ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

A NEW INTELLIGENT AGENTS BASED FRAMEWORK FOR SECURING WEB SERVICES

[1]N.BALASUBRAMANIAN, RESEARCH SCHOLAR
[2]S.NAJIYA MAHJABIN, II YEAR MCA
[3]K.JENIFAR INIYA, II YEAR MCA
MOHAMED SATHAK ENGINEERING COLLEGE, KILAKARAI - 623 806.
[4]ASKARUNISA, PROFESSOR& HEAD, DEPT. OF CSE,
VICKRAM COLLEGE OF ENGINEERING, MADURAI -630 561
TAMIL NADU, INDIA
[1]mugavaibala@gmail.com [2]najiyamahjabin@gmail.com [3]jenifariniya@gmail.com [4]askarunisa@staff.vickramce.org

ABSTRACT:

Service Oriented Architecture (SOA) is a paradigm that may be used to build infrastructures enable with needs and capabilities to communicate through services across distinct ownership and disparate technical domains. Besides SOAP and UDDI, which make the foundation of SOA; WSDL also plays an important role in this architecture. So far, in most of the security solutions that have been offered for SOA, providing security of SOAP messages has been the main objective. In the proposed model, users are restricted to assign the role and to access the service only when (s) he satisfies some predefined identity and spatio -temporal constrains, in addition to the enforcement of usual security and integrity constraints which are used for providing additional security. Finally, we use intelligent agents to provide security through rules and constraints and hence multiple agents are deployed.

Keywords: SOA, Web service, XML, SOAP, Access Control, WSDL.

I.INTRODUCTION:

Service-oriented architecture (SOA) is a development paradigm, defined as an interoperable architecture that enables interoperability over different enterprise and business solutions [13]. In order to protect service-oriented systems effectively from such XML-based attacks, it is vital to investigate the characteristics and behaviors of such attacks thoroughly and rationalize their undesired effects. Access Control mechanism can be used to detect and defend against such XML based attacks. In this paper, we present an approach to protect web services from XML based attacks using Intelligent Agent Role Based access

II. RELATED WORKS

In recent years, web services security is an active research area. The current researches concentrated on some aspects: testing and verifying web service effectiveness, analyzing the test vulnerability of security, analyzing the test reliability of web service, authentication and authorization of web service access, and testing framework .A pattern based language was proposed by Fernandez et al. for an XML firewall[8]. Access to distributed resources is controlled by security assertion coordination pattern with role-based access control. Filtering pattern was used to filter the XML messages and related documents according to the policies.

Bebawy et al. implemented a firewall which deletes the SOAP messages temporarily from the transport layer and scan it for the correctness. If the message is clear, it will induced back into the OSI stack otherwise delete it permanently [11]. This model is well suited only for SOAP (Simple Object Access Protocol) based DoS attacks and Buffer Overflow attacks. Also access control mechanism was not addressed.

Cremonini *et al.* integrated existing web services security specifications with an XML firewall [10]. They analyzed the vulnerability of the WS-Reliable Messaging and designed a semantic aware firewall for web services.

N. Li and Z. Mao proposed an approach UARBAC [7] for RBAC to design and analyze administrative models. UARBAC came along with an extension UARBAC, in which the parameterized objects are employed over constraint based administrative domain. Though this model is scalable and flexible, it did not address the concurrency control.

Claudio A. Ardagna *et al.* proposed a simple architecture with a novel policy language to provide privacy for individuals to keep the control over their own data while exploiting services over web [6]. They used XACML's technical features to describe the policies.

Min Xu, Duminda Wijesekera proposed a framework to enforce ARBAC policies along with XACML for web services [5]. XACML-ARBAC profile uses a session aware administrative model for RBAC to address the concurrency issues. Conflicts between session management and administrative operations can be resolved using this model. Performance overhead and impoverished interface between PEPs and APEPs in distributed environment for session management are some of the issues in this work.

J. Crampton and G. Loizou have extended the RBAC administration in SARBAC [7]. Role hierarchy is used to define administrative scope and administrative domain. It works well when the role hierarchy is defined like a tree with a superpower root role. They have not addressed the concurrency control in this work.

Role Based Access Control has been the subject of interest for many years and a considerable research has been carried out. It is widely accepted as an alternative to traditional discretional and mandatory access controls. The emergence of distributed environment in Web Services poses new demands on access control mechanisms, because the decisions to grant access may depend on contextual information such as the location of the user and the time at which access requests are made general contextual constraints .However none of these models are exactly suitable for web services because of the dynamic and distributed nature of data used in web services. Therefore it is necessary to enhance the existing RBAC models with spatio - temporal constraints and features.

WEB SERVICE SECURITY:

OASIS (Organization for the Advancement of Structured Information Standards) and W3C (World Wide Web Consortium) have over the last years standardized several specifications related to security in Web services and XML.These standards including, XML Encryption and XML Signature. Since WSDL is an XML file, in the proposed security framework XML encryption besides other standards like XKMS (XML key management specification) are used.

XML ENCRYPTION:

Encryption refers to the translation of data into an encoded format for the purpose of achieving data security. XML (extensible markup language) encryption can be used to encrypt arbitrary data. XML Encryption is similar to XML Signature in many ways. For instance, like XML Signature, XML Encryption does not apply only to XML resources as it may be used to encrypt arbitrary binary resources as well.

XML DIGITAL SIGNATURE:

Digital signature uses a pair key, the same as asymmetric encryption but there is a twist; In digital signature, sender uses his/her own private key to sign the selected part of message so any one who can access public key will be able to check the signed part which has been sent from the sender and become sure about the integrity of signed data, which is a reliable method for receiver to ensure that the signed part has not been tampered within the way.

PKI AND THE XML KEY MANAGEMENT:

PKI -The comprehensive system required to provide public-key encryption and digital signature services is known as a public-key infrastructure (PKI).The purpose of a public-key infrastructure is to manage keys and certificates. One of the most important problems about PKI is the high complexity of this infrastructure.

XKMS

XKMS (XML key management specification) is a Web service that provides an interface between an XML application and a Public Key Infrastructure (PKI). XKMS greatly simplifies the deployment of enterprise strength Public Key Infrastructure by transferring complex processing tasks from the client application to a Trust Service. The primary objective of XKMS is to allow a user of a public key when used to verify a digital signature or encrypt data to locate the required key and to associate naming or attribute information with the holder of the corresponding private key.

There are many disadvantages in the earlier works, so we move to Trust web service against WSDL attacks.

III. TRUST WEB SERVICE AGAINST WSDL ATTACKS:

A new practical security framework is to be proposed in this paper as shown in Figure 1, in order to provide security of WSDL files and protect Web services against WSDL attacks.

Step 1: A Web service, called Trust Web service, generates a pair of keys, using one of the key generating algorithms.

Step 2: Trust Web service sends his request to XKMS in an XML format, in order to store his public key in PKI.

Step 3: XKMS will provide public key registration for requester by using his registration key service and passing the request to PKI.

Step 4: PKI will deliver the response of public key storage to XKMS; it acts as an intermediate between Trust Web service and PKI.

Step 5: XKMS will deliver the response of PKI to Trust Web service. Now public key is available for everyone and the related private key is only available for his owner (Trust Web service).

Step 6: As it is can be understood, the Provider Web service, who is a requester to secure his WSDL, Will obtain service provider's public key, using XKMS and PKI.(The PKI will check the requester authentication before providing accessibility of Trust Web service's public key).

Step 7: It is possible not to encrypt the whole XML file. Consequently service provider is able to encrypt any critical elements in WSDL. WSDL file consists of two main parts: Abstract section and Concrete section. Mostly the main important elements of WSDL are in abstract part. But there is still a problem. The normal WSDL is not encrypted, so to inform the service consumer that this WSDL file is an encrypted one, Trust Web service will insert a new tag in WSDL, called <wsdlx:WSDL_secured> and put its value as True. Therefore, it can be encrypted the WSDL file. publish service provider specifications in UDD I(Universal Discovery, Description And Integration) registry. Now the malicious users cannot perform their WSDL (Web Service Description Language) attacks, because these attacks were performed by using critical elements in abstract part of WSDL, which are not accessible any more for all users, but only for the authenticated ones.

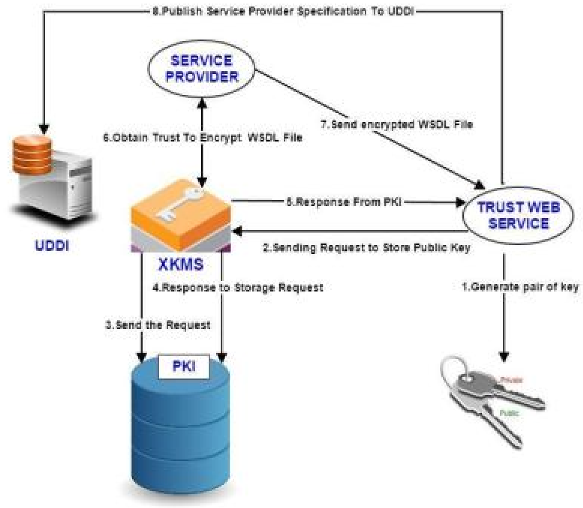
8.Publish Service Provider Specification To UDDI
SERVICE PROVIDER
7.Send encrypted WSDL File
6.Obtain Trust To Encrypt WSDL File
5.Response From PKI
TRUST WEB SERVICE
UDDI
2.Sending Request to Store Public Key
XKMS
4.Response to Storage Request
1.Generate pair of key
3.Send the Request
PKI
Private
Public

Figure 1: Structure of security framework

IV. INTELLIGENT SPATIO ROLE BASED ACCESS CONTROL (ISRBAC):

In this paper, we propose a new Intelligent Spatio Role Based Access Control model (ISRBAC) that uses agents for rule management and for enforcing spatio-temporal constraints more suitable for web services that use heterogeneous environments and multi databases. In order to provide effective secure web services, first we propose this ISRBAC model by adding integrity constraints and spatio-temporal constraints. Second, this system provides separate agents such as a spatial information agent, a temporal information agent and a rule management agent to check appropriate constraints. Finally, this work proposes new agents that are capable of providing rule matching and rule firing so that the accuracy level is increased to an optimal level of security. The steps of the ISRBAC algorithm are as follows.

Step 1: Parse the SOAP message to get information for the further steps using SOAP proxy

Step 3: User proxy Info is processed as follows SOAP agent extracts encrypted user information from <UserInfo> decrypt it with the private key of SOAP Proxy and examines its validity similarly the SOAP agent extracts the role from <RoleInfo>, examines its validity.

Step 4: Executing ISRBAC: If the user is valid and the called service is in scope of the role permission, the SOAP Proxy will retransmit this SOAP message to corresponding Web Service, and the respond of the Web Service will be retransmitted to the client, otherwise returns an error message.

V. CONCLUSION

In this paper, a new security framework was proposed to enhance security level of any Web service dependent environments, like SOA. This model can provide a Web service policy for public. So in a network which WSDL information should only be accessible for authenticated requesters, security of this file is an essential matter Web services security standard. And it also provides an Intelligent Spatio Role Based Access Control model that introduces additional security using agents for managing spatio and temporal constraints. From the above experiments, it has been observed that the accuracy of this model is more than the previous works. Therefore, this system enhances the description ability for Web service, and shows intelligent behavior.

In future, by using WSDL and Intelligent Spatio model we can achieve more effective secure web services.

VI. REFERENCES:

[1] E. Bertino, A. Squicciarini, I. Paloscia, and L. Martino, "Ws-AC: A Fine Grained Access Control System for Web Services," World Wide Web: Internet and Web Information Systems, vol. 9, no. 2, pp. 143-171, 2006.

[2] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, "A Fine-Grained Access Control System for XML Documents," ACM Trans. Information and System Security, vol. 5, no. 2, pp. 169-202, May 2002.

[3] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, "Controlling Access to XML Documents," IEEE Internet Computing,

[4] Claudio A. Ardagna, Sabrina De Capitani di Vimercati,Stefano Paraboschi, Eros Pedrini, Pierangela Samarati, and Mario Verdicchio "Expressive and Deployable Access Control in Open Web Service Applications", IEEE Transactions on Services Computing, Vol. 4, No. 2, pp. 96-109, April-June 2011.

[5] Min Xu, Duminda Wijesekera, "Runtime Administration ofan RBAC Profile for XACML", IEEE Transactions on Services Computing, vol. 4, no. 4, pp. 286-299, Oct-Dec 2011.

[6] N. Li and Z. Mao, "Administration in Role Based Access Control", Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '07), pp. 127-138, Mar. 2007.

[7] J. Crampton and G. Loizou, "Administrative Scope: A Foundation for Role-Based Administrative Models," ACM Trans. Information and Systems Security, vol. 6, no. 2, pp. 201-231, 2003.

[8] E. Bertino, L. Martino, F. Paci, and A. Squicciarini,Security for Web Services and Service-Oriented Architectures, Springer, 2009.

[9] Haiping Xu, Abhinay Reddyreddy, and Daniel F. Fitch, "Defending Against XML-Based Attacks Using State-Based XML Firewall", Academy Publisher, Journal of Computers, Vol. 6, NO. 11, pp. 2395-2407, Nov 2011.

[10] M. Cremonini, S. Vimercati, E. Damiani, and P. Samarati,"An XML-based approach to combine firewalls and web services security specifications", in *Proc. 2003 ACM Workshop XML Security*, Fairfax, Virginia, pp. 69-78, Oct.2003.

[11] R. Bebawy, H. Sabry, S. El-Kassas, Y. Hanna, and Y.Youssef, "Nedgty: web services firewall," in Proc. IEEE Int. Conf. Web Services (ICWS'05), pp. 597-601, 2005.

[12] JIANG Li, CHEN Hao, DENG Fei, ZHONG Qiusheng, "A Security Evaluation Method Based on Threat Classification for Web Service", Academy Publisher, Journal of Softwares, VOL. 6, NO. 4, pp. 595-603, APRIL 2011.

[13] T. Erl, "*Service-Oriented Architecture (SOA): Concepts, Technology, and Design"*, Prentice Hall PTR, Service-Oriented Computing Series, Aug. 2005.

[14] P. Hallam-Baker and S. H. Mysore, "XML

[15] Ernesto Damiani, Sabrina de Capitani di Vimercati , Stefano Paraboschi,Pierangela Samarati, "Design and implementation of an access control documents ", Computer Networks, VoU3,No.I-6,pages 59-75, June 2000.

[16] VERISIGN, "XML key management, The TrustServices" 2000.

[17] Min Xu, Duminda Wijesekera ,"Runtime Administration ofan RBAC Profile for XACML", IEEE Transactions on Services Computing, vol. 4, no. 4, pp. 286-299, Oct-Dec 2011.