A Security Evaluation Method Based on Threat Classification for Web Service

JIANG Li[1, 2]
[1] (Software School of Hunan University, Changsha, China)
[2] (Computer and Information Engineering Department of HuaiHua Vocational and Technical College, Huaihua, China)
13789287996@139.com

CHEN Hao[1] DENG Fei[1, 2] ZHONG Qiusheng[1]
[1] (Software School of Hunan University, Changsha, China)
[2] (Computer and Information Engineering Department of HuaiHua Vocational and Technical College, Huaihua, China)
chenhao@hnu.cn,13874522886@139.com

***Abstract*—Web service is a distributed computing model constructed on the basis of open standard technology with the characteristics of loose coupling, language neutrality, platform-independence, etc., how to efficiently evaluate the security of Web service is a challenging research topic. Current researches concern more about the testing of Web service and rarely about the issue of service security evaluation. On the basis of analyzing the current Web services in terms of security threats, a 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. Finally, a case study on SOA application is discussed in detail, experimental results show that the proposed model works efficiently, it can provide valuable reference to check out security vulnerabilities of Web service and help to optimize the system's security design.**

Index Terms*—Web service; security classification; *security evaluation model; security abilities property

I. INTRODUCTION

Web service is a distributed computing model constructed on the basis of open standard technology, and it is widely used in e-commerce and various enterprises. However, due to the characteristics of loose coupling, language neutrality, platform-independence, it is vulnerable to be attacked by hackers or used by the third-party for some improper commercial interests. If the security of Web service is not properly dealt with, some datum may be disclosed and some other security accident or even worse sequences may be caused, so the security and availability of Web service is one of the important factors to restrict the wide application of Web service.

Because Web service often includes the critical operations of enterprises, and if there is safety problem, significant losses and serious consequences may be caused. The security requirements of Web service include confidentiality, identity validation, authorization, integrity and non-repudiation and so on, so how to efficiently evaluate the security of Web service is a challenging research topic.

Aiming at the above security requirements of Web service, some domestic and foreign standardization organizations, companies and research institutes have done related theoretical and applied research. But the current researches concern more about the testing of Web service and rarely about the issue of service security evaluation. According to the characteristics of Web service and the classification method of threat of STRIDE Model, Web service security evaluation model WS-SEM is designed to analyze the quantizing method and the steps to be carried out of security property from the aspects of anti-spoofing, anti-tampering, anti-repudiation, anti-disclosure of message, anti-denial of Service and anti-elevation of privilege, which can provide users with reference evaluation and protective strategy for Web service security. Through the case study on SOA application of an enterprise, the experimental results show that the model works efficiently, it can provide valuable reference to check out security vulnerabilities of Web service and help to optimize the system's security design.

In this paper, Section 2 introduces some related work and further clarifies the meaning of the work. Section 3 presents the basic structure of STRIDE model and the security objectives of Web services; Section 4 defines the security evaluation model of Web service(WS-SEM); Section 5 is the case validation and analysis of the security evaluation model of Web service through the SOA application of a certain enterprise; and Section 6 concludes the paper and points out the next work.

II. RELATED WORK

In recent years, many researchers have achieved much around the evaluation testing of the Web services security, but the current research on Web service security mainly concentrated in the following aspects.

(1) Testing and verifying Web service effectiveness

doi:10.4304/jsw.6.4.595-603

Tsai W T[1] and others extended WSDL document of Web service respectively from the input/output dependencies, calling sequence, concurrency sequence stipulation and layer functional description these four aspects, and make the WSDL document provide more information for the test, which makes the test of Web service easier and ensures the security of Web service. Later, Tsai, W T [2] and others put forward a strategy by using the strengthened UDDI server to verify Web services. The testing of UDDI register center mainly includes check-in and check-out. The service passed the check-in test will successfully be registered to UDDI center, while the unqualified service is refused to register. After receiving the service request, the Test Master of UDDI register center query the qualified service through the check interface and version information in the UDDI directory and regress test the candidate service.

Heckel R and Mariani L[3] proposed a GT rule-based pre-registration test. At first, the service provider provides WSDL interface document and behavior criterion files. Then, the service provider issues the WSDL document and behavior criterion files of the service to UDDI register center. The UDDI register center will automatically create the test group according to GT rules and execute concrete test cases through the remote-calling service, and at last, UDDI register center will judge whether the service can be passed according to the return result. Only the service passed the test can be allowed to officially publish at UDDI.

Run et al [4], in the traditional UDDI model, use CA mechanism of PKI to ensure the credibility of the message of service QoS, namely, adding QoS certifiers on the original model, and its main task is to attest the issued services and verify the message of consumer service QoS.

Carroll et al [5], from the semantic angle, use digital signatures and resources using statement technology to provide trust for the use of RDF resources, including the semantic Web service.

(2) Analyzing the test to the vulnerability of Web service security

Zhang Liang, Zhu Lei-ming[6] et al., from People's Liberation Army Institute of Electronic Engineering, proposed a Web site security analyzing technology based on web vulnerability threat model, and designed VTTM (Vulnerability Threats Testing Model) by using the basic idea of attack graph for reference. Applying VTTM model to the vulnerability test of Web site can help the testing personnel high-efficiently and accurately determine the greatest threat to Web site and the best test steps, which can reduce the test cost. Also, model it with the example of SQL injection and accurately found that the greatest threat to Web site by solving the model.

(3) Analyzing the test to the reliability of Web service

Web service shall ensure not only the correctness of service function but also its performance and high reliability. Currently, during the research on the reliability of Web service, error injection technology is an important research area. Wu Lei and Li Xinke [7] from Anhui University of Technology, proposed a method by using the improved error injection technology of network layer to test the reliability of Web service based on SOAP. Test the reliability of Web service exchange by injecting the significant error into SOAP message.

(4) Authenticating the identity of the user access to Web service

Professor Liu Zhenpeng[8], from Hebei University, proposed a secure authentication method based on the analysis of filtering technology of WS-Security and J2EE platform. And this authentication method uses a third-party authentication center to provide authentication message, in which at first the SOAP messages containing authentication message passes through filters before arriving at the Web service; if the filtering succeeds, the authentication is believed to have passed. Then you can access or use the service to achieve reliable authentication. At the same time this method will be applied to the design of a federal identification authentication system, and the test results indicate that the identification authentication method is feasible and secure.

(5) Testing framework of Web services security

Shi Yansheng[9] from Beijing Institute of System Engineering, 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. Then they explored and discussed the testing technology of Web services security from security test and vulnerability test.

The above researches discussed the creating methods of evaluating and testing Web service security from different angles with the aims to ensure the authenticity, validity and integrality of the issued service messages, which in some way avoided the threat to Web service security. However, there is little research on the quantitative evaluation of the Web service security degree, which can be shown in the following two aspects:

The first is the Web application in different environment. Although the related security risk attribute is basically the same and similar, the possibility and affecting degree of different security risk happen in different situation are greatly different. The current evaluation and analysis on Web services security seldom show the differentiation, which result in the surface research of most security evaluation without fine and deep study in the level of point, line and grain degree.

The second is that in spite of all kinds study on security problems, there is not one and the only standard to prove what is the absolute security and what is absolutely unsafe. But it is possible to find out a quantitative method to compare the same or similar condition and evaluate which application's security degree is higher or lower according to the uniform evaluation criterion and method and to be used as reference when selecting. However, there is little research about this aspect in this field.

III. STRIDE MODEL AND THE SECURITY OBJECTIVES OF WEB SERVICES

A. STRIDE model

Threat is the potential risk launched by the attackers against the system's security vulnerabilities, and threat modeling is an indispensable part in the life cycle project of security development, which classifies and analyzes the threat the system facing and help the system designers to improve the system security design through systematic inspection of the design and system structure. The basic point of safe threat modeling is: it is impossible to establish a secure system unless you know the threat of the system and take measures to mitigate it [10]. 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.

STRIDE is the acronym of Spoofing, Tampering, Repudiation, Message Disclosure, Denial of Service and Elevation of Privilege.

(1) Spoofing: it means to imitate others on the computer and illegally access and use other user's authentication message (such as the user name and password).

(2) Tampering: it involves maliciously modifying the datum, unauthorized altering the permanent datum (such as the datum stored in database) and altering the datum during transmitting between two computers in an open network.

(3) Repudiation: A user rejects activities, and there is no way to prove that he is refusing to abide the agreement. Repudiation includes that the user can refuse to carry out movements without any validation of a third party.

(4) Message Disclosure: it means to disclose the message to the individual without access privilege or let the intruder read the datum that transmitting between two computers.

(5) Denial of Service(Dos): Dos attack will use some method (Such as: let the Web server unable to obtain or use) to make the effective users can not use certain services.

(6) Elevation of Privilege: it means that the users without using privilege can get the access privilege, so there is enough access privilege to damage or destroy the whole system. Commonly, the attacker effectively intrudes all the system lines of defense and makes he become a trusted member of the system.

B. Security objectives of Web service

The hidden trouble of Web service security Web embodies many aspects, including the factor of a network environmental and the factor of calculation mode, which can be grouped into two: the attack to datum, such as wiretapping, tempering and re-attack, etc. and the attach to system, such as unauthorized access, authorization violation, denial of service[11] and so on.

In order to eliminate the hidden trouble of security Web service faced and meet the above requirement of Web service, the security objectives of Web service shall include the following five aspects [12]:

(1) Confidentiality: Ensure that the unauthorized users or entities can not steal messages. In a network environment of Web service, maintaining the confidentiality of message is important to extend the application. Therefore, we shall prevent illegally access message and stealing messages in the process of transmitting. As for Web service environment, the method of encryption can be used to encrypt a series request and response of Web service transmitted on Internet in order to ensure the confidentiality of the datum. The method of encryption is particularly applicable to this "multipoint-multipoint" communication in an open network environment.

(2) Integrality: ensure that the datum will not be damaged accidentally or deliberately and kept integral and uniform. Integrality does not mean to avoid tempering the transmitting message, but means if the message is tempered, the communication sides can detect this temper and give response to the corresponding strategy. Because in the un-trusted channel, it is impossible to completely ensure that the message not be tempered in the process of transmitting to the destination, we shall judge the fact whether the message is tempered by inspection. The integrality of datum is generally achieved by hash algorithm.

(3) Non-repudiation: Ensure that the message sender can't deny or disaffirm the message transmission and shall provide the entities with reliable mark during the transmitting process. In the network application, to realize the non-repudiation has important realistic significance, for example, the consumers of e-commerce web site can't deny its order request, and the Web-site server can't deny the response of the order either. Generally, non-repudiation is realized by unsymmetrical secret key encryption, and the sender uses private key to encrypt the abstract of the sending message, that is digital signature. While the private key can only be kept in the sender, so others can not use the sender's private key to carry out digital signature. So long as the signature validation by using the sender's public key is successful, it can prove that the sender has sent this message. In the Web service environment, for the transmitted XML message, using XML signature operation can ensure the non-repudiation of the sending behavior.

(4) Identity validation: the entities provided suitable identity certification can access the enterprise application and datum, while the entities can not provide suitable identity certification is refused to access the enterprise's resource.

Web service can use many different identity validation system, and the familiar identity validation system are identity validation based on operation system, identity validation based on Web server, identity validation based on order, Web single log on, client /server single log on and biometrics.

(5) authorization: authorization refers to the awarding of privilege, including awarding the access privilege and ensure the sender be authorized to send message. In the

secure network environment, access control is to limit and control the ability of access to the host computer and application. In Web service environment, authorization is to award entities permission to access Web service resource, and provide basis for access control. The main purpose of identity validation is authorization. The typical authorization strategy is to award access to different recourse according to different collection of the validated users, such as role, group or privilege. Authorization strategy can limit the access to many different resource collections: host computer, documents, Web pages, application interface, methods, cases and database records, etc [13].

IV. WS-SECURITY EVALUATION MODEL

A. Model Design

According to its own features of Web service and threat classification method of STRIDE model, a Web service security evaluation model(WS-SEM) is proposed.

Definition 1: WS-SEM is an evaluation model for the capacity property of WS-Security, which can be denoted by the following four elements:

WS-SEM (A, P, F, S), Where A is the property set of WS-Security abilities; P is the weighting factor; F is the set of trust function of a variety of Web security; and S, the set of a variety of evaluation strategies.

Definition 2: the set of anti-threat ability property of Web service A= {As, At, Ar, Ai, Ad, Ae}, including:

(1) As: the ability of anti-spoofing. In the Web services, the commonly used method is identity validation, and the accuracy of validation determines the strength of anti-counterfeiting capabilities of WS. The related realizing criteria and evaluation index sources include SAML, Kerberos, DSS, GSS, Liberty, WS-Security and WS-Federation and so on.

(2) At: the ability of anti-tampering. In the Web services, message integrity validation method is generally used, thus the ability to ensure the message integrity determines the ability of anti-tampering of WS. The related realizing criteria include WS-Security and XML Signature.

(3) Ar: the ability of anti-denying. In the Web services, the method of signature is generally used, thus the ability to ensure the authenticity of the signature determine the ability of anti-denying of WS. The related realizing criteria include WS-Security and XML Signature.

(4) Ai: the ability of anti-leaking message. In the Web services, the method of message encryption and securing communication channels is commonly used, thus the ability of ensuring the safety of communication channel capacity and the strength of message encryption determines the ability of anti-leaking message of Web services. The related realizing criteria include WS-Security, XML Encryption, XKMS, SSL/TLS, HTTPS, WS-Privacy and P3P, etc..

(5) Ad: the ability of anti-refusing service. It refers to the ability of keeping the system away from the critical condition. There are two types of refusing service attacks: one is to overload the system (the most common is the DDOS); the second is to make the system run into the error. These two methods are essentially the same, and both of them make the system enter the critical condition. So the ability of keeping the system away from the critical condition determines the ability of anti-refusing service of Web service.

(6) Ae: the ability of anti-elevating privileges, In the Web services, a reasonable distribution strategy of privileges and effective audit mechanism is the effective means to reduce of privilege and escalate attacks, so the reasonability of distribution strategy of privileges and the effectiveness of audit mechanisms determines the ability of anti-elevating privileges of Web services. The related criteria include NIST SP 800-92.

Definition 3: Weighting factor P refers to the weighting influence coefficient that the anti-threat ability property of Web service accounts in the security assessment model, and the weighting factors collection P={Ps, Pt, Pr, Pi, Pd, Pe}.

Definition 4: Security trust function F is the mapping relationship between security property and credibility degree of the security.

$$F= f(A_k) \qquad (k \in A)$$

Where as A is the property collection of security ability and f is the influencing factor of the security function based on security property.

Definition 5: the strategy set of security evaluation S is the corresponding security strategy set when evaluating the degree of security aiming at security ability property of Web service

$$S= \{f(As), f(At), f(Ar), f(Ai), f(Ad), f(Ae)\}$$

B. Quantization of the security ability property index

In the previous WS-SEM model, A represents the collection of Web service security ability property, which carry out the multi-angles evaluation on the security ability property from anti-spoofing, anti-tampering, anti-denying, anti-leaking of message, anti-denial of service and anti-elevating privilege these six aspects. In order to collect the related index of Web service security ability property and provide quantitative reference index for the sequential Web service security evaluation, the following part will analyze the basic idea and reference method of quantizing the index of Web service security ability property.

1. The ability of anti-spoofing A_s

The basic idea of quantitative evaluation of the ability of anti-spoofing is to carry out the inspection test of anti-spoofing to the Web service and get the quantitative value of anti-spoofing ability by the means of simulative identity cheat, agreement cheat, violent deciphering and hacker attack with the tool from the third part. In the aspect of concrete implementation measures: we can set the alternation of plaintext and Web service, delete the validation of log on code, list out the users/password after intercepting and capturing part of the messages the user submitted when log on and other means.

2. The ability of anti-tampering A_t

The basic idea of quantitative evaluation of the ability of anti-tampering is to carry out the security inspection of the Web service system by the means of simulating the message tempering requesting forgery and the attack tool from the third part. In the aspect of concrete implementation measures: we can manually modify the quest to match the unmodified and modified results; intercept and capture or manually produce several parts of request in advance, and record the return result; roll back the datum to the state before request and manually modify the plaintext and the password of the request; send the parts to the Web service by simulating the user through program and then check whether the return result is the same as that of the original return. We can also automatically construct the tempered forged request with tools and send out them timely and some other means.

3. The ability of anti-denying A_r

The basic idea of quantitative evaluation of the ability of anti-denying is to carry out the security audit of the users operation in the Web service system by the means of holding back the identity, auditing the record, auditing the terminal, verifying the operation and other means.

In the aspect of concrete implementation measures: the following methods can be used to audit the users' operation:

(1) Through the association of operation IP/ Mac address, operator, operation time, count and record the corresponding operation IP/Mac address datum of the operator in a series time.

(2) Investigate whether the user has used CA, electron seal and other means to mark the operator's identity in the process of using.

(3) Select the user's request by sampling, modify the operator's information and observe whether the operation is successful.

4. The ability of anti-leaking the message A_i

The basic idea of quantitative evaluation of the ability of anti-leaking the message is to carryout the security inspection of message to the Web service system by the means of intercepting the data packet, scanning the security vulnerability, deciphering the order and cipher text, bypass pervasion of message and other ways. In the aspect of concrete implementation measures: we can intercept and capture the user's request, modify the plaintext and cipher text and sent to Web service, then observe whether the operation is successful or not; violently decipher the cipher text part and check whether it can be deciphered in the specified time, then we can get some corresponding quantitative index datum of the ability index of anti-leaking the message.

5. The ability of anti-denial of service A_d

The basic idea of quantitative evaluation of the ability of anti-denial of service is to carry out DDOS simulative attack to the Web service system and validate its ability of anti-denial of service by the means of forging a large number of service requests and combining some pressure test tools from the third part. In the aspect of concrete implementation measures: we can carry out DDOS attack to Web service by combining with some hacker attack tools, initiate request to Web service with apache pressure test tools, simulate the users to operate orders and send out timely by constructing a large number of data packets with ping order, and then observe whether the Web service will response normally.

6. The ability of anti-elevating privileges A_e

The basic idea of quantitative evaluation of the ability of anti-elevating privileges is to carry out simulative attack to the Web service system and validate its ability of elevating privileges by the means of calling the simulative over-privilege method, elevating the user's privilege, violently deciphering and other means. In the aspect of concrete implementation measures: after setting the user's various privilege matching, the system administrator will use the loophole scan of the some low privileged users (such as guest users) and try to escalate the user's privilege with some hacker attack tools, then inspect the system privilege defending mechanism and get some corresponding quantitative index datum of ability index of anti-elevating privileges.

The above has provided the basic quantitative idea and reference method for the evaluation of Web service security property from different aspects, but what each kind of security ability property displays is the integrate response of the property's anti-threat possibility, risk degree and being attacked rate.

$$A = C_n \times O_n \times R_n \qquad (n \in A) \qquad (1)$$

Of which, Cn represents the risk degree, it is the quantitative value of the threat severity; On represents successful attack rate，it is the quantitative value of the successful threat attack; Rn is the attack factor, it is the quantitative value of popularity and maturity of the threat attack technology. The key to quantizing the security ability property of Web service is to quantize these three main factors.

The quantization of threat severity consulted to "DREAD" arithmetic, and the created grade property is as follows:

D: damage potential, ranges [0,1]；

R: reproducibility, ranges [0,1]；

E: exploitability, ranges [0,1]；

A: affected users , ranges [0,1]；

D: discoverability, ranges [0,1]；

Definition 6: the grade property collection of threat severity Z={D,R,E,A,D}.

$$C_n = \frac{\sum_{i \in Z} Zi}{5} \qquad (n \in A) \qquad (2)$$

Of which, Cn represents the risk degree; Zi represents the grade property of threat severity.

The quantitative value of the successful threat attack rate:

$$O_n = \frac{S}{T} \qquad (n \in A) \qquad (3)$$

The quantitative means of On is gained from the attack testing result, where T is the total times of attack test and S is the times of successful attack.

C. Dos Evaluation

To reasonably evaluate the security of Web service and calculate the security value is a reliable prerequisite and foundation of determining whether the Web service is safe or not. We can evaluate and measure the security of Web service from the aspects of anti-spoofing, anti-tampering, anti-repudiation, anti-disclosure of information, anti-denial of Service and anti-elevation of privilege.

Definition 7: Degree of security, dos in short, is a measurement value to measure the anti-attack ability of Web service and a integrate function to the degree of security the Web service can reach as well as the quantitative basis of classifying the security relationship.

$$dos = \sum_{k \in A} f(A_k) \times P_k \tag{4}$$

The range of dos is 0<dos≤1, the bigger the value of dos represents the higher of the system's security degree and the smaller of the risk faced, contrarily, the lower of the system's security degree and the greater of the risk faced. Where A represents the property set of security ability, f (Ak) represents the influencing factor of the security ability property which acts on A, and Pk is the corresponding weighting factor. And f(Ak)*Pk is the security degree of K property.

According to the experience, the reference range of security degree is shown in table Ⅰ:

TABLE I.
REFERENCE OF DOS RANGE

Dos quantitative value	Reference security degree
0<dos≤0.5	low
0.5<dos≤0.8	middle
0.8<dos≤1	high

The general steps of Dos evaluation is as follows:

Step 1: classify the threat to Web service according to STRIDE model;

Step 2: aiming at the threat of each class, use the current corresponding attack technology to test the security and get the quantitative value of the successful attack rate;

Step 3: determine the mapping relationship between the security property and the security trust function;

Step 4: determine the corresponding weighting factor $P_k(k \in A)$ according to the situation of each security property existing in the application model;

Step 5: according to the corresponding basic quantitative value gained above, use the security evaluation formula to calculate the security quantitative value of the Web service.

V. CASE ANALYSES IN APPLICATION

A. Application Background

The following is a case study of an enterprise's SOA application system. As a medium-sized manufacturing enterprise, it has completed the first phase of SOA business process transformation project, and the SAP materials management, CIM production management and other core businesses have adopted Web service mode in encapsulation. The overall structure diagram of the system is shown in Figure 1.

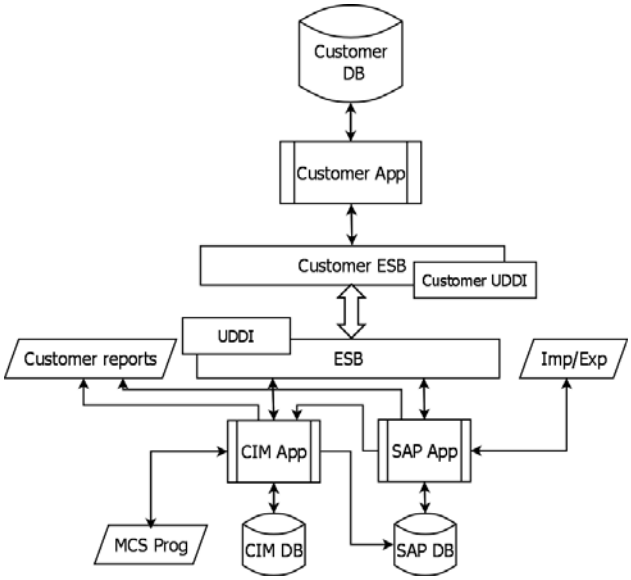

Figure 1 Structure Diagram of SOA Application System

B. Experiment steps

Step 1: to deeply understand and analyze the application realization and system framework of the evaluation system so as to master the application situation of Web service;

Step 2: to carry out the threat modeling and risk evaluation of SOA application system by using STRIDE model and WS-SEM evaluation model;

Step 3: to enact the basic parameters and influencing factors in the process of quantization the security ability property index according to the requirements of the model;

Step 4: aiming at each threat of SOA application system, use the current corresponding attack technology to test the security, and according to the quantitative method of security ability property index stated in section 4 to collect the original test datum, then get the most basic security property index quantitative value through many times of experiment.

Step 5: to calculate the value of dos by combining each security property index quantitative value and the enacted basic quantitative value from the experiment, and get the dos quantitative value of Web services in the SOA application system, and then put forward reference for the system administrators to find the weak links in security defense and optimize the design of system security.

C. Threat analysis

Use STRIDE model and WS-SEM evaluation model of Web service to analyze SOA application system and check whether there is any S, T, R, I, D, or E threat exists in the components or process by analyzing how each threat of STRIDE model influence each component as well as each connection or relationship between the solution groupware and other solutions groupware, and write it down.

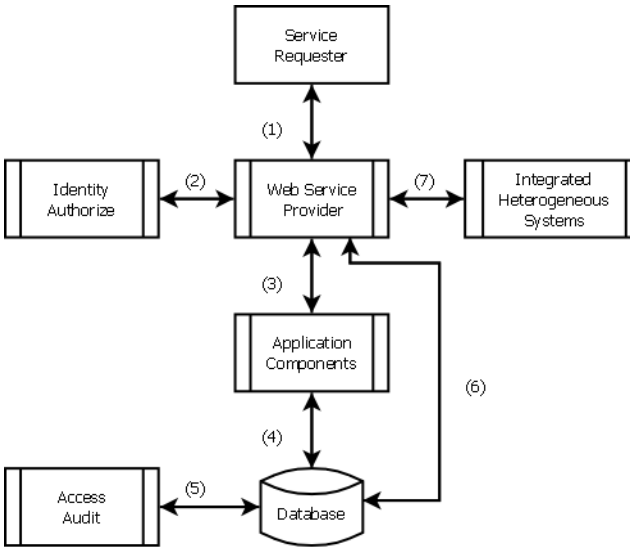

Figure 2 STRIDE Threat Modeling

According to Figure 2 and with the reference to WS-SEM security evaluation model in section 4, the analyzing process of threat and risk is shown in table II.

D. Enactment of the basic parameters and influencing factor in the threat experiment

According to formula 4.2, the calculation formula of risk degree, calculate the quantitative value of corresponding threat severity to each security property in the project, and see table III.

According to the definition of weighting factor in section 4 and with the combination of the threat distribution in table 5.1, enact the weighting factor; according to the popularity and maturity of the corresponding threat attack technology, enact the attack factor; see table IV.

TABLE Ⅱ.
ANALYZING THE THREAT AND RISK

Threat	STRIDE	Control Protocol	Threat identification
1	S,R,I,D,E	HTTP,SSL	The third-party intruder access service providers' service by counterfeiting the legitimate users (S), customers and suppliers deny the de facto and self-defeating behavior (R), third-party intruder detect the content of communications between customers and suppliers (I), customers or third-party intruder maliciously constructed critical conditions of service to make the service provider refuse service (D), customers trying to improve their privilege (E)
2	I,D,E	LDAP, Kerberos	An intruder who has entered the system detects other users' authentication information (I), attack authentication server to make it refuse service (D), modify their privileges throughout the system (E)
3	T,I,D	IPC,SOAP	An intruder within the network detects the communication information between application server and web servers, and filters useful information (I), modify the datum of application server or web server (T), attacks the application server to make it refuse service (D)
4	T,I,D	ODBC,JDBC	An intruder within the network detects the communication information between application server and database servers, and filters useful information (I), modify the datum of database server (T), attacks the database server to make it refuse service (D)
5	T,I,D	ODBC,JDBC	
6	T,I,D	ODBC,JDBC	
7	T,I,D	SOAP	An intruder within the network detects the communication information between other heterogeneous system server and web servers, and filters useful information (I), modify the datum of other heterogeneous system server (T), attacks other heterogeneous system server to make it refuse service (D)

TABLE Ⅲ
QUANTITATIVE VALUES OF RISK DEGREE (Cn)

A corresponding risk degree	DREAD property value					Cn quantitative value
	D	R	E	A	D	
Cs	1.0	0.6	1.0	0.6	0.8	0.80
Ct	1.0	0.4	0.8	0.3	0.4	0.58
Cr	0.4	0.6	0.6	1.0	0.8	0.68
Ci	0.6	0.4	1.0	0.1	0.8	0.58
Cd	1.0	0.8	0.4	1.0	0.6	0.76
Ce	1.0	0.4	0.8	0.6	0.2	0.60

TABLE Ⅳ
QUANTITATIVE VALUES OF WEIGHTING FACTOR P AND ATTACK FACTOR(Rn)

Security ability property	Quantitative value of corresponding weighting P	Quantitative value of corresponding Rn
As	1/23=0.043	0.85
At	5/23=0.217	0.60
Ar	1/23=0.043	0.75
Ai	7/23=0.305	0.80
Ad	7/23=0.305	0.90
Ae	2/23=0.087	0.65

E. Collection and quantitative calculation of the experiment datum

According to the setting and calculation of the corresponding parameters in the process of security property quantization, we can separately get the quantitative value of attack factor, risk degree, rate of successful attack, security property, security trust function and weighting system of Web service. According to the calculation formula of dos in section 4, we can get the reference evaluation value of Web service degree in SOA application system. See table V as follows.

TABLE V
COLLECTION OF EXPERIMENT DATA

Security property	Attack factor R	Risk degree C	Rate of successful attack O	Security property A $A=C_n*O_n*R_n$	Security trust function $f(A_k)=1-A_k$	Weighting factorP	property's contribution degree $f(A_k)*P_k$
As	0.85	0.8	0.333	0.23	0.77	0.043	0.03
At	0.60	0.58	0.375	0.13	0.87	0.217	0.19
Ar	0.75	0.68	0.222	0.11	0.89	0.043	0.04
Ai	0.80	0.58	0.250	0.12	0.88	0.305	0.27
Ad	0.90	0.76	0.250	0.17	0.83	0.305	0.25
Ae	0.65	0.6	0.044	0.02	0.98	0.087	0.09
Dos							0.87

F. Analysis on the experiment result

To reasonably evaluate the security degree of Web service and calculate its value is the precondition and basis of judging whether the Web service secure or reliable. According to the definition of WS-SEM model in chapter 3 and the original experiment datum, we can get the related evaluation value of the Web service security degree. The security index can be acquired by the formula 4.4:

$$dos = \sum_{k \in A} F_k \times P_k = 0.87$$

According to the quantitative calculation of security ability property from multi-angles as in table 5.4, the security analysis of this enterprise's SOA application system is as follows:

Generally speaking, within the enacted six risk classes of this model, the risk of anti-spoofing ability As of the enterprise's SOA application system is the largest, and its value is As=0.23, so we must optimize the security measures aiming at this kind of threat risk, and the risk of other parts (anti-tampering, anti-repudiation, anti-disclosure of message, anti-denial of Service and anti-elevation of privilege) is relatively small.

VI. CONCLUSIONS

Aiming at the fact that at present, for the Web service security studies, most of them are limited to the implementation mechanism of Web service security but little on the application study from the aspects of threat classification and dos evaluation, this paper has carried out applied research based on the evaluation method of STRIDE model in Web Service Security, and carried out the threat classification and dos evaluation of Web service provided by WS-SEM model for the target system, and then provided a quantized reference index of dos evaluation for Web service security to validate whether the Web service is secure and reliable and also to avoid the tragedy consequence resulted from Web service component integrated in the software system where there is security hidden trouble, thus provides a valuable reference to check out security vulnerabilities of Web service and optimize the system's security design.

VII. ACKNOWLEDGMENTS

This paper is supported by the Basic Scientific Research and Operational costs of Central Universities. The authors are grateful for the anonymous reviewers who made constructive comments.

REFERENCES

[1] Tsai W T,Paul R,Y Wang,et al1. Extending WSDL to Facilitate Web Services Testing// Proceedings of 7th IEEE International Symposium on High Assurance Systems Engineering.Tokyo,Japan,2002:171-172
[2] Tsai W T, Paul R, Cao Z. Verification of Web services using an enhanced UDDI server 2003,131-138
[3] Heckel R.Mariani L. Automatic conformance testing of web services 2005:2-10
[4] Run S. A model for Web services discovery with QoS. ACMSIGecom Exchanges,2003.4(1): 1-10
[5] Carroll J J,Bizer C,Hayes P,et al1.Named graphs,provenance and trust//Proceedings of the 14th International Conference on World Wide Web.Chiba,Japan,2005:613-622
[6] ZHANG Liang, ZHU Leiming, WANG Kang. A Website Security Analyzing Technology Based on Web Vulnerability Threat Model. Microcomputer Applications. 2008.24(5):56-58
[7] WU Lei, LI Xinke, WANG Hong. Research on the Reliability Testing of Web Services Based on Fault Injection Technology [J]. Mini-Micro Systems, 2007, 28(1): 127-131
[8] LIU Zhenpeng, CHANG Xiaomeng. A Safe ID Authentication Policy in Web Service. Computer Research and Developmeng.2006.43:551-555
[9] SHI Yinsheng, DENG Shiwei, GU Tianyang. Research on the Web Services Security Testing Technology. Computer Engineering and Science. 2007. 29[10]
[10] Michale Howard,David Leblanc.Writing Secure Code[M].Microsoft Press.2002

[11] Anonymous et al. Maximum Security [M]. Translated by ZHU Luhua et al. Beijing: China Machine Press, 2003
[12] Heather Kreger. Web Services Conceptual Architecture (WSCA1.0)[EB/OL].April 2002.http://www-128.ibm.com/developerworks/cn/webservices/ws-wsca/part3/index.html.
[13] 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
[14] Rui WANG, Ning HUANG, Requirement Model-Based Mutation Testing For Web Service, 4th International Conference on Next Generation Web Services Practices,2008:71-76
[15] DAI Changying, ZHANG Guangzhi. Trust Evaluation Model in Web Services. Computer Engineering.2009.5:139-141
[16] LI Haihua, DU Xiaoyong, TIAN Xuan. A Capability Enhanced Trust Evaluation Model For Web Service. Chinese Journal of Computers. 2008.31(8):1471-1477

JIANG Li, born in 1980, Graduate of Hunan University. Her main research interests include Service Science and Web Service technology.

CHEN Hao, born in 1975, Associate Professor of Hunan University. His main research interests include mobile search, Web mining and service science.

DENG Fei, born in 1978, Graduate of Hunan University. Her main research interests include Service Science and Web Service technology.

ZHONG Qiusheng, born in 1986, Graduate of Hunan University. His main research interests include mobile search and Web service technology.