ISSN 2047-3338

Security Issues in Web Services

Hirrah Siddique and Syed Shah Muhammad

Department of Computer Science and Engineering, University of Engineering and Technology, Lahore-Pakistan

***Abstract*– Computing based on Web services is currently very much popular and demanded in the software industry providing a variety of services that are required by various organizations and users. Due to the vastness and flexibility of the architecture the web services have to face a great number of threats and attacks and overall security issues. A secured architecture is very critical for the web services due to the dynamic nature of the system. Most of the work had done by researchers on the security issues for web services. In this paper, we shall review the security issues stated in the past and solutions of those issues, and then we shall present our findings on the security challenges that are present to the web services. MPMSD (Multi-Part Multi-Signature Document) is an emerging field of study and played an important role in the security of web services. In the paper, we will also discuss the MPMSD (Multi-Part Multi-Signature Document) and also identify the future challenges for the web services security.**

***Index Terms*– Web Services, SOAP, WSDL, XML, UDDI, SOC, MPMSD and Digital Signature**

I. Introduction

WEB services are the emerging and very much productive field of study according to the advancement of the technology and the demand of the hour. WS are serving a large community related to the Information Technology industry. We are covering the literature related to the web services and other technologies related to web services and after that the security issues and their solutions.

A) Service Oriented Computing (SOC)

Service oriented computing [1] is a newer and latest technology which provides the trend of platform independence as well as language independence to the components. It is basically a way to create the distributed applications. SOC is the major technology that is a basis for the Web Services technology. It provides a distributed technology with service orientation. A web service is the current technology of the Service Oriented Computing (SOC). Security is a great challenge and issue for the services for the Service Oriented Applications.

B) Service oriented Architecture (SOA)

The Service Oriented Architecture (SOA) is the collection of the services that communicate with each other. SOA describe the interaction between the software agents as the exchange of the messages between the requester of the services and the provider of the services. There are three basic roles of the SOA. The first is the service provider that provides services. Second is the services requester or the client which request for any service. The third one is the services registry. The requester of the services, use the operation of find to the requested service's description from the discovery agency and binds that description with the provider of the services and then invoke the services.

The rest of the paper is organized as follows: Section II describes web services, Section III explains General security framework for the web services. Section IV discusses Challenges and security issues of the web services; Section V provides Future recommendations and finally Section IV draws some conclusions.

II. Web Services

Web service [2] is a modular application that can be describe, and located and published and invoked over a network. It is platform and language independent and could be run on any platform and written in any programming language. There are three roles of services oriented architecture (SOA) involved in the web service, that is the service provider, second is the service requester and the third one is the broker.

Service provider- Could be a company, an industry, or business that is capable of providing services.

Service requester- could be accompany, an industry or business that needs the services.

Broker: a broker is an entity, a place or a system that helps both service requester and the service provider to discover each other.

The technologies which form the foundation of the web services are WSDL, SOAP and UDDI.

SOAP: Simple object access protocol is used to communicate among the different web services. In this protocol the message flows from the sender to the receiver through SOAP [3] message path. The SOAP message consisting of Envelope, Body and Header. SOAP envelop is used to encapsulate the SOAP message. SOAP body contains the information about the receiver. The Header contains the information about the node, the process of the message.

WSDL: Web services description language (WSDL) used to describe the functionalities of the services. When a requester receives the document WSDL, it must be validated, and to do that the simplest method is to use the digital signature for the WSDL that the requester would use to validate.

UDDI: Universal Description Discovery and Integration used as a registry for the Web Services. It's all about to publish the information and discover the information. It is mostly used standard in the industry that is to integrate the business with other business. The basic purpose of the UDDI is to discover the services that are available and to interact with them dynamically by the users. The process consist of three phases, searching (discovery), Binding and Executing. The Web Service Model is shown in the Fig. 1.

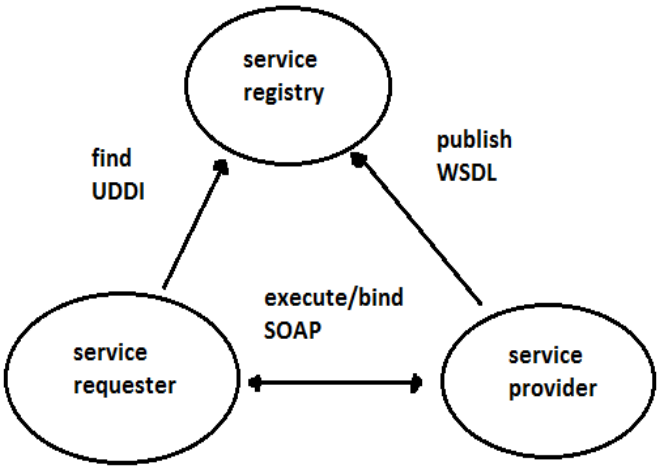

Fig. 1: Web services model

The Web Service is an attractive and the powerful and latest technology for the development of the distributed applications as well as for integration of the applications. For the wide acceptability by the developers and the clients in the business to business (B2B) and business to consumers (B2C) environment, so it must be secured. Therefore the study and the research of the security issues in the Web Services is a need of the hour.

III. General Security Framework For The Web Services

Security of the web services is a very important task and the most important and basic issues of security are stated following:

Authentication: The authentication is to identify the proof of the identity of the entity. An entity could be a user, service or a process. The solution for this issue is to authenticate the requester as well as the provider and the registry. All the components and entities should be authenticated. This could be done by the Trusted Third Party. Once the user is login to the registry, there should be single sign on for each service which the user can access. Once the user has been authenticated by using its login Id and password, there should be a route established among the different web services on the basis of their relationship of the trust that is called the federated trust.

Authorization: Authorization is the process of deciding that what processes an entity can do and on which resources, i.e., to grant and revoke the privileges to the authenticated entities. There are two technologies to ascertain the authorization and authentication for the web services which are Extensible Access Control Markup Language (XACML) [14] and Security Assertion Markup Language (SAML) [15] which reduce the overhead of the assertion of the Authentication and Authorization in the Web Service.

Confidentiality: Confidentiality refers to the process that only the sender and the intended receiver of the message could access the message and no unauthorized entity could access that message. For this purpose the message is encrypted and decrypted. Encryption is the process to convert the plaintext into ciphertext by using some key and the encryption algorithm. Decryption is the reverse of the encryption in which the ciphertext is converted to plaintext. XML Encryption is used for the encryption and the confidentiality in the web services and act as the basis of the confidentiality for the web services. It is done by using the XML Signature [16].

Non Repudiation: It refers that there should be no repudiation at the time of sending or receiving the message. XML Signature is used for non-Repudiation but it not enough for the today's challenging security threats. So there is need for a Trusted Third Party TTP.

Availability: It states that the resources and the services should be available to the authorized parties all the time. Denial of the services (DoS) is an attack which is used to disturb the availability of the services.

Integrity: When a message is sent to user and the message is not received by the receiver as it was sent, then this is the loss of the integrity of the message. Techniques that are used to maintain the integrity are MD5 and SHA.

Multi Part Multi Signature Document MPMSD: This scenario is used manually in the offices, where an employee generates a document and passes it to others, in turn the next reviewer, reviews the document and give his comments and signature and passes it to the next reviewer and so on. The resulting document is a multi-comment and multi reviewed composite document and the type of resulting composite document is called Multi Part Multi Signature Document. This process could be used for the authentication and authorization and the integrity of the document in the Web Service by using

Digital Signature [4] and XML document. The scenario for the MPMSD is explained in the Fig. 2.

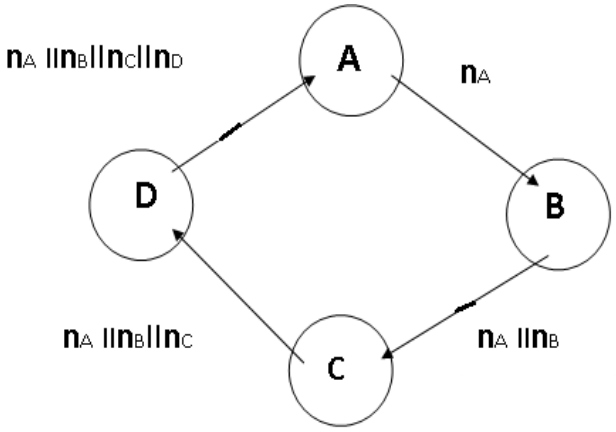

Fig. 2: MPMSD Scenario

IV. Challenges And Security Issues Of The Web Services

There are some significant challenges which we find during the review of the literature which are identified by us and we found some recommendations for those challenges.

Discovery: The requester and the provider of a service in the Web Services they have to identify and to compose the WSDL specific service that is based on the UDDI Registry. There are a large number of service candidates in the registry and due to this large number, the performance rank for the algorithms that are used to search, match and then compose the services can vary from case to case.

Quality of Service and Protection: Most of the Web services that are deployed do not provide the guarantees for the Quality of Service and the Quality of Performance. Quality of Service is important to define that what will be the level expected for the performance of a particular Web Service.

Denial of Service Attacks (DOS): Availability is one in the Web Services that enables the Web Service application in detecting the DOS (Denial of Service) attack, then continues the process and after the DOS attack to recover from the attack and to resume the services again in a graceful way.

V. Recommendations To Face The Challenges

Here we are going to explain some recommendations for the security of the Web Services.

1- The data and the application should be *replicated* in a robust way because the Web services are more susceptible to the DOS attacks.

2- The *logging standards* used in the entire SOA and the information about the accountability and the non-repudiation are not sufficient because the logging that is provided by different UDDI registries, the different identity providers and the web services varies greatly, hence there should be more additional software and the services to support the security in the SOA.

3- There should be use of *Modeling and Design for the secured software and attacks prevention.* The purpose of the modeling and designing is to ensure that there are no defects in developing and implementing the software for the web services. Modeling the threats and vulnerabilities and the analysis about the expected attacks could be effectively helpful in realizing the weaknesses and the strengths of the security systems for the web services.

4- There should be use of the *simulation techniques and the analysis for the performance* for the Quality of the performance and the services for End to End. These techniques played an important role in developing complex information system. Same techniques should be used in the web services security model. There should be QoS for each individual service offered; end to end Quality of service is critical in the composite services.

5- By using *XML Firewalls* the web services could be prevented from the web based risks. XML Firewalls could be very much handy if deployed well in the web services security and could be act as the end points in the WS Security. XML Firewalls could filter the contents that are malicious to attacks and the parameters carry the SQL queries and specially crafted for attacking the WS. It could also validate the Signature of the user and also validate the user identity as well.

6- There should be use of the *penetration testing* for the interfaces of the web services before they are open for the external access, because there could be some mistakes that could be malicious to attacks.

VI. Conclusions And Future Recommendations

Computing based on the web services is currently a technology that is the driver in the industry of software and so much productive with respect to the recent and the future needs and requirements in the software industry. By reviewing the literature we found that Data mining techniques could be used to detect the malicious attacks to the web services. The purpose of the Services oriented Computing is to create a collection of the software based services that could be automatically discoverable and accessible to the user by using standardized protocols. There are some points in the web services that need modification and more research work that are, description of the service, automatic discovery of the service and QoS, reliability and QoS for the individual service in the composite services environment are the issues that need to be solved.

References

[1]. Anoop Singhal; "Web Services Security: Challenges and Techniques"; Computer Security Division, NIST psinghal@nist.gov

[2]. Hua Yue; Xu Tao; (2012)" Web Services Security Problem in Service-oriented Architecture"; International Conference on Applied Physics and Industrial Engineering; Physics Procedia 24 (2012) 1635 – 1641

[3]. Gupta, K. N.; Agarwala, K. N. Agarwala, P. A. (2005). Digital Signature: Network Security Practices. PHI Pub. New Delhi

[4]. Gutierrez, C.; Medina, E. F.; Piattini, M. (2005). Web Services Enterprise Security Architecture: A Case Study. Fairfax. Virginia. USA

[5]. Jiehan Zhou, Eila Niemelä ;(2006)" Toward Semantic QoSaware Web Services: Issues, Related Studies and Experience"; VTT Technical Research Centre of Finland Kaitoväylä 1, 90571 Oulu, Finland Jiehan.Zhou@vtt.fi, Eila Niemela@vtt.fi; Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence (WI 2006 Main Conference Proceedings)(WI'06) 0-7695-2747-7/06 $20.00 © 2006

[6]. L. D. Martino, E. Bertino;(2006); "Security For Web Services - Standards And Research Issues", Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086; CERIAS Tech Report 2006-34

[7]. Ma An-feng, Zhao Feng-yu. Based on rampart module axis2 Web Service Security Research [J]. Computer Applications and Software, 2009, 26 (9): 31 33.

[8]. Meng Wei, Zhang Chen, Liu An-huai, Liu Hailing Web Services Security Model and Implementation of Computer Engineering and Applications. Computer Engineering and Applications [J], 2006, 42(26):134-136

[9]. Michael N. H.; Singh, M. P. (2005). Service-Oriented Computing: Key concepts and principles. *IEEE Internet computing*. 9(1):75-81

[10]. Mcintosh, M.; Austel, P. (2005). XML Signature Element Wrapping Attacks and Countermeasures. Fairfax. Virginia. USA

[11]. Neil. M.O. (2003). Web-Service Security. Tata Mcgraw Hill Pub. New York.

[12]. OASIS XACML pro_le for Web-services Working Draft 04, 29 Sep 2003.

[13]. OASIS UDDIVersion 3.0.2 UDDI Spec Technical Committee Draft, Dated 2004- 10-19.

[14]. OASIS Security Assertion Markup Language (SAML) 2.0 Technical Overview - Working Draft 03, 20 February 2005.

[15]. Subharta Sinha; Smriti Kumar Sinha (2010). "Security Issues in Web Services: A Review and Development Approach of Research Agenda". Assam University Journal of Science & Technology: Physical Sciences and Technology Vol. 5 Number II 134-140, 2010.

[16]. Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language. W3C Working Draft 26-March-2004.

[17]. XML-Signature Syntax and Processing W3C Recommendation 12 February 2002.