Fuzzy Method for Risk Management in Computer Security

Seyed Mahmood Hashemi
College of Software Engineering
Beijing University of Technology
People's Republic of China
Hashemi2138@yahoo.com

Jingsha He
College of Software Engineering
Beijing University of Technology
People's Republic of China
jhe@bjut.edu.cn

Abstract: There are many risks for computer systems in network. One goal for developers is designing a management system for threaten risks. However most risks can not be resolved, managing of risks is appropriate approach to empower the system. In this paper, a new method for risk management base on fuzzy logic is presented. Management of risks includes recognition of assets and evaluation of risks for them. In presented method all steps are doing with a fuzzy system. Fuzzy systems allow us to more flexible. Other feature of fuzzy system is the ability to use various opinions. Actually, opinions of stakeholders of computer system are proper resources to manage the risks.

Key-Words: risk management, computer security, fuzzy system

1 Introduction

Nowadays, computer systems have important role in business and other fields. Security of computer systems is a critical part. All components of computer systems involve with security concept, because security is a property of entire system. It is essential that all components and employees adapt to security policies. Security policies are covered by the ISO 27001 standards. The objective of security is protection of computer systems from risks. Computing security in an important concern for researchers and working on issues of technology and development. Although we do not argue that all threats in the developing world can be recognized, analysis of risks is important to understanding threats. In computer systems key role belongs to assets. Assets are defined as anything that has value to the organization [2]. Assets are vulnerability against risks. Risk management is a discipline that exists to deal with non-speculative risks. Those risks are done only when a loss can occur [3]. Risk analysis is the estimation of the probability of an event occurring and the likelihood of loss or failure should it occur. There are numerous risk analysis methodologies available today, some qualitative and other are quantitative. Since the all organizations need to a system to analyze risks in dynamic environment and with ambiguous concepts, this paper presents a new way for risk analysis. Another problem in risk analysis is decision about proper weights for assets. The objective of this paper is developing risk analysis approach with fuzzy system. Presented approach help developers to protect their systems easier and more efficient.

Fuzzy system has two features for risk analysis. Firstly, adaptation to dynamic environment and secondly using the linguistic rules, so experts concerns with security problem.

The rest of this paper is organized as follow: section 2 is about background. Section 3 introduces fuzzy system briefly. Proposed algorithm is presented in section 4. Section 5 discussed about experimental results and section 6 is conclusion.

2 Background

Network security estimation is to detect computer system or network facilities to find security holes and vulnerability possibly imposed by hacker, take measures earlier, and protect network system from threats. The aim of security risk assessment is to comprehend where the current and future risks are, estimate security threat and the influence extent brought by them, and provide gist for establishment of security policy, and foundation and running of information system [4, 8]. [6] shows that it is possible to improve the security of a system by applying program transformations to the existing code base. Bottino (et al. 2006) suggests architecture for secure computers [1]. Risk management plays a critical role in protecting an organization's information assets from security risks [5]. In order to achieve at least an analytical tractability, we need to separate the problem into three major parts: 1-attack and failure modeling 2-impact modeling 3-recovery modeling. Probabilistic approaches can be used to build impact models and estimate the loss due to system failures. The objective of [7] is thus to present and discuss several useful reliability models dealing with the availability analysis of information systems. Two major reasons have triggered the development of this work: (1) lack of a holistic approach to network reliability analyses in the current literature and (2) to enhance the knowledge of formal reliability analysis in the computer engineering discipline. There are number of approaches that trace the system about risk analysis. [9] compares the performances for 4 of them. OCTAVE concentrates on assets, threats and vulnerabilities. One of the main concepts is self-direction. This means that people in the organization must lead the information security risk evaluation. OCTAVE is a methodology that improves the decision making process concerning protection and management of resources in a company. OCTAVE has tree phases: 1-build asset-based threat profile 2-identify infrastructure vulnerabilities 3-develop security strategy and plan [11]. Main objective of CORAS is to develop a framework that exploits methods for risk analysis, semi formal methods for object-oriented modeling'. The methodology is based on UML. The ISRAM methodology is marketed as a quantitative approach to risk analysis that allows to the participation of the manager and staff of the organization. The CORA risk model uses data collected about threats, function and asset, and the vulnerabilities of the functions to calculate the consequence. [12] introduces new concepts to reuse and combine results of the CORAS method for risk analysis. Risk analysis is done for individual components. There exists ISO standards which explain the theoretical risk analysis approach and provide generic guidance on choosing security objectives, like the ISO 27000 standards family, however they do not describe the practical aspects. [10] proposes a formal model for the quantitative risk assessment with the usage of measures and metrics. A metric is an abstract subjective attribute derived from measurement. Metrics measure the attributes of entities. Authors of [14] use a Bayesian Network (BN) to define the risk factors. They present relationship between risks via a case study. [15] analysis five dimensions of information security then uses fuzzy sets to risk priority.

3 Fuzzy System

More previous works can not adapt to real world needing, because they follow crisp steps (include recognizing environment, recognizing assets, weighting assets, weighting risks and so on). In this model, fuzzy system is used for its ability in modeling the non-crisp concepts. Fuzzy

systems are introduced briefly in this section.

Fuzzy systems are knowledge-based systems or rule-based systems [13]. Fuzzy system consist the number of rules. Each rule relates input(s) to output(s). Input(s) and output(s) in fuzzy system are recognized in fuzzy sets. Let a system with uncertainty have the input output relation $y = f_S(x)$, where $y \in R$, and $y \in R^{nX}$. A fuzzy system represents the knowledge related to inputs and output by nC fuzzy rules R_1, … R_C which are expressed in the form

R_i : If ($x_{k,1}$ isr $A_{i,1}$) and … and ($x_{k,nX}$ isr $A_{i,nX}$) then ($y^*_{k,i}$ isr B_i). (1)

Where $y_k=f_S(x_k)$ is an observation vector (x_k, y_k) of the system; $x_{k,j}$ is the j^{th} variable of x_k ; $A_{i,j}$ is the membership function of the fuzzy set for the j^{th} variable in the i'th rule, which determines a fuzzy number for the j'th variable of input space; $y^*_{k,i}$ is the estimate of $y_k=f_s(x_k)$ by R_i; the operator "and" denotes the *t-norm* operation between two membership values; and "isr" denotes the belonging of an object into a fuzzy set. An important contribution of fuzzy systems theory is that it provides a systematic procedure for transforming a knowledge base into a non-linear mapping.

The objective of non-linear mapping is producing output(s) with input(s). Mapping is done when there is a relation. Producing a relation (formula) from rules is role of Inference Engine. Researchers propose many inference engines and each of them has own features (strength/weakness).

4 Problem and Proposed Algorithm

There is a computer system consists numbers of assets. Computer system works in the network (distributed environment). When we say about "system", it means there more components connected to each other. This situation is growing when the system is great and distributed. The great system has numbers of stakeholders. Actually, each stakeholder participates to development of system. Final system (final result after development phase) also has numbers of components and each of them has some risks individually. For each component of system, all its stakeholders have opinions and their opinions must be respected. Actually opinions of stakeholders follow priority and this priority must be done.

In other side, system is doing an environment with various risks. There are two main sources to specify the risks and their weights. First source is the experiments of the environment. Suppose environment (network) has five nodes: 'A', 'B', 'C', 'D' and 'E'. These nodes became disabling 3, 2, 1, 1, 2 times in special period respectively. If this experiment is kept in a log, we know nodes 'C', 'D' are more reliable than nodes 'B', 'E' and node 'A' is worst reliable than other ones. The second resource for specifying the environment risks is set of expert opinions. In this paper stakeholders have the role for writing and retrieval experiments from the log.

Since network environment has risks permanently, security of computer system means management of risks. Therefore problem is management of risks for a system in distributed environment. Solving the problem needs to number of steps. Firstly, there is need to recognition of assets. Experts (stakeholders) who are work in system can guide for recognition the risks of components in the system, but their knowledge is declarative. Another problem is difference of priority for stakeholders. Thus for finding the assets needs to extract the knowledge of stakeholders in order to their importance.

Fuzzy system is proper tool for converting declarative concepts to numerical values. Indeed, fuzzy system allows more experts

with different priorities participant in recognition of assets.

The second step is finding the risks for each component of system in working environment. In this step, there is need to "Learning". "Learning" can be divided into two classes: constraint and scoring. In "constraint learning" approach, the experiments are recorded in a log then new situations are compared with them and similar record is selected. In "scoring learning" approach, a scoring function defined. This paper uses "scoring learning" approach, but we use fuzzy rules insist of scoring function.

The goal of scoring function is presenting how well experiments are fit to analysis system. There are two resources to help us for this duty. The first resource is developers of component and the second resource is experiments. Since a system available in network, usual risks are recorded in a log and this log can be used as the resource for risk management. In proposed algorithm, fuzzy system has the role for defining the scoring function. In fuzzy system, knowledge (such as knowledge of stakeholders and experiments) is represented with rules. Rules include two parts. The fist part of rules (IF-part) is called 'incipience' and the second part of rules (THEN-part) is called 'consequence'. We represent all opinion (stakeholders and developers) and type of components in incipience and consequence of different rules. "Inference Engine" of fuzzy system combines rules and then produces a result from them.

Stakeholders are divided into three groups according to their importance to development the system: "lower", "middle" and "upper". Each of them specified with a fuzzy set.

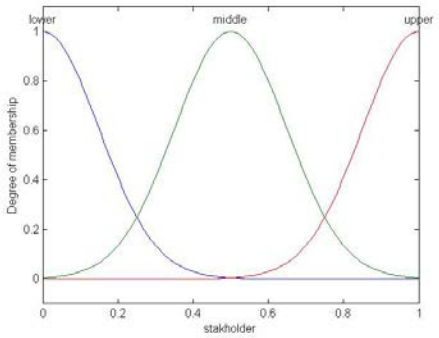

Fig. 1. Membership functions for stakeholders

System's assets are also divided into four fuzzy sets as named: "unimportant", "normal", "important" and "vital".

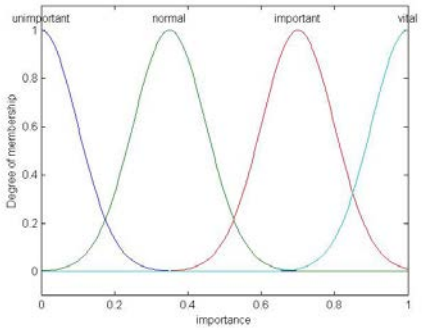

Fig. 2. Membership functions for components

'Incipience' of rules is type of stakeholders and type of component. In other words, each rule declares opinion of specific stakeholder about a component. In 'consequence' there is needed to result. Since system is based on experiment knowledge, result is declarative. Therefore, there is need to numbers fuzzy sets for result. Five sets are designed for results which are called: 'great', 'very good', 'good', 'medium', 'non-acceptable'.

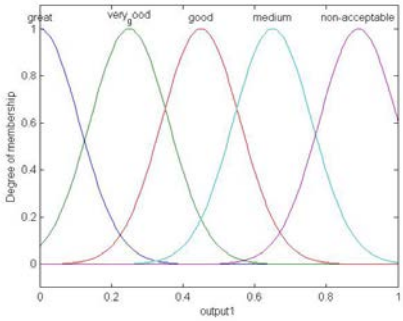

Fig.3. membership functions for result

Now we can define some rules. Actually, definition of rules is a critical role in designing of fuzzy system, because combination of incipiencies provides a space to inference. Thus inference engine can work without error, when all point in input space has at least one rule.

1. If (input1 is upper) and (input2 is unimportant) then (output1 is great) (1)
2. If (input1 is upper) and (input2 is normal) then (output1 is great) (1)
3. If (input1 is upper) and (input2 is normal) then (output1 is very_good) (1)
4. If (input1 is middle) and (input2 is vital) then (output1 is very_good) (1)
5. If (input1 is lower) and (input2 is important) then (output1 is medium) (1)
6. If (input1 is lower) and (input2 is vital) then (output1 is very_good) (1)

Fig. 4. rules

5 Experimental Results

Let there are 5 stakeholders (“S1”, “S2”, “S3”,”S4” and “S5”) and 4 components (“C1”, “C2”, “C3” and “C4”) in the system with various types for each of them. the output of system for 4 components is represented in table 1.

Component	Output
C1	great
C2	great
C3	very-good
C4	medium

Table 1. outputs of the system

These outputs need to interprets with administrative of the system.

6 Conclusion

In this paper, a new scheme for risk management of computer system is presented. Proposed scheme is based on fuzzy system. It means, we have to define numbers sets for ‘Incipience’ and ‘Consequence’. Indeed, there is need to define some rules. Exact definition for incipience, consequence and rules cause proposed scheme specify and manage risks for computer systems carefully. Developers of computer systems can design and program components when there exact specification of risks.

Reference

[1]. Louis J. Bottino, William J. Hughes, “SECURITY MEASURES IN A SECURE COMPUTER COMMUNICATIONS ARCHITECTURE”, IEEE, 1-4244-0378-2, 2006

[2]. Ali Mohammad Padyab, Tero Paivarinta, Dan Harnesk, “Genre-Based Assessment of Information and Knowledge Security Risks”, IEEE, 47th Hawaii International Conference on System Science, 2014

[3]. Dr Ghassan Kbar, “Security Risk Analysis for Asset in relation to Vulnerability, Probability of Threats and Attacks”, IEEE, 978-1-4244-3397-1, 2008

[4]. Liu Mixia, Yu Dongmei, Zhang Qiuyu, Zhu Honglei, “Network Security Risk Assessment and Situation Analysis”, IEEE, 1-4244-1035-5 .2007

[5]. Mohammad Ashiqur Rahman, Ehab Al-Shaer, “A Formal Approach for Network Security Management Base on Qualitative Risk Analysis”, IEEE, 978-3-901882, 2013, IFIP

[6]. Muawar Hafiz, Ralph E. Johnson, “Security-oriented Program Transformations”, ASM, CSIIRW, 1-60558-518-5, 2009

[7]. Suleyman kondaki, “Analysis of information security reliability”, ELSEVIER, Reliability Engineering and System Safety 133 (2015) 275-299
[8]. Rakesh Kumar, Dr Hardeep Singh, “A Qualitative Analysis of Effects of Security Risks on Architecture of an Information System”, ACM, SIGSOFT, software engineering notes, Vol. 38, 2013
[9]. Anita Vorster, Les Labschagne, “A Framework for Comparing Different Information Security Risk Analysis Methodologies”, ACM, Proceeding of SAICSIT 2005, pp. 95-103
[10]. Jakub Breier, Ladislav Hudec, “Risk Analysis Supported by Information Security Metrics”, ACM, International Conference on Computer Systems and Technologies, CompSysTech’11, 2011
[11]. Januszkiewicz Paulina, Pyka Marek, “Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology”, IEEE, Second International Conference on Availability, Reliability and Security (ARES'07), 2007
[12]. Johannes Viehmann, “Reusing Risk Analysis Results, An Extension for the CORAS Risk Analysis Method”, IEEE, International Conference on Social Computing, 2012
[13]. Li-Xin Wang, “a course in fuzzy system and control”, Prentice-Hall International, Inc., pp. 4-7, 1997
[14]. Nan Feng, Harry Jinnan Wang, Minqiang Li, “A security risk analysis model for information system: Casual relationships of risk factors and vulnerability propagation analysis”, ELSEVIER, Information Sciences 256 (2014) 57-73
[15]. Maisa Mendonca Silva, Ana Paula Henriques de Gusmão, Thiago Poleto, Lúcio Camara e Silva, Ana Paula Cabral Seixas Costa, “A multidimensional approach to information security riskmanagement using FMEA and fuzzy theory”, ELSEVIER, International Journal of Information Management 34 (2014) 733–740