *9* in confidentiality means that this threat in the confidentiality area is very dangerous. Similarly, the value *1* in availability means that this threat can not be dangerous for the availability.

TABLE IX. THREAT EFFECTS

Expert	Confidentiality (C)	Integrity (I)	Availability (A)
E1	9	3	1
E2	8	2	2
E3	7	4	1

Finally, the threat effects could be calculated with formula 4. For this example, the result is 5.09 (based on Table III).

$$threat_{effect} = \sum_{CIA=1}^{3} \left(\frac{\sum_{e=1}^{n} CIA_{e}}{n} \right) * W_{CIA} \qquad (4)$$

I. *Risk Effects*

Risk effects are modeled using three parameters: asset values, vulnerability effects, and threat effects. The following sub sections will show how the risk effect can be calculated with the fuzzy model.

1) *Fuzzification*

Three membership functions are used for the three inputs, as can be seen in Figures 4, 5 and 6.

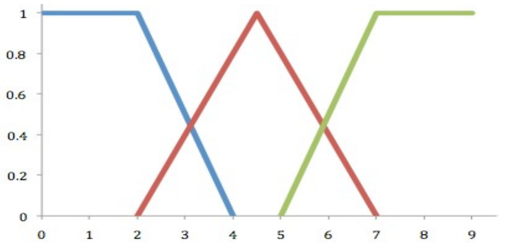

Figure 4. Three Level Membership Function for Asset Value.

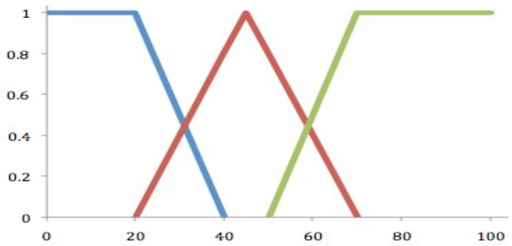

Figure 5. Three Level Membership Function for Vulnerability Effect.

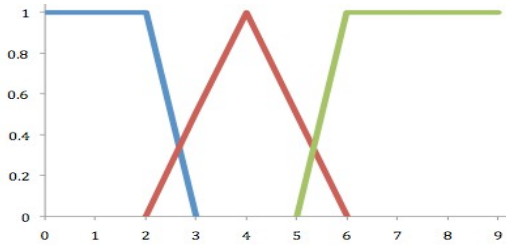

Figure 6. Three Level Membership Function for Threat Effect.

2) *Inference Engine*

The inference engine is fuzzy rule-based and is used to map an input space to an output space. The required rules for risk assessment are created as follows:

Rule 1:
if *(Threat_Effect = Low)*
then *Risk_Effect = Low*

Rule 2:
if *(Threat_Effect = Medium and Vulnerability_Effect = Low)*
then *Risk_Effect = Low*

Rule 3:
if *(Threat_Effect = Medium and Vulnerability_Effect = Medium)*
then *Risk_Effect = Low*

Rule 4:
if *(Threat_Effect = Medium and Vulnerability_Effect = High)*
then *Risk_Effect = Medium*

Rule 5:
if *(Threat_Effect = High and Asset_Value = Low)*
then *Risk_Effect = Medium*

Rule 6:
if *(Threat_Effect = High and Vulnerability_Effect = Low and Asset_Value = Medium)*
then *Risk_Effect = Medium*

Rule 7:
if *(Threat_Effect = High and Vulnerability_Effect = Medium and Asset_Value = Medium)*
then *Risk_Effect = Medium*

Rule 8:
if *(Threat_Effect = High and Vulnerability_Effect = High and Asset_Value = Medium)*
then *Risk_Effect = High*

Rule 9:
if *(Threat_Effect = High and Vulnerability_Effect = Low and Asset_Value = High)* ***then*** *Risk_Effect = Medium*

Rule 10:

if *(Threat_Effect = High and Vulnerability_Effect = Medium and Asset_Value = High)*
then *Risk_Effect = High*

Rule 11:

if *(Threat_Effect = High and Vulnerability_Effect = High and Asset_Value = High)*
then *Risk_Effect = High*

3) *Defuzzification*

Finally, we build another membership function to represent the different possibilities identified by the risk assessment, as displayed in Figure 7. This process is called defuzzification. Two of the most common techniques are the centroid method and maximum method. In the centroid method, the crisp value of the output variable is computed by finding the center of gravity of the membership function. In the maximum method, the crisp value of the output variable is the maximum truth-value (membership weight) of the fuzzy subset. The defuzzification technique that is used for this model is the centroid method.

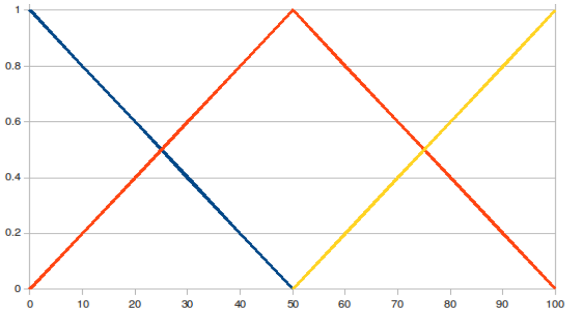

Figure 7. Three Level Membership Function for Risk Assessment.

V. Experimental Results

Table X shows the results of the FEMRA method for some risks (which were extracted based on Table V). In this table, the asset values, vulnerability effects and threat effects were calculated with formulas 2, 3 and 4 and the risk effects were calculated based on these three previous values and the fuzzy model.

TABLE X. Results

Risk Id	Asset Value (0-9)	Vulnerability Effect (0-100)	Threat Effect (0-9)	Risk Effect (0-100)
R1	6.92	91.66	6.92	83.6
R2	9.00	46.66	7.56	83.6
R3	9.00	46.66	4.80	18.3
R4	9.00	50.00	3.08	18.8
R5	9.00	50.00	5.00	19.2
R6	9.00	60.00	5.00	45.6
R7	5.44	63.33	5.48	57.1
R8	5.00	73.33	2.68	46.0
R9	9.00	80.00	2.92	49.7
R10	9.00	80.00	6.92	83.7

VI. Conclusion and Future Work

To implement an ISMS, we need a powerful tool to assess risks within an organization. In this paper, we have proposed a fuzzy expert based system to assess those risks. The most important ability of this model is that it can represent each risk with a numerical value, so the managers can design better plans to achieve the desired level of security for the organization.

There are relationships between the assets in the security cube that must be considered in the future. In fact, existing vulnerabilities for an asset can be considered as a risk for another asset because of these relationships between assets.

Acknowledgements

The authors would like to thank Alexandre Montplaisir for his suggestions. The financial support of Ericsson Software Research and NSERC is gratefully acknowledged.

References

[1] K. Haslum, A. Abraham and S. Knapskog, “Fuzzy Online Risk Assessment for Distributed Intrusion Prediction and Prevention Systems”, In: Tenth International Conference on Computer Modeling and Simulation, IEEE Computer Society Press, pp. 216-223, Cambridge, 2008.

[2] International Standard Organization, ISO/IEC 27005, Information Security Risk Management, 2008.

[3] ENISA, Risk Management: Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools, Technical Department of European Network and Information Security Agency, 2006.

[4] L. Zadeh. Fuzzy sets. Info. & Ctl., 8:338–353, 1965.

[5] D. M. Zhao, J. H. Wang and J. F. Ma, “Fuzzy Risk Assessment of Network Security”, Fifth International Conference on Machine Learning and Cybernetics, pp. 4400-4405, Dalian, 2006.

[6] B. C. Guan, C. C. Lo, P. Wang and J. S. Hwang, “Evaluation of information security related risk of an organization: the application of multi criteria decision making method”, IEEE 37th Annual International Carnahan Conference on, pp. 168- 175, 2003.

[7] Y. M. Wang and T. M. Elhag, “Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment”, Expert systems with applications, pp. 309-319, 2006.

[8] J. A. Zachman, “The Zachman Framework”. http://www.zachmaninternational.com/index.php/home-article/13#maincol

[9] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems”. http://csrc.nist.gov/publications/nistpubs/800- 30/sp800-30.pdf