Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

UDDI and SAML based framework for Secure Semantic Web Services

Anil Sharma*
M.Tech (Information Security) Scholar,
Ambedkar Institute of Technology,
Govt. of NCT, Geeta Colony, Delhi, India
Sharma.anil19@yahoo.com

Suresh Kumar
Asst. Professor
Department of Computer Science & Engineering
Ambedkar Institute of Technology
Govt. of NCT, Geeta Colony, Delhi, India
sureshpoonia@yahoo.com

Manjeet Singh
Asst. Professor
Department of Computer Science & Engineering
YMCA University of Science & Technology,
Faridabad, Haryana, India
mstomar2000@yahoo.com

Abstract: A Semantic Web Service (SWS) is a software system designed to support interoperable application-to-application interactions over the Internet. SWSs are based on a set of XML standards, such as Web Service Description Language (WSDL), Simple Access Object Protocol (SOAP) and Universal Description, Discovery and Integration (UDDI). So far these services and the corresponding provider's URLs are advertised on specific UDDIs. As such, after finding the requested service any given client contacts the right provider to negotiate the service access procedure. These first contacts between clients and providers are usually not protected (Encrypted), the non-possession of public key infrastructure (PKI) especially by clients can be considered among the main cause behind this security problem. In this paper, we propose a securing approach based on PKI infrastructure and UDDI functioning, which must play in addition to its initial missions the role of a trust centre, leading to adequate security for semantic web services. The authentication and authorization information is exchanged using SAML (Security Assertion Markup Language), ratified by OASIS standards.

***Keywords*:** Semantic Web Service, PKI, UDDI, Security, SAML

I. INTRODUCTION

A Semantic Web Service (SWS) is a software system designed to support interoperable application-to-application interactions over the Internet. SWSs are based on a set of XML standards, such as Web Service Description Language (WSDL) [1], Simple Access Object Protocol (SOAP) [2] and Universal Description, Discovery and Integration (UDDI) [3]. So far these services and the corresponding provider's URLs are advertised on specific UDDIs. Semantic Web Service (SWS) is the emerging standard in web based application. The SWS define new trends to develop secure communication between machine to machine, which needs techniques to identify and verify a machine before sharing any information on network.

SWS are advertised over specific Directories named UDDI [4] where any client can first looking for the appropriate WS and then get the corresponding provider URL. After that, the client has to contact the adequate provider to get the access grant (which is a kind of certificate) to the requested WS. With this access grant, the client becomes able to access to this WS. Figure-1. Illustrates the advertising mechanism of WS. Unfortunately, WS security still constitutes the big challenge; in fact, despite the multitude of security proposals done mainly by specialized consortium, organizations and researchers such as W3C, OASIS [5], [6], [7], [8], [9], [10], this problem seems to be not yet well solved. The non possession of public key infrastructure (PKI) especially by clients (customers) can be considered amongst the main causes behind this security problem.

As illustrated in figure 1. If the client doesn't own a PKI, then any hacker can interfere in the exchanged messages between this client and the contacted provider and do what he wants. In this paper, we propose a detailed idea based on both the PKI and the improvement of the UDDI functioning which attempt to provide security for web services.

II. BACKGROUND STUDY

Security of web services (SWS) can be viewed from different sides because of the multitude of corresponding utilization. If we consider the case of utilization of WS for sharing information and services across organizations, then we can say that the corresponding security proposals and solutions are not bad but still require more improvements. [20] Proposed PKI based security system to authenticate semantic web service providers as well as web service consumers. But if we consider the case of public WS which can be provided to any given client by specialized providers then, we can say that the existing proposals and solutions lack a lot of security. This is mainly due to the non possession of the adequate security tools by most of the clients as we will explain next. Thus, our main concern in this paper focuses on this last case. Specialized consortium and organization such as W3C, OASIS ... have proposed several standards and solutions which attempt to provide security for SWS.

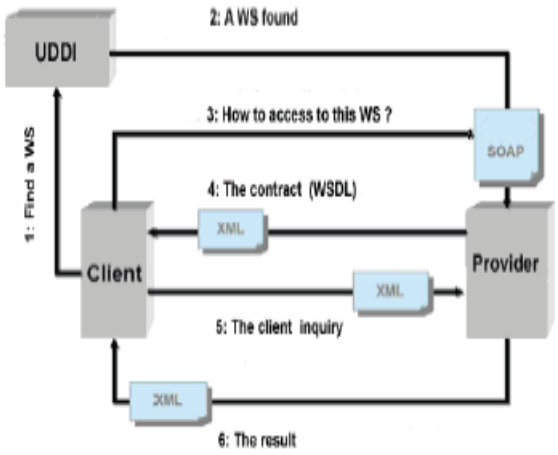

Figure 1. Semantic Web Service Advertising Mechanism

The framework illustrated by figure 2 is the most commonly used one to provide security for SWS. This framework shows that the security problem is divided into two levels; the transport level and the application level.

A. Transport Layer Security (SSL/TLS):

SSL/TLS are frameworks that include cryptographic protocols which are intended to provide secure communications on the Internet [11]. The server authentication is based on specific certificates and the client is authenticated via password or certificates.

B. Web Services Security (WS Security):

WS- Security [12] offers application level security as an extension to SOAP. It defines how to integrate various XML Security concepts as XML Signature [14], XML Encryption [15] or the Security Assertion Markup Language (SAML) [16] into SOAP. This specification is flexible and is designed to be used as the basis for securing web services within a wide variety of security model including PKI, Kerberos and SSL. Specifically, this specification provides support for multiple security token formats, multiple trust domains, multiple signature formats and multiple encryption techniques.

C. Security Assertion Meta Language (SAML):

Security Assertion Markup Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data [16]. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content. The standard purpose of using SAML is to realize Web Single-Sign-On. The user authenticates at the first site, retrieves an authentication and authorization token and subsequently uses this token to access further services without the need of re-authentication.

D. XML Access Control Specifications XACML:

XACML [17] is an extension to SAML that focuses on access control rights. XACML defines how to express access policies. Furthermore it specifies a request/response protocol between a policy decision and a policy enforcement point. XACML is considered the better way to implement role based access control (RBAC) [18] which restricts the WS accessibility according to predefined security policies and rules. Unfortunately, despite the consistency and the robustness of these security tools, WS still require more protection especially if they are intended for the public as we will explain in the next subsection.

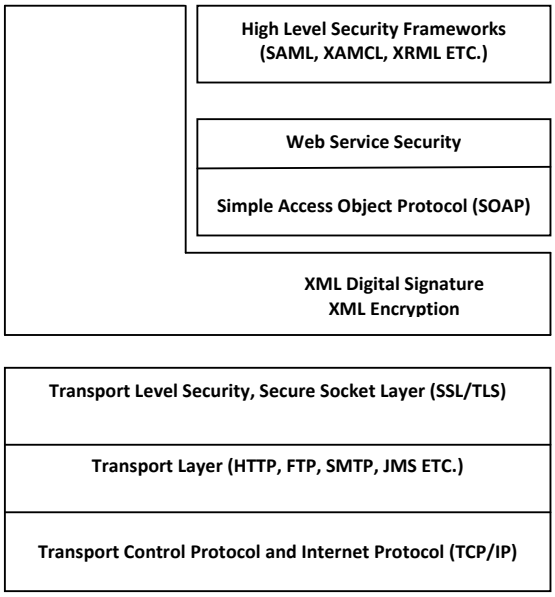

Figure 2. SWS Security Framework

E. Problem With the Existing Architecture

Public SWS and the corresponding providers URLs are advertised over specific UDDI where the only role to be achieved is limited to the advertisement. Consequently, users (clients) can just look for then find the required services for their different needs as illustrated in Figure 1. The first contact between any given client and the selected provider can't be protected (encrypted) especially if this client don't know the PKI (public key) of the provider and in addition he don't own a personal PKI. Consequently, any hacker can easily interfere in exchanged messages between any given client and provider to do what he wants. To deal with this problem, we proposed a new architectural model which can provide safe communications between involved parts and consequently secure SWS as such we explain next.

III. UDDI BASED TRUST CENTRE FOR SECURE SWS

Our proposal requires first the possession of a personal PKI by every involved actor (a client or a provider) to encrypt all exchanged messages between them. Second, we suggest that the UDDI should achieve in addition to its actual missions the following roles:

a. A prior registration of any provider or client of the advertised WS;
b. The publication in an encrypted manner of the PKI of every party or actor (a client or a provider);
c. The authentication of every party before any given access to the advertised WS.

In this manner, UDDI will play indeed the role of a trust centre and all exchanged messages between any given provider and client will be well protected.

A. The Mechanism of the Proposed Solution

As mentioned earlier, every provider or client of the advertised WS must be previously subscribed on the UDDI server to guarantee the security of any given transaction between them. We suppose also that the UDDI server owns a personal PKI which allows it to communicate in a secured manner with every involved actor.

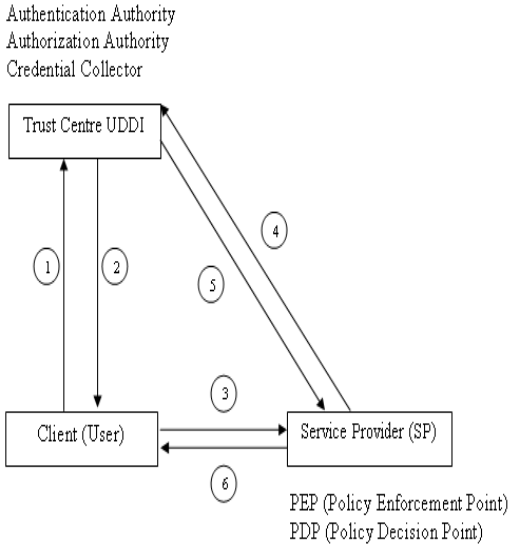

Figure3. The Mechanism of the Proposed Solution

Thus, if a given new provider would like to advertise any WS, he must achieve the following steps:

a. Register his complete identity which will serve to the authentication process over the UDDI centre;
b. Advertise both his PKI and the WS which can provide over the UDDI;

In the same manner if a given new client would like to access (consume) any advertised WS, he must achieve the following steps:

c. register his complete identity which will serve to the authentication process over the UDDI centre;
d. advertise his PKI over the UDDI;

Of course, to reduce the involvement of the UDDI centre during the authentication process and consequently the response time of our proposal, we suggest that only the first transaction or contact between any given provider and a new client which requires this involvement. It means that once a new client (customer) becomes known by any given provider, then he will be added automatically to a list of known customers with the corresponding PKI. So we suggest that every provider must own a list of customers where to store the required information to the authentication process of each of which and the corresponding PKI to encrypt every exchanged message with them. In this manner, hackers will not be able to interfere in exchanged messages. Figure-3 illustrates the mechanism of the proposed solution;

B. Scenario

This scenario is the elaboration of a kind of communications between client and service provider through attribute exchange with authentication reference called an artifact. An artifact is "small" bounded size of byte string. When artifact is conveyed to the source site the artifact unambiguously references an assertion. The artifact is conveyed to the service provider, which then acquires the referenced assertion by some further step.

a. Client looks for the required SWS and request for registration with Trust Centre (UDDI).
b. Then client get an artifact and public key of service provider.
c. The client request for the required service with the artifact.
d. SP request the Trust Centre an authentication document called Assertion, passing the artifact presented by the client intended to get service.
e. If the artifact is valid, the Trust Centre returns the authentication document to SP with adequate information about the client.
f. After the successful authentication, the SP allows the client to access the required service.

C. Threat model and Countermeasures

In the upper scenario, we can infer a few threat models. In the first place, we assume that a valid user requests a malicious SP for some resource. After the SP allows access to a resource, it stores the artifact sent by the client for other purpose. It may impersonate the same client with the artifact to some other SP. To alleviate this concern, the artifact needs to have shortest possible validity period consistent with successful communication of the artifact from source to destination. This is typically in the order of a few minutes. This ensures that a stolen artifact can only be used successfully within a small time window. The second case is that a malicious Client asks for some resource from a SP with other's artifact. A countermeasure is that it makes the trusted party to determine if an artifact is being requested by more than one client or not. In such a case, the trusted party must not provide the assertions to the SP, and then access to the resource will not be permitted.

Finally, the use of SAML assumes and requires trust between participants, but the SAML protocol does not include provisions to establish or guarantee this trust. SAML is not concerned with guaranteeing confidentiality, integrity, or non-reputability of the assertions in transit. For these purpose, it needs XML Enc and XML Dsig or other mechanism provided by the underlying communication protocol and platform. Consequently, the proposed solution improves substantially the security of WS especially if these services are intended for the big public.

IV. CONCLUSION & FUTURE WORK

We proposed in this paper a new solution that attempt to improve the security of web services especially those intended for the general public. Our proposal is based on two components; the first one is the personal PKI which is required by every client or provider of SWS. And the second one is some improvements of the UDDI functioning which should play the role of a trust centre in an attempt to provide adequate security for semantic web services. Our proposed solution is intended to improve the security of any kind of distributed application intended for the public. Several investigations are understudy, especially the implementation and the real evaluation of our proposal on a specific distributed application.

V. REFERENCES

[1] Web Services Description Language (WSDL), Version 2.0 Part: Adjuncts, W3C Working Draft, June 2007. [Online] Available: http://www.w3.org/TR/wsdl20-bindings/wsdl20-adjuncts.pdf

[2] SOAP Version 1.2 Part 1: Messaging Framework, W3C Proposed Recommendation, April 2007. [Online] Available: http://www.w3.org/TR/2007/REC-soap12-part1-20070427/

[3] Universal Description, Discovery and Integration (UDDI). 2002. UDDI v. 3.0, UDDI Spec Technical Committee Specification. October 2004. [Online]. Available: http://uddi.org/pubs/uddi-v3.0.2-20041019.htm

[4] P.Fremantle, D.Koeing, and C.Zenter. Building Web Services with java: making Sense of XML, SOAP, WSDL and UDDI, 2nd Edition. (Developer's Library), Sams, 2004.

[5] D. A. Haidar, F. C. N. Cuppens-Boulahia, and H. Debar. An extended RBAC profile of XACML. In Proceedings of ACM SWS'06, Alexandria, Virginia, USA, pp. 13-22, November 2006.

[6] D. Booth, H. Haas, F. McCabe, and E. Newcome. Web services architecture. W3C Working Draft, August 2003. [Online] Available: http://www.w3.org/TR/2003/WD-ws-arch-20030808/

[7] M. A. Rahman, A. Schaad, and M. Rits. Towards secure soap message exchange in a soa. In Proceedings of ACM SWS'06, Alexandria, Virginia, USA, pp. 77-84, November 2006.

[8] M. Khemakhem, H. B. Abdallah, and A. Belghith. Towards an agent-based framework for the design of secure web services. In Proceedings of ACM SWS'08, Alexandria, Virginia, USA, pp. 81-86, October 2008.

[9] J. Pamula and al. A framework for establishing, assessing and managing trust in inter-organizational relationships. In Proceedings of ACM SWS'06, Alexandria, Virginia, USA, pp. 23-32, November 2006.

[10] T. Imamura, B. Dillaway, and E. Simon. Xml encryption syntax and processing, W3C recommendation, December 2002. [Online] Available: http://www.w3.org/TR/xmlenc-core, December 2002.

[11] A. Freier, P. Karlton, and P. Kocher. The ssl protocol, version 3.0. In Internet draft, Netscape, November 1996. [Online] Available: http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt.

[12] A. Nadalin, C. Kaler, P. Hallam-Bake, and R. Monzillo. Web services security: Soap message security 1.0. OASIS standard, March 2004, [Online] Available: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

[13] D. Box, D. Ehnebuske, G. Kakivaya, A. Layman,N. Mendelsohn, H. Nielsen, S. Thatte, and D. Winer. Simple object access protocol (soap) 1.1, W3C Note, May 2000, [Online] Available: http://www.w3.org/TR/2000/NOTE-SOAP-20000508.

[14] D. Eastlake, J. Reagle, D. Solo, M. Bartel, J. Boyer, B. Fox, B. Lamacchia, and E. Simon. Xml signature syntax and processing. W3C Recommendation, May 2000. [Online] Available: http://www.w3.org/TR/xmldsigcore/

[15] D. Eastlake, J. Reagle, T. Imamura, B. Dillaway, and E. Simon. Xml encryption syntax and processing. W3C Recommendation, December 2002. [Online] Available: http://www.w3.org/TR/xmlenc-core/

[16] J. Hughes, E. Maler, Security assertions markup language (saml), version 2.0. OASIS working draft 3, February 2005. [Online] Available: http://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0-draft-03.pdf

[17] T. Moses, Xml access control markup language (xacml), version 2.0. OASIS standards, Feb 2005. [Online] Available: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[18] Bhavani Thuraisingham, "Security standards for the semantic web", ELSEVIER, Computer Standards & Interfaces, Vol. 27, 2005, pp.257–268.

[19] Bhavani Thuraisingham and Pranav Parikh, Trustworthy Semantic Web Technologies for Secure Knowledge Management ,2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, IEEE/IFIP-2008, pp186-193.

[20] Kumar S. Prajapati, R.K. Singh, M. De, A. "Security enforcement using PKI in Semantic Web" International Conference on Computer Information Systems and Industrial Management Applications (CISIM), Oct 2010, pp. 392-397.