Improving Web Service Selection using Fuzzy Quality of Protection

V.Prasath, R.Buvanesvari, V.Anitha, M.Keerthana

Abstract— We aim to solve the selection of secure web services in a global and flexible manner by introducing a Fuzzy logic method. This paper presents a stride model based evaluation of web service security using quality of protection parameters like spoofing, tampering, reputation, information disclosure, denial of service and elevation of privileges. In this paper quality of protection parameterized tasks that are given to fuzzier where the input values for decision making that are converted into the range between 0 and 1 for selection and choice of the most appropriate web service with respect to quality of protection.

IndexTerms—fuzzy,qualityofprotection,webservicediscovery, web service security

I. INTRODUCTION

Web service [1] framework brings in a new revolution in traditional computing. Through using service oriented architecture (SOA) [2] based on web service technologies, enterprises can now address platform interoperability problems and therefore grasp ever changing business challenges and opportunities. However, most research papers on web service focus on quality of service (QoS) [3] issues, which only have been identified as an important factor in web service selection recently. It is not hard to imagine that service requestors will face a large number of choices of services that can provide the similar function in lack of security mechanism. Current researches concern more about the testing of Web service and rarely about the issue of service security evaluation. Because Web service often includes the critical operations of enterprises, and if there is safety problem, significant losses and serious consequences may be caused but the current research on Web service security [4] mainly concentrated in the following aspects.

A. Vulnerability Test of Web service

Zhang Liang, Zhu Leiming [5] et al., proposed a Web site security analyzing technology based on web vulnerability threat model, and designed Vulnerability Threats Testing Model by using the basic idea of attack graph for reference which can reduce the test cost.

B. WS-Security Testing framework

Shi Yansheng [6] proposed a testing framework of Web services security. The testing framework is used to guide the test procedures of Web services security, which can reduce the blindness of the test activities and improve the tests criterion of the test activities and enhance the test efficiency.

Manuscript received February, 2014

Mr. V.Prasath, Department of Computer Science & Engineering, Pondicherry University/ PKIET/ Karaikal (U.T.Puducherry), India.

Mrs.R.Buvanesvari, Department of Computer Science & Engineering, Pondicherry University/ PKIET/ Karaikal (U.T.Puducherry), India.

V.Anitha, Department of Computer Science & Engineering, PondicherryUniversity/PKIET/Karaikal(U.T.Puducherry), India.

M.Keerthana, Department of Computer Science & Engineering, PondicherryUniversity/PKIET/Karaikal(U.T.Puducherry), India.

C. Analysisng security on applications

Van Solms [7] argues that success in maintaining security mainly depends on people. Security awareness as a means of human security can be improved through comprehensive education and implementing reward punishment mechanisms. It is supposed to create so called security culture. Gap of security between members and management of the organization about information security should be reduced otherwise it potentially become another source of threats in the future.

D. Quality of Protection Determination

Artsiom Yautsiukhin [8] provide a methodology for the aggregation of security requirements. It helps to select the most suitable security configuration according to a contractor's business process and different levels of trust between involved partners. The proposed methodology captures and binds security requirements useful for contractors with ones understandable by clients.

E. Trust and Reputation Management

Le-Hung Vu, Manfred Hauswirth and Karl Aberer [9] present a new QoS based semantic web service selection and ranking solution with the application of a trust and reputation management method to address this problem. It gives a formal description and validate it with experiments which demonstrate that yields high quality results under various realistic cheating behaviors.

II. RELATED WORK

With the increase in the use of web services which are delivered over the public Internet, there is a growing concern about security. Multiple providers may provide similar functionalities with different values of non-functional properties. Their non-functional properties need to be considered during service selection. There are characterized as quality of service. The large amount of security threats existing in web service could be complex and hard to identify during the fault analysis. Consequently, security requirements may not be able to fully protect the service against possible attacks. To avoid from security failure of the web service it need to make it tolerant in the presence of security threats. In order to tolerate the security threats it is required to care for partiality of security in security requirements of the web service. This partiality must be accepted and formally described within the security requirement model for the web service selection [10].

Security for web services means providing authentication, authorization, confidentiality, and non-repudiation as basic representative [11][[12]. Each of these aspects is described below.

1) Authentication verifies are who they claim to be. The result of authentication is a set of credentials.
2) Authorization grants permission for principals to

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

access resources, providing the basis for access control, which enforces restrictions of access to prevent unauthorized use.

3) Confidentiality keeps the message secret. This process requires encryption, which scrambles the message in such a way that only authorized identities can decrypt and see the data.
4) Cryptography provides cryptographic algorithms and protocols for protecting data and messages from disclosure or modification.
5) Accountability ensures security auditing provides a record of security-relevant events and permits the monitoring of a principal's actions in a system. Non-repudiation provides irrefutable proof of data origin or receipt.
6) Security administration defines the security policy maintenance life cycle embodied in user profiles, authentication, authorization, and accountability
7) Non-repudiation proves that one identity sent the data only to another identity. This then proves that the specific transaction was entered into by the recipient, and neither party can refute or deny that it occurred later.

The commonly used method of determining the threat is to classify the threat and determine its composition elements, and STRIDE is a typical threat classification model for security evaluation. Categorizing threats is the first step toward effectives mitigation (Ambler, 2005) [13]. Threats can be classified into six classes based on their effect (Swiderski et al., 2004) [14]:

1) Spoofing: - Using someone else credentials to gain access to otherwise inaccessible assets.
2) Tampering: - Changing data to mount an attack.
3) Repudiation: - Occurs when a user denies performing an action, but the target of the action has no way to prove otherwise.
4) Information disclosure: - The disclosure of information to a user who does not have permission to see it.
5) Denial of service: - threatens the ability of valid users to access resources.
6) Elevation of privilege: - Occurs when an unprivileged user gain privileged status.

This is generally referred to as the STRIDE model. The model was used by Microsoft for categorizing threats (Casteele, 2005) [15]. The model is used by developers and designers to identify and resolve security issues in the application code. This means that the STRIDE model is used to categorize the threats by taking into account their effects on the security of the application (Casteele, 2005).

III. FUZZY RISK ASSESSMENT

The idea fuzzy sets believed that all real-world problems could be solved with efficient, analytical methods and/or fast electronic computers. A fuzzy set can be defined mathematically by assigning to each possible individual in the universe of discourse a value representing its grade of membership in the fuzzy set. Fuzzy set characterized by a function f A(x), which associated with each point in x a real number in the interval [0,1]. It provides meaningful representation of measurement uncertainties and vague concepts expressed in natural language [16].

The level of risk is estimated on the basis of the likelihood of threat value, mapped against the estimated negative impact. The likelihood of each threat value and the impact was determined in consultation with the expert group drawing on their collective experience where it not possible to provide a well founded estimation of the likelihood of an occurrence, the value is appropriate. In many cases the estimate of likelihood depends heavily on the business impact under different conditional consideration [17].

Fuzzy set is applied to capture fuzziness in the form of inconsistencies and vagueness coming from subjective judgments by decision makers. We solved several issues use of this fuzzy logic in secure web service discovery:

- First correctly define the QoP properties that use in the effective ranking methods.
- How to improve fuzzy based web service discovery and the representation of QoP to achieve effective web service selection?
- How to automatically set the risk rating value to service providers attributes?
- Each service consumer should be able to evaluate their own trust.
- It should be robust against possible lying from service providers.

IV. QOP METHODOLOGY

Security represents the secureness of the web service which will be compared to 'optimal security. Six inputs like spoofing, tampering, reputation, information disclosure, denial of service and elevation of privileges are given to fuzzier then fuzzy output is risk rating acquired. We assume that the fuzzy system under consideration has n inputs Q1, Q2,…,Qn (which are one on several security attributes). Each input has five linguistic terms on the input Q1 possesses the fuzzy output {Very Low(vl),Low(l), Medium(m), High(h), Very High(vh} [18].The common fuzzy if-then rule has the following type:

Rule 1: If (Q1 is S1) and (Q2 is T1) and … and (Qn is E1) then f1 (Q1, Q2,…, Qn).

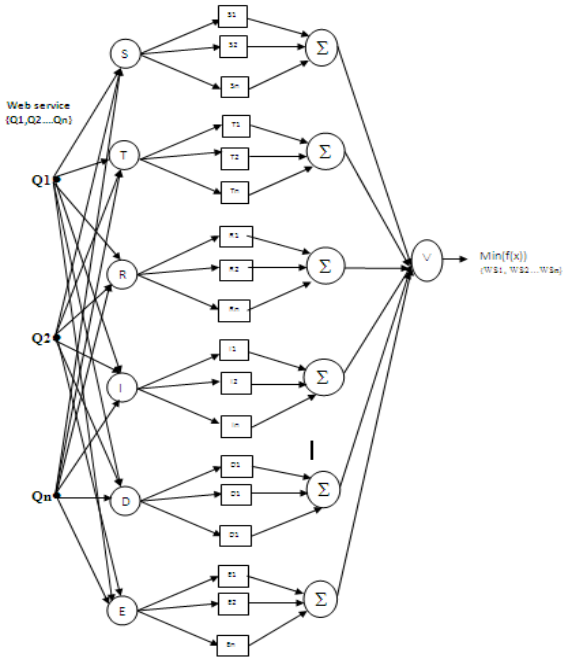

Figure 1. Architecture of fuzzy layered QoP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Stage 1:
To determine the degree of satisfaction of each web service security requirements all possible derivation chains starting from Q1 and ending to Qn should be derived.
Stage 2:
The node in this second layer is a fixed as STRIDE. The weighting value of each rule is calculated by evaluating the antecedent of the rule by human experts, first converting the input values to fuzzy membership values by utilizing the input membership functions and then applying to operator to these membership values.
Stage 3:
In this layer node labeled Σ function is used to normalize the input threat strengths.
Stage 4:
This stage labeled V min {f(x)} which computes the overall output as the summation of all inputs for stride model for each threat defined in web service security.

Table 1. QoP criteria used for evaluating web services

Sl. No	Parameter	Asset	Threat	Description	Measurement
1	Wsdl Scanning	Information gathering	Information Disclosure	It describing the functionality offered by the web service and the parameters required to use it.	Rating
2	Web Method Enumeration	Information gathering	Information Disclosure	Not all implemented methods may be published in the WSDL document	Rating
3	Error message Information Leakage	Information gathering	Information Disclosure	Error messages within SOAP faults can contain detailed platform information and implementation details such as code fragments or stack traces.	Rating
4	Numerical Values	Fuzzing	Information Disclosure	Any value that is only as a numerical value or is expected to be a numerical value.	Rating
5	Base64 Encoded Values	Fuzzing	Tampering	Base64 is used to encode binary data in order to conform to XML specifications.	Rating
6	Character Strings	Fuzzing	Tampering	This verybroad category general guidelines for any data that is not of any particularly classifiable form.	Rating
7	General values	Fuzzing	Tampering	If it is not possible to indentify the nature of the values beings supplied this category provides a general overview of the types of inputs that should be tested.	Rating
8	Sub system parameter	Fuzzing	Spoofing	This category relates to any values that may used to influence output on the client side of the application.	Rating
9	Addressing parameters	Fuzzing	Tampering	System often use addressing information to access information directories.	Rating
10	Logging values	Fuzzing	Tampering	Any value that is logged directly to some medium has the potential to somehow corrupt logs or provide an inaccurate view.	Rating
11	Sql Injection	Injection	Spoofing	Any value that may be used as part of an SQL query should be tested for the ability to change SQL processing in some way,possibly causing data disclosure.	Rating
12	Command Injection	Injection	Tampering	If an internal system is used to execute existing commands and input to these commands is not properly validated,it may be possible to run commands of the user's choosing.	Rating
13	Lpath Injection	Injection	Spoofing	If LDAP queries are constructed directly from user input, this may result in significant system compromise,particularly in the disclosure of user credentials.	Rating
14	Xpath Injection	Injection	Information Disclosure	The use of user supplied input in an XPath query may provide an attacker with the ability to modify the query.	Rating
15	Code Injection	Injection	Elevation of Privileges	If an validated user supplied input is supplied to calls to eval-type functions, malicious commands may be inadvertently executed by the web service	Rating
16	Cipher choice	Confidentiality	Information Disclosure	The choice of encryption cipher will influence the strength of the encryption and the ability for an attacker to successfully crack the encryption and recover plaintext data	Rating
17	Encryption Coverage	Confidentiality	Information Disclosure	Encryption should be applied overall sensitive portions of messages to ensure they are protected against un authorized eaves dropping..	Rating
18	Replay Attacks	Integrity	Spoofing	A replay attack involves the malicious use of a valid message or set of messages that has already been accepted by the web service previously.	Rating
19	Integrity Check Coverage	Integrity	Tampering	Integrity checks should be used to protect important data against unauthorized modification.	Rating
20	Invalid Xml	Integrity	Denial of service	WS-Security and other web sevice security standards are XML-based and their implementations require properly formed XML to function properly.	Rating
21	Unsupported algorithms	Integrity	Tampering	Verify that if unsupported algorithms are requested or the client claims to root support required algorithms,access is denied and processing of the request does not continue.	Rating
22	Separator Injection	Logging	Repudiation	Log entries are commonly delimitedusing a particular separator character.	Rating
23	White Space Injection	Logging	Repudiation	White space characters can be used to modify the appearance of log entries when they are viewed.	Rating
24	Brute-Force and Dictionary Attacks	Authentication	Elevation of Privileges	These types of attacks are typically used against password authentication systems and rely on the ability to repeatedly test potential passwords against the authentication service.	Rating
25	Forged Credentials	Authentication	Elevation of Privileges	Credentials should be issued by an authorized party and verified by the application when presented.	Rating
26	Missing Credentials	Authentication	Spoofing	A user that fails to present credentials should not be allowed access and the application should discard their request.	Rating
27	Token Forgery	Authorization	Elevation of privileges	As SOAP is a stateless message-based protocol ,some mechanism must be implemented to provide authorization between SOAP requests or maintain session state.	Rating
28	Hijacking Attacks	Authorization	Tampering	As SOAP is a stateless message-based protocol, some mechanism must be implemented to	Rating

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

				provide authorization between SOAP requests or maintain session state.	
29	Parameter Tampering	Availability	Denial of service	This broad class of attacks refers to the modification of SOAP request parameters in transit between client and server.	Rating
30	Coercive Parsing	Availability	Denial of service	Coercive parsing is the name given to the class of attacks that involve supplying illegal or malformed SOAP requests to the web service in order to cause undesirable behavior.	Rating

V. VULNERABILITY AND WEIGHT CLASSIFICATION

Fuzzy logic sets are based on linguistic rules to include developer expertise into modeling the threat. In this model Mamdani inference method was used to capturing the expert knowledge in a more intuitive, human-like manner, and for the aggregation of the fuzzy values using centroid technique was exploited for the defuzzification. AND rules are trust values are tightly coupled with one another, i.e dependent on each other. OR rules and a combination of OR and AND rules are used for loosely coupled variables only. The number of rules is decided by an expert who is familiar with the system to be modeled. However, no expert is available and the number of membership functions assigned to each input qualities is chosen empirically by examining the desired input-output data [19]]. However, in our case, with a relatively small set of rules and only six input and one output variables are defined.

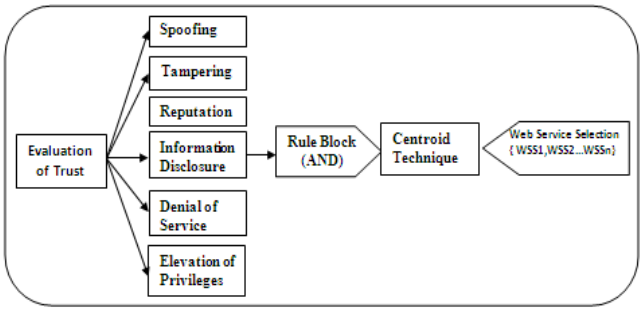

Figure 2. Design System for Fuzzy Quality of Protection

FUZZY RULES: Six fuzzy inputs like Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege then fuzzy output is Trust Rating Rate. Fuzzy rules are implemented below for STRIDE model to test each web service into risk evaluation.

IF (Spoofing is Low) AND (Tampering is Low) AND (Repudiation is Low) AND (Information disclosure is Low) AND (Denial of service is Low) AND (Elevation of privilege is Low) THEN (Trust Rating=Very Low)

VI. TRUST EVALUATION

In order to evaluate the robustness of the chosen fuzzy approach, a comparison with the weighted approach is conducted for STRIDE cases given in table 1 which service providers are deceiving users with wrong trust values [20]. The first steps is to take the crisp inputs (STRIDE) and are fuzzified against the appropriate linguistic fuzzy sets to determine the degree to which these inputs belong to each appropriate fuzzy set. This crisp input is always a numeric value. The fuzzified inputs are applied to the antecedents of the fuzzy operator to obtain a single number that represents the result of the antecedent evaluation.

Membership function says each potential threat that is mapped to a membership value between [0, 1] for five linguistic terms are assigned for each threat as Very low, Low, Rather low, Medium Rather high, High, and Very high. At last the input fuzzy set transforming a fuzzy output of a fuzzy inference system into a crisp output.

According to the vulnerabilities and weights classifications above, the threat value of STRIDE are exclusive vulnerability are gotten for each web service. After weighted summation Σ, the final threat level is achieved for each web service. Then the overall rank can be determined by membership function. The specific formulas stands for the threat value of web service security, O(R) stands for the final overall score threat value.

$$\text{Weight (i)} = \sum_{1}^{n} R(i).S$$

$$\begin{aligned}\text{Overall Rating} &= WS(R) \\ &= \min\{ WS1\ldots n * R(S), WS1\ldots n * R(T), WS1\ldots n * R(R), WS1\ldots n * R(I), WS1\ldots n * R(D), WS1\ldots n * R(E) \} \\ &= \min(WS1\ldots n \{O(R)\})\end{aligned}$$

VII. CONCLUSION

In this paper, we have introduced a new QoP based web service selection and ranking with trust rating management. This paper provides evaluation method based on STRIDE model in web services security that are carried out through threat classification level. Finally fuzzy-based approaches for web service ranking have provided for more realistic applications in representation and evaluation of imprecise QoP requirements. The selection of threat value to be monitored by trusted expert is an interesting point not yet to be mentioned.

REFERENCES

[1] World Wide Web Consortium. Web Service Activity. www.w3.org/2002/ws/.

[2] Z. Stojanovic, A. Dahanayake and H. Sol, "Modeling and design of service oriented architecture", Proc. of 2004 IEEE International Conference on Systems, Man and Cybernetics, the Hague, the Netherlands, Vol. 5, pp. 4147- 4152, Oct. 2004.

[3] D.A. Menasce, "QoS issues in Web services", IEEE Internet Computing, Vol. 6, Iss. 6, pp. 72-75, Nov/Dec.2006.

[4] Jiang Li1chen Hao1 Deng Fei1, 2 Zhong Qiusheng. "A Security Evaluation Method Based on Threat Classification for Web Service". JOURNAL OF SOFTWARE, VOL. 6, NO. 4, APRIL 2011.

[5] Zhang Liang, Zhu Leiming, Wang Kang. "A Website Security Analyzing Technology Based on Web Vulnerability Threat Model" Microcomputer Applications. 2008.24(5):56-58

[6] Shi Yinsheng, Deng Shiwei, Gu Tianyang. "Research on the Web Services Security Testing Technology". Computer Engineering and Science. 2007. 29[10]\

[7] Myung-Hee Kang, Kyung-Nam Kim, Hwang-Bin Ryon."An authorization mechanism for Web Services using an attribute certificate". Proceedings IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 14-16 Oct. 2003, 144~150

[8] Artsiom Yautsiukhin. "Quality of Protection Determination for Web Services". This work was partly supported by the project EU-IST-IP-SERENITY, contract N 27587.

[9] Le-Hung Vu, Manfred Hauswirth and Karl Aberer. "QoS-based Service Selection and Ranking with Trust and Reputation". Management

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

School of Computer and Communication Sciences Ecole Polytechnique F¶ed¶erale de Lausanne (EPFL) CH-1015 Lausanne, Switzerland .

[10] Davoud Mougouei1, Wan Nurhayati Wan Ab. Rahman. "Fuzzy Description Of Security Requirements For Intrusion Tolerant Web-Services", Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia.

[11] J.Scambray and M.Shema, Hacking Exposed Web Applications, McGrawHill, 2002.

[12] Li Jiang, Hao Chen, Fei Deng, Qiusheng Zhong."A Security Evaluation Method Based on Threat Classification for Web Service", Journal of Software, Vol 6, No 4 (2011), 595-603, Apr 2011

[13] Ambler, W. S (2005). Introduction to security threat modeling. Agile Modeling. Available at http://www.agilemodeling.com/ artifacts/securityThreatModel.htm

[14] Swiderski, F. & Snyder, W. (2004). Threat modeling. Microsoft Press Professional Book Series

[15] Casteele, S.V. (2005). Threat modeling for web application using STRIDE model.

[16] Zadeh L.A., "Knowledge Representation in FuzzyLogic,". IEEE Trans. Knowledge and Data Eng., vol. 1, pg. 89.100, 1989 .

[17] Rachna Satsangi1,Dr. Pankaj Dashore 2 and Dr.Nishith Dubey "Risk Management in Cloud Computing Through Fuzzy Logic". International Journal of Application or Innovation in Engineering & Management Volume 1, Issue 4 December 2012

[18] Abdallah Missaoui, and Kamel Barkaoui. "A Neuro-Fuzzy Model for QoS Based Selection of Web Service". J. Software Engineering & Applications, 2010

[19] Simone A. Ludwig, Venkat Pulimi, Andriy Hnativ. "Fuzzy Approach for the Evaluation of Trust and Reputation of Services ". Fuzz-IEEE 2009 Korea August20-24 2009S. Sodiya, S. A. Onashoga, and B. A. Oladunjoye Threat Modeling Using Fuzzy Logic Paradigm Issues in Informing Science and Information Technology Volume 4, 2007.

[20] Colin Wong and Daniel Grz elak, "A Web Services Security Testing Framework", SIFT SPECIAL PUBLICATION, Information security services, Version 1.00.

[21] Duan Youxiang 1 , Gao Yang. "Evaluating Vulnerabilities Quantitatively Based On the Rank of Web Services confidentiality ,Journal of Next Generation Information Technology, volume 2, Number 1, February, 2011.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.