Component Security Evaluation Using Fuzzy Logic

Shah Nazir, Muhammad Nazir
Department of Computer Science,
University of Peshawar, Pakistan
shahnzr@upesh.edu.pk, mnazirsajid@gmail.com

ABSTRACT: *Components are the imperative parts and the unit of a system. It plays a fundamental role in smoothly running and proper functionality within a system. A component is said to be secure, if it has towering scope of security. Security is the shield from unauthorized right to use. Unofficial users are informally accessing and modifying the components within a system. Such accessing and modifications are ultimately affects the functionality and efficiency of a system. As software development activities are growing day by day, the security of components is important. In the proposed methodology fuzzy logic (FL) based approach is used to model and evaluate the security of component. The method is designed for some inputs which are availability, authentication, confidentiality, safety and stability.*

Keywords: Component, Secure Component, Fuzzy Logic, Secure System, System Security

Received: 22 January 2015, Revised 23 March 2015, Accepted 29 March 2015

1. Introduction

Component is a unit of system which acts a key responsibility in the functionality of a system. It lessens improvement time for component reuse and parallel development. The protection is well supported by upgrading the existing component in the development of a system. Components are better tested and debugged and the new system turns into less cost. It is always recommended to go for reuse which is not only save time to build up the software from initiate, but also carry error gratis code and the code is always experienced for lots of reuse [1, 2]. When choosing composition of components we have to consider necessary functional, nonfunctional and system appraisal requirements.

Security is the important obligation of a system. It is the protection from unauthorized access and modification. When system is developed from different components, there may be high security threats to the designed system [3]. The threat affects functionality and efficiency of the system. Security classification addresses the basic three essential issues which are the classification security of component in isolation, component compatibility for security properties and to visualized the classified properties of outer entities [4]. The basic concern of component security is how to build the secure component and composition for the component.

The purpose of this paper is to put forward a methodology for evaluating the security of components. A fuzzy logic based approach is tried to model and evaluate the security of components. Fuzziness is beneficial in situation of vagueness and uncertainty. The proposed method incorporates some inputs for security of components which are availability, authentication, confidentiality, safety and stability.

The residue of this paper is as, next section is related work. Section 3 is proposed methodology and section 4 is conclusion.

2. Literature Review

Several different methodologies are planned by different researchers for the security. K. M. Khan and J. Han characterized the security characteristics and suitability of the component. The method uses logic programming for the representations of software component characteristics and comparison [4]. A. K. Ghosh and G. McGraw approach stated the certification to test software components for security properties. It uses white box and black box testing techniques to test and verify the security of software components [5]. K. M. Khan and J. Han proposed a scheme consisting of three steps which are system explicit security requirement, component specific security rating and the assessment technique for the security properties of the component [6]. M. K. Khaled et al. classified the properties of security into two wide categories which are non functional security and functional security. Non functional security component are fixed with component functionality while functional security are outer protection of software components [7].

J.H. Lee et al. used component specification technique and described some definitions of component. The operators defined are, component version, functional requirements, nonfunctional requirements and cooperating component. Z scheme is used for the specification of component [8]. X. CAI et al. proposed quality assurance for both the component and for system of the component. ComPARE is used to assess real life component [9]. M. Moriconi et al. proposed a method in which the various representations of the software system architecture and the required security of the system to architecture level are described. It is illustrated with the help of WOpen open distribution transaction processing reference architecture [10].

In this paper fuzzy logic based approach is used for the evaluation of components security and is quite beneficial in situation of uncertainty.

3. Fuzzy Logic for Evaluating Security of Component

A fuzzy logic based approach is tried to model and evaluate the security of components. The detail of fuzzy logic concepts is given in Zadeh [11]. Fuzzy logic consists of different inputs and member ship function (mf). The inputs in the proposed methodology are availability, authentication, confidentiality, safety and stability.

Different MF used for inputs are: 1) availability are Not_Available, Medium_Available and Fully_Available. 2) Authentications are Low_Authentication, Medium_Authentication and High_Authentication. 3) Confidentiality are Not_Confidential, Medium_Confidential and High_Confidential. 4) safety are No_Safety, Medium_Safety and High_Safety. 5) stability are Not_Stable, Medium_Stable and High_Stable.

Inputs and membership functions are described given below:

3.1 Availability

Availability of a component means the fraction time that is working and functional. It can be affected by component load, errors and malicious attacks. The range of mf for availability is given below in equation.

$$\mu_{(Availability)} = \{0 < x \leq 0.32 = low, 0.30 < x \leq 0.64 = Medium, 0.59 < x \leq 1 = High\}$$

3.2 Authentication

Authentication is the process of determining someone validity of realism and faithfulness. It is mathematically shown below.

$$\mu_{(Authentication)} = \{0 < x \leq 0.33 = low, 0.30 < x \leq 0.62 = Medium, 0.58 < x \leq 1 = High\}$$

3.3 Confidentiality

It is the ethic principle associated with component. Communications are exiting among component and user. Confidentionality can be privileged and cannot be accessed or modified by any illegal user. Confidentiality is shown below in equation.

$$\mu_{(Confidentiality)} = \{0 < x \leq 0.30 = low, 0.30 < x \leq 0.63 = Medium, 0.59 < x \leq 1 = High\}$$

3.4 Safety

Safety is the state of protection from consequences of breakdown or failure. It is also non desirable event which can damage or harm the software component. Mf for safety is given below.

$$\mu_{(Safety)} = \{0 < x \leq 0.33 = low, 0.30 < x \leq 0.61 = Medium, 0.58 < x \leq 1 = High\}$$

Graphically the mf for inputs are shown below in figures.

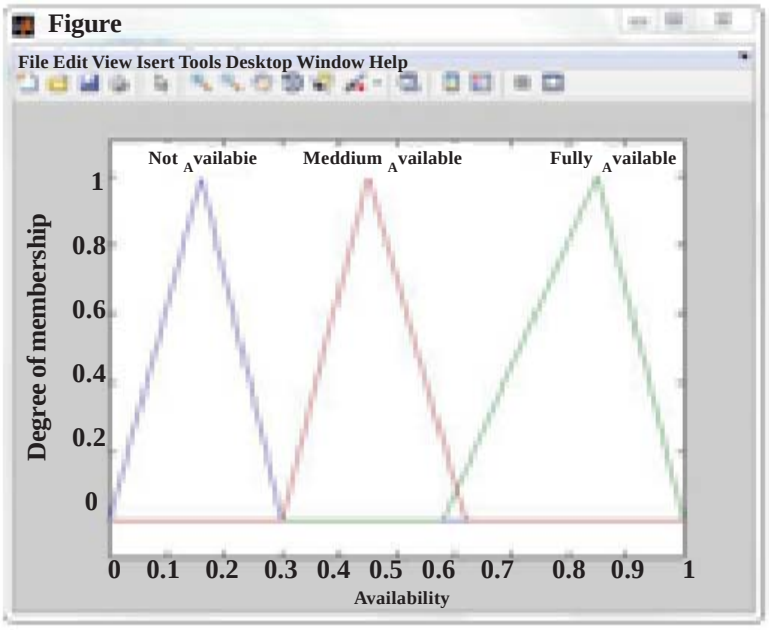

Figure 1. MF for Availability

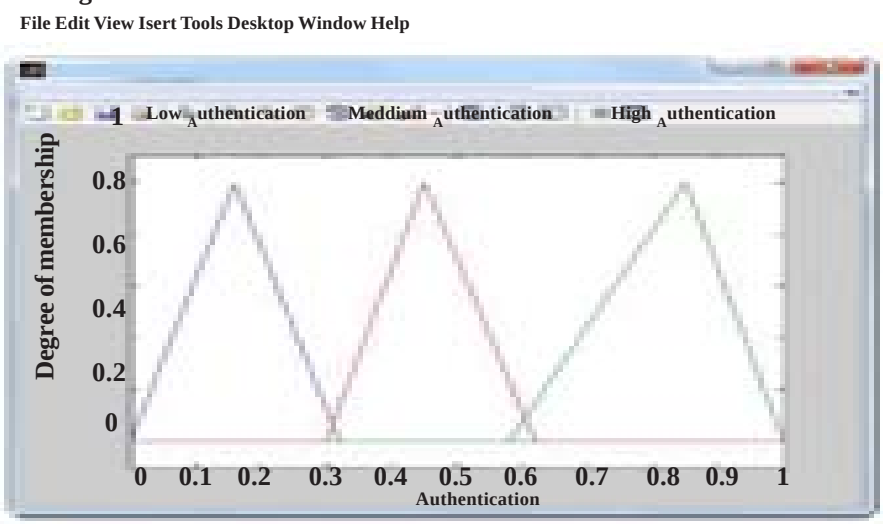

Figure 2. MF for Authentication

3.5 Stability

Competence of an entity to remain unaffected over time under stated or realistic conditions. It is the state, or degree of being stable. Mathematically it is shown below in equation.

$$\mu_{(Stability)} = \{0 < x \leq 0.33 = low, 0.30 < x \leq 0.62 = Medium, 0.59 < x \leq 1 = High\}$$

The FL method is shown in figure 6. It consists of MF, fuzzy rules and the rules are stored in data base.

Using fuzzy tool box the model is designed and is shown in figure 7.

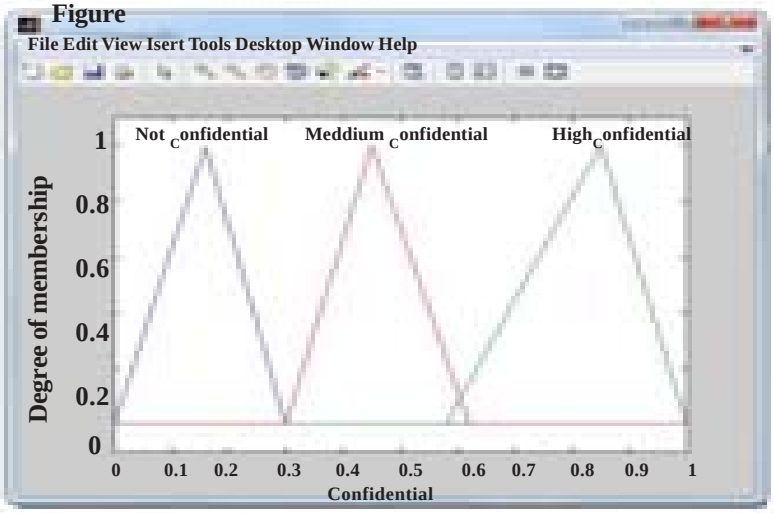

Figure 3. MF for Confidentiality

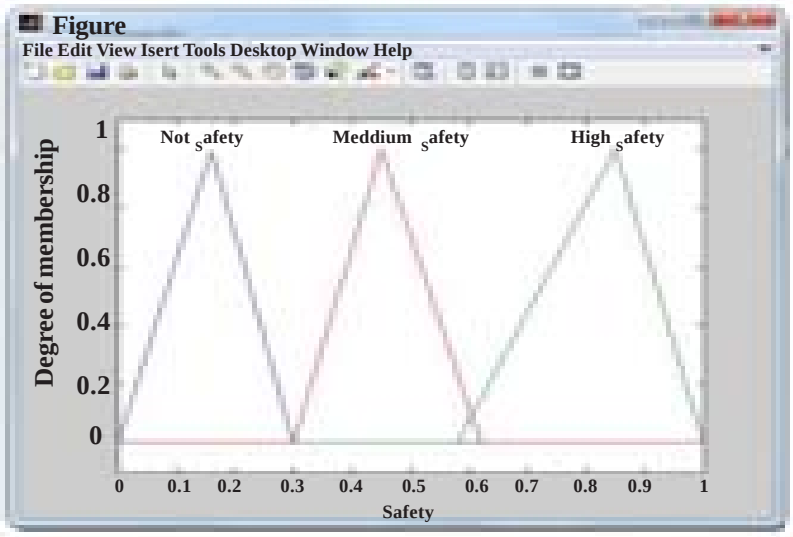

Figure 4. MF for Safety

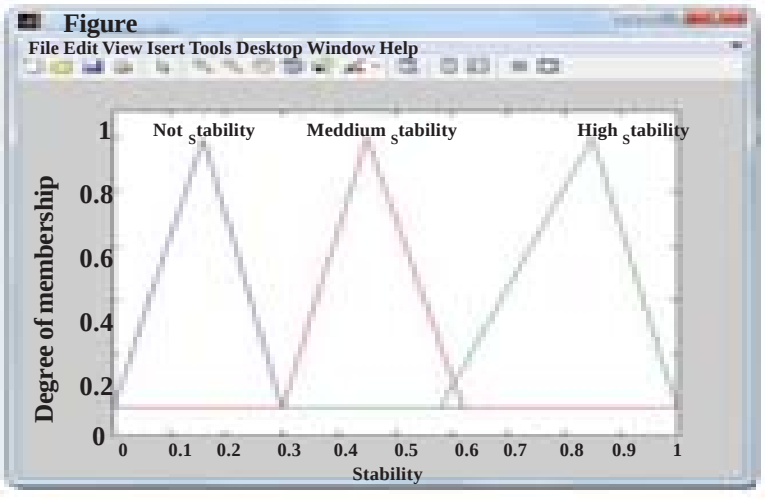

Figure 5. MF for Stability

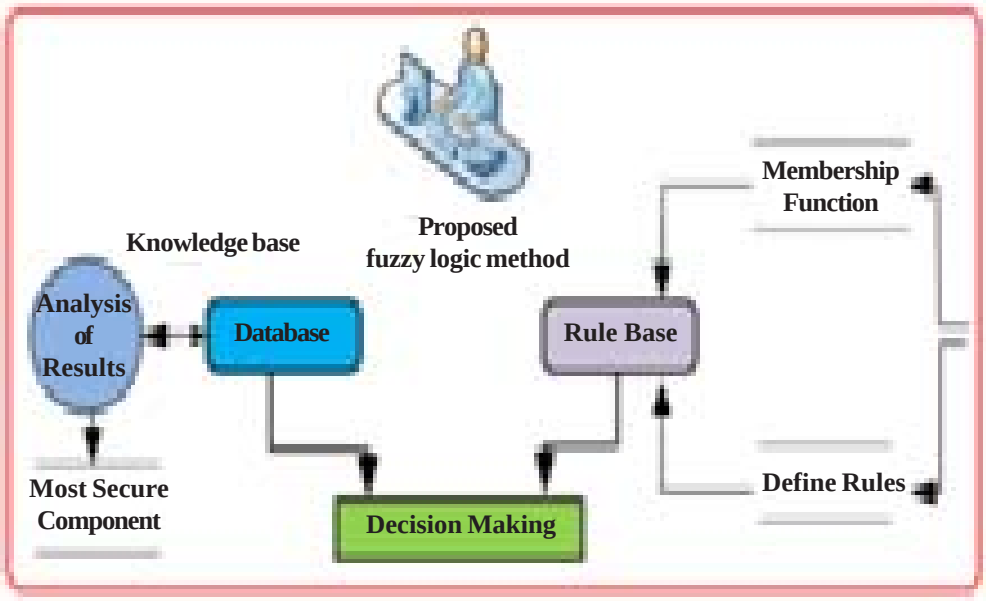

Figure 6. Proposed Fuzzy Logic Model

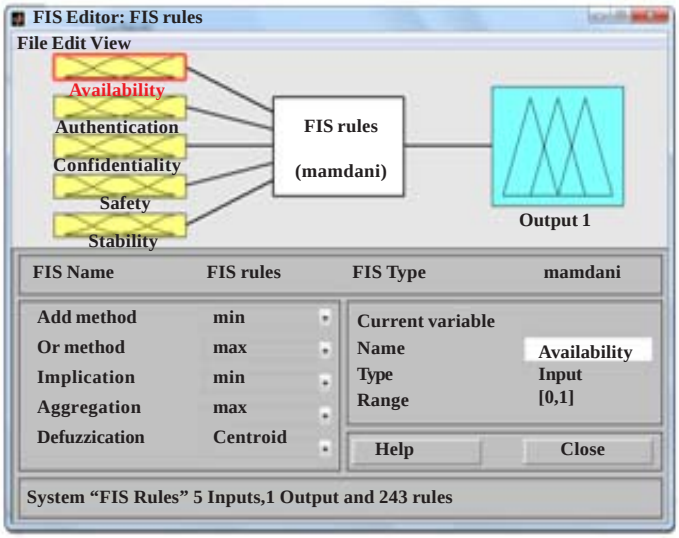

Figure 7. Proposed Model for Inputs and Outputs

The different MF are designed for available inputs and outputs. Figure 8 shows the different MF.

The proposed fuzzy rules are in the form like as:

(1) If (Availability is Not_Available) and (Authentication is Low_Authentication) and (Confidentiality is Not_Confidential) and (Safety is No_Safety) and (Stability is Not_Stable) then (output1 is Low_Secure) (0.1)

(2) If (Availability is Not_Available) and (Authentication is Medium_Authentication) and (Confidentiality is Medium_Confidential) and (Safety is No_Safety) and (Stability is Not_Stable) then (output1 is Low_Secure) (0.3)

(3) If (Availability is Mediium_Available) and (Authentication is Medium_Authentication) and (Confidentiality is Medium_Confidential) and (Safety is No_Safety) and (Stability is Not_Stable) then (output1 is Medium_Secure) (0.5)

(4) If (Availability is Mediium_Available) and (Authentication is Low_Authentication) and (Confidentiality is High_Confidential) and (Safety is High_Safety) and (Stability is High_Stable) then (output1 is High_Secure) (0.8)

. . .
. . .

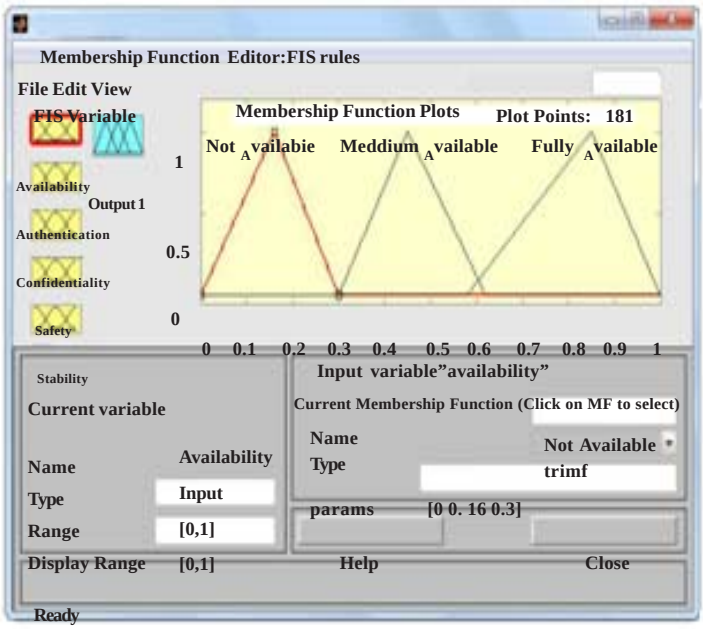

Figure 8. Membership Functions for Inputs and Outputs

243 fuzzy rules for three mf and five inputs.
Using fuzzy tool box rules are designed in rule editor and is shown in figure 9.

On the basis of designed rules and model the security of components can be evolved. Inputs are given according to domain expert opinion in command interface of the designed model as

a = readfis ('FIS Model')
a =
name: 'FIS Model'
type: 'mamdani'
andMethod: 'min'
orMethod: 'max'
defuzzMethod: 'centroid'
impMethod: 'min'
aggMethod: 'max'
input: [1x5 struct]
output: [1x1 struct]
rule: [1x243 struct]

Five inputs of the components which are availability, authentication, confidentiality, safety and stability are given to the designed model in the form as:

Out = evalfis ([0.9 0.5 0.1 0.2 0.2], fismat)
Out = 0.5000

Ou t= evalfis ([0.6 0.8 0.7 0.2 0.9], fismat)
Out = 0.9000
Graphically the inputs and outputs are shown as:

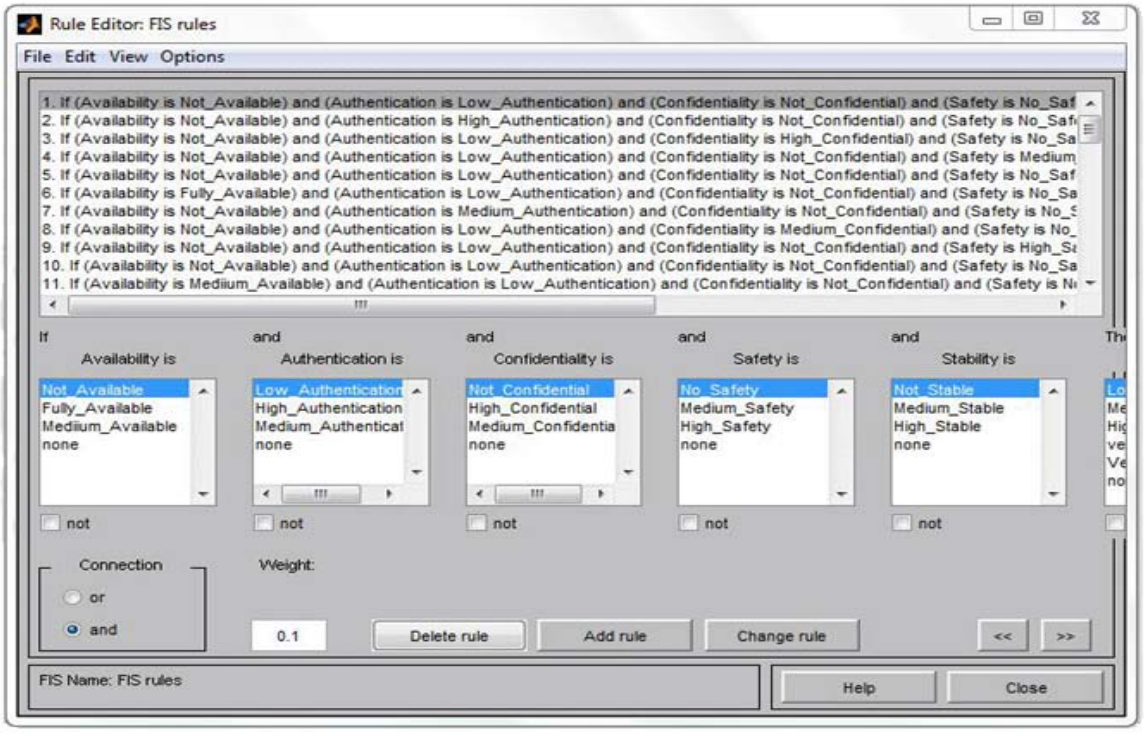

Figure 9. Rule Viewer of Proposed Model

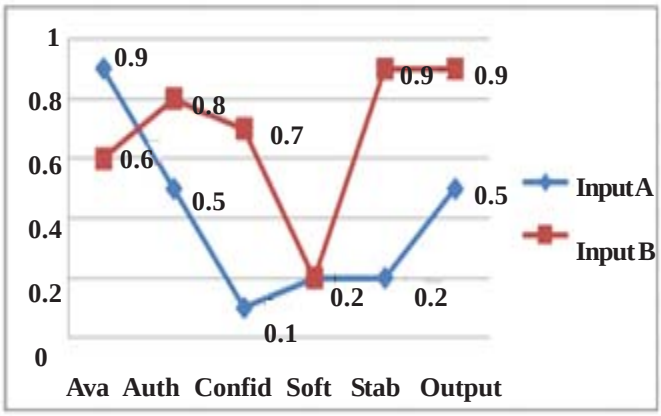

Figure 10. Inputs and Outputs

So from the above results, 0.900 is chosen as the most secure component.

4. Conclusion

Security is the important factor of a component. Most of the components are failing and are not efficiently working due to the lack of availability of security. Security plays a key role in efficient and successful working of a component. Our proposed methodology is quietly very helpful in situation of uncertainty and ambiguity, and thus leads toward to choose the most secure component.

Reference

[1] Sandhu, P. S., Singh, H. (2006). A neuro-fuzzy based software reusability evaluation system with optimized rule

selection, in 2nd International Conference on Emerging Technologies Peshawar, Pakistan, p. 664-669

[2] Nazir, S., Anwar, S., Khan, M. A., Khan, H., Nazir, M. (2012). A Novel fuzzy Logic Based Software Component Selection Modeling, in International Conference on Information Sciences and Application (ICISA) Korea,p. 1-6.

[3] Khan, K., Han, J., Zheng, Y. (2000). A scenario based security characterisation of software components, *In*: Proceedings of the 3rd Australasian Workshop on Software and System Architectures, p. 55-63.

[4] Khan, K. M., Han, J. (2003). A Security Characterisation Framework for Trustworthy Component Based Software Systems, *In*: Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC'03).

[5] Ghosh, A. K., McGraw, G.. (1998). An Approach for Certifying Security in Software Components, *In*: Proc. 21st Nat'l Information Systems Security Conf., Nat'l Inst. Standards and Technology, p. 82–86.

[6] Khan, K. M., Han, J. (2006). Assessing security properties of software components: a software engineer's perspective, in Software Engineering Conference, 2006. Australian, p. 10 p.-210.

[7] Khaled, M. K., Jun, H., Yuliang, Z. (1999). Security Properties of Software Components, *In*:Proceedings of the Second International Workshop on Information Security, p. 52-56.

[8] Lee, J. -H., Yoo, C. -J., Chang,, O.-B. (2002). Component Contract-Based Interface Specification Technique using Z, *International Journal of Software Engineering and Knowledge Engineering*, 12, p. 453-469, August.

[9] Cai, X., Lyu, M. R., Wong, K.-F. (2002). Component-Based Embedded Software Engineering: Development Framework, Quality Assurance and a Generic Assessment Environment, *International Journal of Software Engineering and Knowledge Engineering*, 12, p. 107-133.

[10] Moriconi, M., Qian, X., Riemenschneider, R. A., Gong, L.(1997). Secure Software Architectures, in IEEE Symposium on Security and Privacy, p. 84-93.

[11] Zadeh, L. (1988). Fuzzy Logic, Computer, 1, p. 83-93.