Original Research Paper

VOLUME-6 | ISSUE-3 | MARCH - 2017 • ISSN No 2277 - 8179 | IF : 4.176 | IC Value : 78.46

TRIDE Model to Evaluate the Security Mechanisms for Mitigating WebService Attacks

Engineering

KEYWORDS: IIS Web Server, .Net Framework, Secure Web Service, SQL Server, TRIDE Model

Shahanaz Begum I — Computer Science and Engineering, BIT Campus, Anna University, Tiruchirappalli-24, India

Geetharamani G — Mathematics, BIT Campus, Anna University, Tiruchirappalli-24, India.

ABSTRACT

Web service construction resembles a distributed computing model having the important characteristics such as loose coupling, language neutrality, platform-independence, interoperability etc, which are forming the base for Service Oriented Architecture(SOA) popularly known as an Enterprise Architecture. The exposure of Web service over the Internet is liable to get attacked as it has some vulnerabilities for exploitation by the attackers to perform some attacks. It is important to pay attention towards the provision of the security mechanisms to prevent the web services from the threats leading to User identity Spoofing, Tampering of data , Refusal of tracing back to the caller, Sensitive Information leakage, Service denial and Unrestricted access to privileges type of attacks. Security challenges are faced at the consumer, Service provider and Service registration levels, hence it is mandatory to enforce trust at the different levels of service access. In this research work TRIDE Model is proposed to evaluate the different security mechanisms that are applied to defend against Web service attacks. The performance of current research work is analyzed with the STRIDE Model available with the present literature work. The experimental results are obtained by testing these security mechanisms in the dynamic environment. This Proposed work is implemented using .NET Framework, Visual Studio 2013 Community Edition, SQL Server 2012 and IIS Web Server.

I. INTRODUCTION

Web service depicts the distributed Computing model built on the foundation of Open Web Platform involving many web technologies encompassing many characteristics such as loose coupling, Interoperability, Platform, Language and Operating System Independence and so on. Researchers are facing the challenges in proposing techniques for efficient evaluation of security features of a Web service which lays the foundation for constructing Service Oriented Architecture(SOA) for successful implementation and automation of business logic.

Software Testers concern in satisfying functional requirements of a web service and rarely about solving the security issues in web service. In this research paper, a security evaluation method such as Tride model was developed and as benchmark Stride model was referred for evaluating the degree of web service security. .NET framework, Visual studio 2013 are utilized for creating webservices and web clients. Web server is utilized to host the web services and web applications used in a particular business scenario are discussed in this research work. SQL Server 2012 is utilized to create databases and its related tables are holding the data associated with the web services and web applications.

The research paper organization is given as follows, Chapter II introduces the work related to the domain of the research work discussed in this paper, Chapter III explains the TRIDE model and how it helps in evaluating the security features of a web service. Chapter IV is on Performance analysis and Chapter V gives the concluding statements.

II. LITERATURE SURVEY

Most of the Web service standardization organizations and research consortiums are working in the perspective of achieving the security requirements of a web service.

Hada and Maruyama explained how the multiple service instances of a web service are composed and their usefulness in business workflows. They discussed on the design of two protocols namely session oriented multiparty authentication protocol for establishing trust among service partners of a session and multiparty authentication protocol where each service instance taking part in a session for message transfer were assigned a unique identifier to solve some security issues that may arise due the dynamic behaviour of multi parties.

Papazoglou and Geogakopoulos discussed on location based web services and challenges faced in developing web services in computing environments involving mobile and wireless applications.

G.Itkis considered the scenarios involving local signing use cases, server signing use cases and validation of signatures which were implemented in mobile and distributed computing of e-commerce environments .

Martin Potocnik and Matjaz proposed a model for automatic understanding of complex event types and validated the model effectiveness by implementing it on national telecommunication provider

Cong Liu et al tried an approach to solve the problem of negligence in providing defense mechanisms against privacy-preservation security issues in the traditional business process mining approaches

Mangler et al. described RESTful services and mentioned the need for a good interface description language since WSDL(2.0) is not efficient in its usage and WADL lacking the widespread use and was found with missing features. The authors introduced RIDDL an adaptable and extensible service description language for efficient description and composition of web services.

Zhang et al, found the need for automatic composition of web services making use of domain ontology and semantic technology leveraging automatic discovery, dispatch and compositions of web services. The web services were made available on demand by this extended feature of domain characteristics, synthetic semantic support and automatic composition of web services.

William Stallings has described in his book the symmetric and asymmetric encryption techniques, authentication techniques and ways of providing network and system security.

Jiang Li et al, research work focused on web service security evaluation techniques to locate and provide countermeasures for the attacks identified in STRIDE Model dealing with web service attacks. They performed their study on a SOA Application and applied the testing techniques on a model developed by them and they obtained favourable results in removing the vulnerabilities underlying the listed attacks specified in their work.

Jie xu et al. described the complications involved in establishing authentication path between two distributed services. They introduced the cross-realm authentication protocol and evaluated

using Globus and Crown.

III PROPOSED WORK

In this proposed research work web service security mechanisms were implemented in a dynamic environment. This work was targeted in providing countermeasure against tampering, denial of service attack, elevation of privileges, repudiation and message disclosure attacks against the working of message transfer between web services in an e-business environment by proposing TRIDE Model.

This work was implemented utilizing .NET Framework, Visual Studio 2013 Community Edition, and SQL Server 2012 and IIS Web Server.

Experimental Setup

This work involved the creation of four applications namely Customer Application, Producer Web Service, Session Authority Application and Payment Gateway Application. Producer Web service in turn invoked Registration, Login, Order placement and Product Purchasing Web services. The business scenario chosen for the evaluation of the security mechanisms applied is given in Figure: 1.

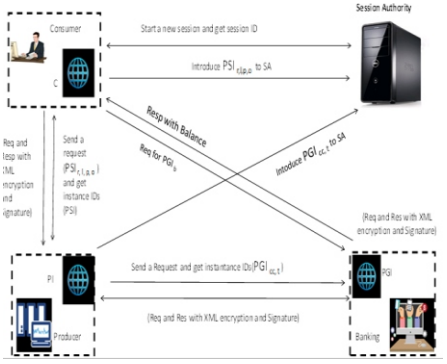

Figure 1: A business scenario depicting the business flow with the application of security mechanisms

Session Authority application was created with SessionAuthority database with Session-Partners table. Payment Gateway application was created with PaymentGateway database with customer and transaction tables. PaymentGateway webservice in turn invoked customer accounts and transaction web services with their data held in associated tables.

To protect against Web services from DoS Attacks the SOAP Messages are validated. Web services are invoked for performing enterprise communication. The attackers misuse this happening in making the web service unavailable to authorized users by performing DoS Attack. In this proposed experiment when the items are viewed by the users the requests could be given in multitudes which makes the web service resources unavailable. The availability of the web service is ensured by checking whether the occurrence of requests exceeded a threshold, before the soap request is forwarded to the corresponding server. This information appears in the element minoccurs in the wsdl file. WS-Security addresses only message integrity and confidentiality and user authentication and authorization.

Elevation of privilege is prevented by having access control over users accessing specific web services invoked by Payment gateway web service namely transaction details viewing. The customer will be allowed to view his account details only and not others details. Role based access control is granted based on the discrimination between customers and system administrators(who could view daily transaction details and insert products into the products table)

Information flow between different services with cryptographic techniques such as XML Encryption is attempted to prevent information leakage and tampering. Repudiation is prevented with the help of the XML Digital signature applied at the sender end making use of private key for signing the XML Messages and verification of XML Messages at the receiver end by making use of the public key.

The security is enforced between the different service instances to avoid misuse of any service instance in a specific session by the hacker. And every transaction flow is allowed to pass through the Session authority to maintain the state of the session and unique id of each service instance of a particular business session.

All the transactions in web services are in XML format so whatever the cryptographic technique that is applied will be enforced over XML messages. SOAP request SOAP response and WSDL Information are all complying with XML format

The steps followed for carrying out the different operations in a business flow is given below:

1. C (Customer) obtains Sid(Session ID) from SA (Session Authority)using GUID method

2. C requests P(Producer) and receives PSIr(Producer Service Instance for registration service), Service Instance ID as response from the initial request

3. C Introduces PSIr into SA (ie In Session-Partners table, PSI id for registration service,r is stored)

4. C Sends request to Producer by invoking PSIl(ie Producer Service Instance for login service with parameters username and pwd, they are encrypted and sent. PSIl web service validates login credentials, If Euname and Epwd is valid , PSIl service responds true, ie Eresponse)

Else Returns false **Information disclosure** is prevented by using XML Encryption

5.C Introduces PSIl id for login service into SA as SP(Session partner)

6. C requests PSIp(Producer Service instance for product list viewing web service) with Epcategory parameter restricted with count 1 and PSIp responds with PL(Products list with the selected category)

PSIp – Web service Method in Producer Application to provide list of products or their details to Customer based on Category selection,

If Epcategory >1,(product category) response is ignored else send product list as response to C) **Denial of service** is prevented

7.C introduces PSIp (Producer service instance id for Product view service)to SA as SP

8. C requests PSIo(Producer service instance with products order service) with Epid as parameter and get response from PSIo(the product cost)

PSIo – Web service stores customer order details in order table of Producer database

If Cid(Customer id), Pid (Product id) and Sessionid are valid Insert order into Order Table and respond true Else refuse order

9. C introduces PSIo(Producer Service instance id for product order service) into SA as SP

10.PSIo service calls PGIc(PaymentGateway service instance calls customer accounts service with credit card information) for credit card validation on banking website(Ecc)(after buy option is selected) {PGIc -Payment Gateway webservice method validates customer credit card details)

If Ecc is valid payment is allowed

VOLUME-6 | ISSUE-3 | MARCH - 2017 • ISSN No 2277 - 8179 | IF : 4.176 | IC Value : 78.46

Else return invalid cc(credit card no)

11.PSIo introduces PGIc (PaymentGateway service instance id, invoking customer account service) to SA as SP

12.SA with Sid for a particular C contains PSIr,l,p,o and PGIc , PGIt as service instance partners

13.PGIc calls PGIt to perform transactions for valid CC(credit card no) of Customer C

(PGIt – Webservice method in PaymentGateway performs bank transaction for Product purchased)

(If (Account balance) > Pt(Product transaction Amt) Perform transaction

Else Insufficient balance

XML Encryption and XML Digital Signature are applied here

Tampering of data, **Information Disclosure** and **Repudiation** are prevented

14. C request PGIb(Paymentgateway service invoking balance checking service) with Eaccno and get response on Ebalance (Encrypted balance)

PGIb – Web service method in PaymentGateway application is invoked to show Customer balance.
If Anumber == Cid show Cbalance
If Anumber == Aid(Admin) access is denied
Here Role based service access is used to prevent customers trying to access Transactions table with Admin privileges
Elevation of Privileges is Prevented.

IV PERFORMANCE EVALUTAION

The following figures depict the performance of the proposed work in terms of the time taken against the number of service instances in applying the security mechanisms over the working of the web services while the flow of messages were occurring between the service partners in a particular session with the application of security mechanisms and without the application of security mechanisms.

TRIDE Model was proved to have better performance while providing the countermeasures against the Attacks tested in STRIDE Model except the Spoofing attack which is infeasible in this proposed approach. These defense mechanisms were tested in the dynamic environment. The proportion of the time consumed for applying different security mechanisms to achieve security features in a Web Service such as XML Encryption and XML Digital Signature, Role based access, Filtering of data based on the expected value of minoccurs element in WSDL File to prevent DoS Attacks are accomplished and is depicted in Figure 2.

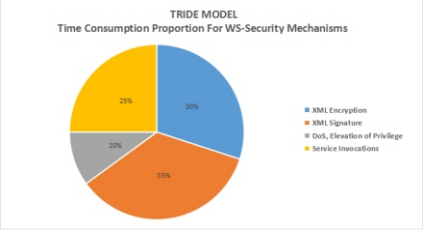

Figure 2. Time consumption proportion for WS-Security Mechanisms

The comparison of control protocols/ Security mechanisms utilized in the STRIDE Model and TRIDE Model in the Web Services which are applied in the business scenario is shown in Table 1.

CONCLUSIONS

This research paper deals with the provision of security mechanisms against the attacks performed to compromise a web service. The security measures are provided to achieve integrity, non-repudiation, confidentiality, and prevention of availing elevated privileges. The TRIDE model proposed in this research work is evaluated by comparing with the STRIDE model proposed in earlier research work. This research work has the future scope of attempting this approach in the Cloud environment for providing secure service computing environment to combat the spoofed attack also along with other attacks.

Table 1: Comparison of security mechanisms utilized in STRIDE and TRIDE Model.

Threats	STRIDE Model (Control Protocols Utilized)	TRIDE Model (Security Mechanism applied)
Spoofing	HTTP,SSL	Not Feasible
Tampering	IPC, SOAP	XML Encryption, XML DigSig
Repudiation	HTTP,SSL	XML Encryption, XML DigSig
Information Leakage	LDAP, Kerberos, IPC, SOAP	XML Encryption
Denial of Service	LDAP, Kerberos, IPC, SOAP	Element minoccurs in WSDL is controlled by web service coding
Elevation of Privilege	LDAP, Kerberos	Role based access control

REFERENCES

1. S. Hada and H. Maruyama, "Session Authentication Protocol for Web Services," Proc. Symp. Application and the Internet, pp. 158-165, 2002.
2. M.P. Papazoglou and D. Georgakopoulos, "Service-Oriented Computing," Comm. ACM, vol. 46, pp. 25-28, Oct. 2003.
3. G. Itkis, "Forward Security: Adaptive Cryptography – Time Evolution," Handbook of Information Security, John Wiley and Sons, 2006.
4. Martin Potocnik and Matjaz B. Juric, "Towards Complex Event Aware Services as Part of SOA", IEEE Transactions on Services Computing, Vol. 7, No.3, July-September 2014.
5. Cong Liu, Hua Duan, Qingtin ZENG, MengChu Zhou, Faming Lu and Jiujun Cheng "Towards comprehensive support for privacy preservation Cross-Organization Business Process Mining", IEEE Transactions on Services Computing, no.99, pages: 1-1l.
6. J. Mangler x, E. Schikuta y, C. Witzany, Quo Vadis Interface Definition Languages towards a interface definition language for Restful Services, 978-1-4244-5299-6/0c9/$26.00 (c)2009 IEEE.
7. Zhang Hai-tao and Gu Qing-rui, A Dynamic Web services Composition and Realization on the Base of Semantic", 978-1-4244-5824-0/$26.00 _c 2010 IEEE, pp: 624-627.
8. William Stallings, "Cryptography and Network security : Principles and Practice" , fifth edition, Prentice hall, 2011.
9. Jiang Li, Chen Hao, Deng Fei, Zhong Qiusheng, "A Security Evaluation Method Based on Threat Classification for Web Service", Journal Of Software, vol. 6, no.4, APRIL 2011, ACADEMY PUBLISHER, doi:10.4304/jsw.6.4.595-603
10. Jie Xu, Member, IEEE Computer Society, Dacheng Zhang, Lu Liu, Member, IEEE, and Xianxian Li "Dynamic Authentication for Cross-Realm SOA-Based Business Processes, IEEE Transactions on Services Computing, Vol. 5, No.1, January-March 2012.