International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 2, February 2014

A Web Service Quality of Protection using AHP Method

V.Prasath

Assistant Professor, PKIET, Karaikal, U.T.Puducherry

ABSTRACT

As the number of Web services on the internet increase, the need for finding the exact web service that matches the user's request also increases. So ranking of web services is required in order to find the right web service. The main goal of this research paper is to achieve security of the web service can be summarized to this single value. In this paper we propose analytical hierarchy process (AHP) to evaluate the weights of criteria instead of collect the weights directly from service consumer. Next to reduce the complexity of involving all the security parameters we follow the greedy approach to evaluate and estimate each and every parameter of web service security.

General Terms

Web Service Security

Keywords

Ws-Security, AHP, Greedy, Service Discovery

1. INTRODUCTION

Web services are one of the most promising technologies for building distributed systems that has the potential of becoming the core of a new web-based middleware platform, providing interoperability between computational services. In this specific context security is very important feature. Nowadays, many companies and organizations implement their core business and application services over Internet. Thus, the ability to efficiently and effectively select and integrate inter-organizational and heterogeneous services on the Web at runtime is an important step towards the development of the web service applications [1]. If multiple Web services provide the same functionality, then a Quality of service requirement can be used as a secondary criterion for service selection. Next high importance of Web services is security. To ensuring the web service to some level of security to real systems has been evident since it has been discovered that most attacks may exploit vulnerabilities [2, 3, 4]. These vulnerabilities stem from web service are poorly designed and developed. Security is a set of non-functional attributes like confidentiality, integrity, availability. The current Universal Description, Discovery and Integration (UDDI) registries only support Web services discovery based on the functional aspects of services. To practically examine the resistance of attacks of a small subset of security patterns that are commonly used in web service applications. To perform this evaluation, it has to built a system with web services security testing patterns and using them to study systems under known categories of attacks to web service applications [5] and determine which aspects of security are enhanced through the use of each security pattern for web service system. This paper will describe a testing methodology for web services security and outline a process that can be adopted to evaluate web services security can be summarized to single value. To define security as a measure of vulnerabilities in the accuracy of a risk or security measurement, analytical hierarchy process is used. In order to render the definition useable, it is necessary to associate the terms in the definition with a measurement scale that represents the security of a system as a value between 1 (secure) and 9 (insecure).

2. RELATED WORK

Several authors conducted performance evaluation studies of WS-Security. Security for web services means providing authentication, authorization, confidentiality, and non-repudiation as basic representative [6]. Each of these aspects is described below

Li Jiang, Hao Chen, Fei Deng, Qiusheng Zhong [7] proposed Web service security evaluation method based on threat classification is proposed, which can process security evaluation to Web service from different angles of view, such as spoofing, tampering, repudiation, message disclosure, denial of service and elevation of privilege, and can provide a referential evaluation index of Web service security for the users through the threat modeling and evaluating the degree of security.

Bachar Alrouh and Gheorghita Ghinea [8] consider and compare the performance of various security mechanisms applied on a simple web service tested with different initial message sizes. The test results show that transport layer security mechanisms are considerably faster than message level security mechanisms.

Artsiom Yautsiukhin. [9] argue that security must be guaranteed for data processing and requirements must be negotiated with a client and inserted into the agreement between a client and a contractor. The problem is that a client and a contractor have different views on how these requirements should look like. We propose a methodology which binds

these views and describes a process for selection the security configuration that helps to achieve negotiated level of protection.

GannaFrankova and ArtsiomYautsiukhinork [10] propose a methodology that identifies the concrete business process providing the highest quality of service and protection among all possible design alternatives. the orchestrator should design its business process aggregating web services in such a way as to make it more efficient from the quality of service and protection point of view.

González, Ricardo Mendoza [11] propose in a theoretical manner including the knowledge offered by the proposed specification based on patterns in a new level for the architectural structure of WS-Security specification, which is currently one of the most popular specifications to establish secure web services.

Duan Youxiang , Gao Yang. [12] says vulnerabilities have been threatening Web Services confidentiality, so it is meaningful to quantitatively evaluate them, which can reflects web services security reasonably and directly, and it will be convenient for user to choose service and deploy security measures. AHP(Analytic Hierarchy Process) algorithm is been involved in this paper to dissect indicator. Operations research and fuzzy mathematical theory are also used to qualitatively and quantitatively evaluate vulnerabilities based on the rank of web services confidentiality.

3. PROPOSED WORK

In this proposed approach as shown in Figure 1, first use of greedy approach to select desired security parameter and the weighting of each criteria will be evaluated by using AHP and then ranking the web services based on this evaluated value. The steps of our approach are shown in below

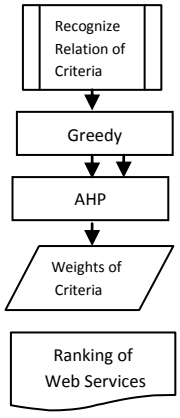

Fig 1: Quality of Protection using AHP

3.1 AHP

The AHP is a very flexible and powerful tool because the scores, and the final ranking, are obtained on the basis of the pair wise relative evaluations of both the criteria and the options provided by the user. In addition, the AHP is simple because there is no need of building a complex expert system with the decision maker's knowledge embedded in it.

AHP is a pair wise comparison method that each criterion is comparing to each other and gets the score with respect to Table 1.The AHP can be implemented in three simple consecutive steps:

1) Computing the vector of criteria weights

2) Computing the matrix of option scores

3) Ranking the options

Table 1. Preference Level

Descriptor Value	Numerical Score
Exceptional	1
Outstanding	2
Excellent	3
Very Good	4
Good	5
Satisfactory	6
Fair	7
Marginal	8
Poor	9

3.2 Computing criteria weights and Pair Wise matrix

In the following the steps of AHP pair wise evaluation are described:

Step1: Sum all the values in each column.

Step2: The values in each column are divided by the corresponding column sums.

Step3: Convert fractions to decimals and find the average of each row. This sum is corresponding to weight of the criterion of the row.

	A	B	C
A	1	x	1/y
B	1/x	1	1/z
C	y	z	1

Fig 2. Evaluation Weight Matrix

In order to compute the weights for different criteria, the AHP starts creating a pair wise comparison matrix A. The matrix A is a m*m real matrix, where m is the number of evaluation criteria considered each entry ajk of the matrix A represents 1the importance of the jth criterion relative to the kth criterion. if ajk >1 ,then the jth criterion is more important than the kth criterion, while if ajk<1,then the jth criterion is less important than the kth criterion, if two criteria have the same importance, then the entry ajk is 1.The

entries ajk and akj satisfy the following constraint [13]

$$a_{jk} \cdot a_{kj} = 1$$

Once the matrix A is built, it is possible to derive from A the normalized pairwise comparison matrix A norm by making equal to 1 the sum of the entries on each column, i.e. each entry jka of the matrix A norm is computed as

$$\bar{a}_{jk} = \frac{a_{jk}}{\sum_{l=1}^{m} a_{lk}}$$

Finally, the criteria weight vector w (that is an m-dimensional column vector) is built by averaging the entries on each row of A norm, i.e.

$$w_j = \frac{\sum_{l=1}^{m} \bar{a}_{jl}}{m}$$

4. RISK EVALUATION

There are many different approaches to risk analysis. Our approach presented here is based on these standard methodologies and is customized for web services security testing methodology based on STRIDE attacks. The STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege) model was used by Microsoft for categorizing threats (Casteele, 2005). 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)[14].

Table 2. Threat Mappings

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	Rating

				overview of the types of inputs that should be tested.	
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	Rating

				inadvertently executed by the web service				age			protect important data against unauthorized modification.	
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		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
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		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
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		22	Separator Injection	Logging	Repudiation	Log entries are commonly delimitedusing a particular separator character.	Rating
19	Integrity Check Cover	Integrity	Tampering	Integrity checks should be used to	Rating		23	White Space Injection	Logging	Repudiation	White space characters can be used to modify the	Rating

				appearance of log entries when they are viewed.	
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 implement ed 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 implement ed to provide authorization between SOAP requests or maintain session state.	Rating
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 attacks that involve supplying illegal or malformed SOAP requests to the web service in order to cause undesirabl	Rating

				e behavior.	

SOAP Sonar web services penetration testing tool used to evaluate web services security under known attacks [15]. Bringing this approach to find attacks that found the major security flaws of the web service meaning the four Spoofing, five Tampering and four Reputation Parameters attacks errors that poses number of threat to web service security.

If we involve all the thirty parameters mentioned in table2, complexity for estimating the effectiveness of web service increases. As a solution to this, we follow the mechanism of greedy approach. The core principle of the Greedy approach is to involve minimum number of input to achieve the final optimized result.

Spoofing Attacks - Sub-system, SQL Injection, Xpath Injection, Replay Attacks.

Tampering Attacks - Code Injection, Invalid XML, Encryption Coverage, Numerical Values, Command Injection.

Repudiation Attacks - White space injection, Separator Injection, HTML Injection, Size Overflow.

We do pair wise comparing between criteria and the below matrix is the result of the comparison with respect to Table1.We assume that based on above attacks exits in number of times with respect of four QoP criteria is gathered and the matrix is prepared.

Table 3. Preference Level for Spoofing

PARAMTER	Sub-system	SQL Injection	Xpath Injection	Replay Attacks
Sub-system	1	2	1	1/3
SQL Injection	1/2	1	1/4	1
Xpath Injection	1	4	1	3
Replay Attacks	3	1	1/3	1

Table 4. Preference Level for Tampering

PARAMTER	Code Injection	Invalid XML	Encryption Coverage	Numerical Values	Command Injection
Code Injection	1	3	1	5	1
Invalid XML	1/3	1	1/4	3	1/2
Encryption Coverage	1	4	1	1/4	1
Numerical Values	1/5	1/3	4	1	1/3
Command Injection	1	2	1	3	1

Table 5. Preference Level for Reputation

PARAMTER	White space injection	Separator Injection	HTML Injection	Size Overflow
White space injection	1	1	3	2
Separator Injection	1	1	2	1
HTML Injection	1/3	1/2	1	1
Size Overflow	1/2	1	1	1

Based on the above table we apply steps1-3 in section 3.3 and the weights of criteria are as follow:

S1=0.22 S2=0.13 S3=0.1 S4=0.25

T1=0.28 T2=0.12 T3=0.22 T4=0.91 T5=0.23

R1=0.37 R2=0.15 R3=0.28 R4=0.20

We assume that based on above example the data of six alternatives STRIDE with respect of four QoP criteria is gathered and the overall matrix is prepared with respect to number of attacks existing in each web service using Soap Sonar test tool.

5. CONCLUSIONS

In this paper we addressed web service security by involving Greedy approach to select desired security parameter using stride pattern and AHP method for evaluation weighting of criteria for each web service for final ranking.

6. REFERENCES

[1] Bin Xu, Tao Li, Zhifeng Gu, Gang Wu "Quick Web Service Discovery and Composition in SEWSIP", Proceedings of the 8th IEEE International Conference on E-Commerce Technology and the 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06).

[2] J. Viega and G. McGraw, Building Secure Software, How to Avoid Security Problems the Right Way, Addison Wesley, 2002

[3] G. Hoglund and G. McGraw, Exploiting Software, How to Break Code, Addison Wesley, 2004.

[4] M. Howard and D. LeBlanc, Writing Secure Code, Microsoft Press, 2002.

[5] Vu, L., Hauswirth, M., and Aberer, K. (2005). "QoSbased service selection and ranking with trust and reputation management". In Proc. of the Intl. conf. on Cooperative Information Systems (CoopIS), Agia apa, Cyprus.

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

[7] 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

[8] Bachar Alrouh and Gheorghita Ghinea. "A Performance Evaluation of Security Mechanisms for Web services", Fifth International Conference on Information Assurance and Security 2009.

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

[10] GannaFrankova and ArtsiomYautsiukhinork."Service and Protection Level Agreements for Business Processes", This work has been partly supported by the IST-FP6-IP-SERENITY and IST-FP6-IP-SENSORIA projects

[11] González, Ricardo Mendoza. "Web Service-Security Specification based on Usability Criteria and Pattern Approach" Journal of Computers . Aug2009, Vol. 4 Issue 8, p705-712. 8p

[12] Duan Youxiang, 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

[13] Analytic Hierarchy Process, www.dii.unisi.it/~mocenni/Note_AHP.pdf

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

[15] http://www.softpedia.com/get/Authoring-tools/Authoring-Related/SOAPSonar-Enterprise-Edition.shtml

[16] Mojtaba Khezrian1, Wan M. N. Wan Kadir2, Suhaimi Ibrahim3, and Alaeddin Kalantari. "A Hybrid Approach for Web Service Selection", /International Journal Of Computational Engineering Research Jan-Feb 2012 , Vol. 2, Issue1.