RESOLVE - Impervious Trusted Semantic Web

Shubha Singh
Asst. Prof., MCA Department,
Kanpur Institute of Technology,
Kanpur -208001(india)

Pradeep Rai
Asst. Prof., CSE Department,
Kanpur Institute of Technology,
Kanpur-208001(India)

Prof. Raghuraj Singh
H.O.D., C.S.E. Department,
Harcourt Butler Technological Institute,
Kanpur-208002 (India)

ABSTRACT

World Wide Web is now having highly confidential data. The semantic Web is further extracting information from this data. But Extracting information through Agents required high level of security consideration.

This paper is proposing a system called RESOLVE for protecting this highly secured information through its full proof mechanism. It works with double layer of Security.

Keywords

Web services, Web Security challenges, Semantic Web, RESOLVE, and Cryptography.

1. INTRODUCTION

The World Wide Web is now a platform for providing a wide variety of e-commerce, business-to-business, business-to-consumer and other information based services. Web Services are the technology enabled bridges decoupled systems across various platforms, programming languages and applications. Interoperability among these applications is the main feature which is ensured by the use of standards such as SOAP, XML, and WSDL.

Nowadays organizations are implementing Web Services technologies on a broader scale just to enhance their market availability, but some basic issues such as security must be addressed and understood first. At this time, there are no broadly-adopted specifications for Web Services security, routing, reliable messaging, and reliable transactions. As a result developers can either develop services that do not use these capabilities or can develop ad-hoc solutions that may lead to interoperability problems. Therefore, it becomes increasingly important to provide additional capabilities to ensure global availability, reliability and security.

Some security aspects of Web Services are currently being standardized in OASIS. For example, the WS-Security specification describes how to use existing W3C security recommendations such as XML Signature and XML Encryption, to ensure the integrity and confidentiality of SOAP messages. Other work also describes how existing digital credentials and their associated trust semantics can be securely associated with SOAP messages.

The advent of the Semantic Web technology will pave the way for the development of Semantic Web Enabled Web Services. The use of Semantic Web technologies such as ontologies will truly transform the Web into a distributed device of computation that is based on machine process able and machine interpretable content.

In the current paper we are proposing a system specially meant for Web services which are dealing with the information which needs high security aspects just as credit card , bank related transactions etc. In this paper we have introduced a new perspective of security in which database oriented operation are mostly used. This particular system uses double security system just to ensure the full proof security.

2. Web Services Security Challenges and Requirements

Security can be a key inhibitor to the widespread implementation and adoption of Web Services. At the highest level, the objective is to create an environment, where message level transactions and business processes can be conducted securely in an end-to-end fashion.

The requirements for providing end-to-end security for Web Services are:

2.1. Authentication mechanisms

This is needed in order to allow the mutual authentication of service provider and a service invoker to verify their identities.

2.2. Authorization to access resources

Once authenticated, authorization mechanisms control invoker access to appropriate system resources. There should be controlled access to systems and their components.

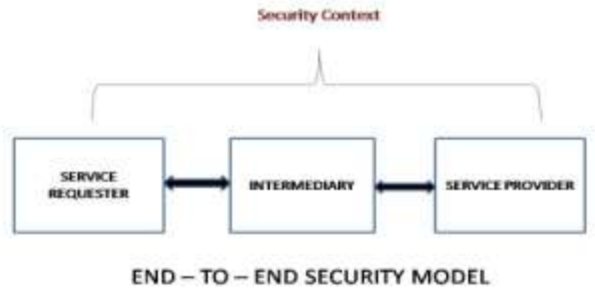


Figure -1

2.3. Data integrity and confidentiality

It ensures that information has not been modified during transmission and is only accessible to intended parties. Encryption technology and digital signature techniques can be used for this purpose.

2.4. Integrity of transactions and communications

This is needed to ensure that the business process was done properly and the flow of operations was executed in a correct manner.

2.5. Non-repudiation

So that a party to a transaction cannot deny the occurrence of the transaction.

2.6. End-to-end integrity and confidentiality of messages

The integrity and confidentiality of messages must be ensured even in the presence of intermediaries.

2.7. Provide Security and Audit Trails

This is needed in order to trace user access, behavior and system integrity verification.

2.8. Distributed enforcement of security policy

Implementers must be able to define a security policy and enforce it across various platforms with varying privileges.

2.9. Point to Point Security Context

Implementers must note that security is a balance of assessed risk and cost of countermeasures. Depending on implementers risk tolerance, point-to-point transport level security can provide enough security countermeasures.

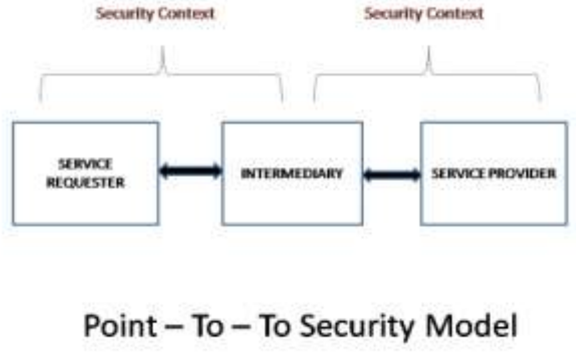


Figure-2

3. Current Security Specifications for Web Services

In order to be able to facilitate the management of multiple identities polices and trust relationship at every point of interaction the notion of Security Authority (SA) is introduced. The SA is depicted in above Figure, where it acts as a facilitator for identity, policy management: authentication, authorization and audit. The SA enables cross-domain trust management, delegation and federation networks. Currently there are extensive efforts in standard bodies for developing specifications to address Web Services security .Major vendors have promised support for open security standards. Some of the important security standards are summarized next.

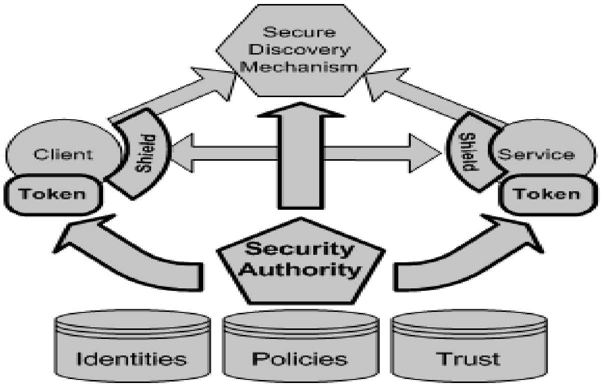


Figure-3

3.1. XKMS

XML Key Management Services (XKMS) is used for clients to securely access public key-related services such as key generation, registration and revocation. It also includes methods for the validation of certificates and signatures. In essence, XKMS buffers applications from dealing with the complexities of PKI. XKMS allows applications to delegate the details of this task to remote or local Web services

3.2. SAML

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains (between *identity provider* and a *service provider* .SAML assumes the *principal* (often a user) has enrolled with at least one identity provider. This identity provider should provide local authentication services to the principal. A service provider relies on the identity provider to identify the principal. At the principal's request, the identity provider passes a SAML assertion to the service provider. On the basis of this assertion, the service provider makes an access control decision.SAML is also trying to solves the *Web Browser Single Sign-On* (SSO) problem.

3. 3 XACML

XACML stands for *eXtensible Access Control Markup Language*. It is a declarative access control policy language implemented in XML and a processing model.It describes how to interpret the policies

3.4. XML Signature and XML Encryption:

XML Signature (also called *XMLDsig*, *XML-DSig*, *XML-Sig*) is a W3C recommendation that defines an XML syntax for digital signatures.In functionality it is in common with PKCS#7 but is more extensible and geared towards signing XML documents. It is used by various Web technologies such as SOAP, SAML, and others.

XML Encryption, also known as XML-Enc, is a specification, governed by a W3C recommendation that defines how to encrypt the contents of an XML element. Encryption can be used to encrypt any kind of data, it is known as "XML Encryption" because an XML element (either an Encrypted Data or Encrypted Key element) contains or refers to the cipher text, keying information, and algorithms.

3.5. WS-Security

WS-Security is a flexible and feature-rich extension to SOAP to apply security to Web services. It is a member of the WS-* family of web service specifications and was published by OASIS. The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security.

3.6. WS-Secure Conversation

A Web Services specification, created by IBM and others, that works in conjunction with WS-Security, WS-Trust and WS-Policy to allow the creation and sharing of security contexts. Extending the use cases of WS-Security, the purpose of WS-SecureConversation is to establish security contexts for multiple SOAP message exchanges, reducing the overhead of key establishment.

3.7. WS-Trust

is a WS-* specification and OASIS standard that provides extensions to WS-Security, specifically dealing with the issuing, renewing, and validating of security tokens, as well as with ways to establish, assess the presence of, and broker trust relationships between participants in a secure message exchange

3.8. WS-Federation

is an Identity Federation specification, developed by BEA Systems, BMC Software, CA, Inc., IBM, Layer 7 Technologies, Microsoft, Novell, Ping Identity, and VeriSign. Part of the larger Web Services Security framework, WS-Federation defines mechanisms for allowing disparate security realms to broker information on identities, identity attributes and authentication.

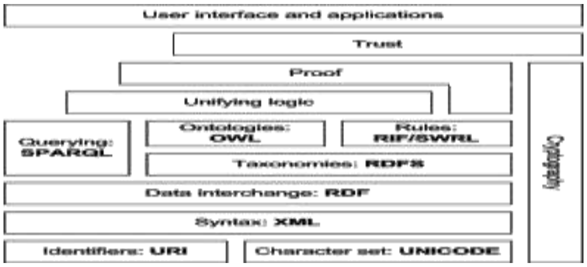
3.9. Web Services Security Kerberos Binding

is a Web Services specification, authored by IBM and Microsoft, which details how to integrate the Kerberos authentication mechanism with the Web Services Security model.

4. RESOLVE

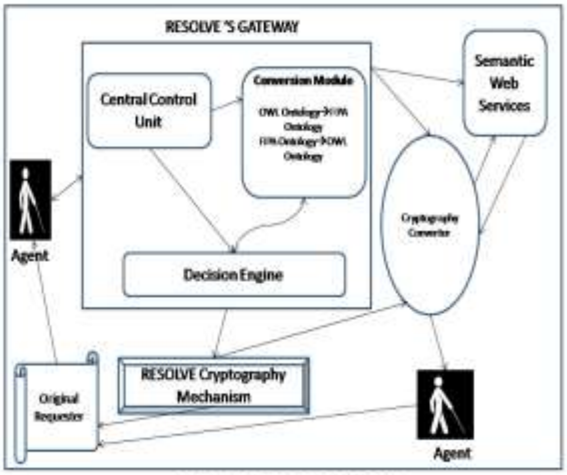
Our proposed system RESOLVE basically deals with a Multi Agent System.. The applications which involve high level of database related queries as well as the information needs high level of security are the target area of this proposed System.

To understand the functioning of the RESOLVE, we have to first understand the functioning of semantic web. Semantic web is an effort to enhance current web so that computers can process the information presented on WWW, interpret and connect it, to help humans to find required knowledge. In the same way as WWW is a huge distributed hypertext system, semantic web is intended to form a huge distributed knowledge based system. The focus of semantic web is to share data instead of documents. In other words, it is a project that should provide *a common framework that allows data to be shared and reused across application, enterprise, and community boundaries. It is a collaborative effort led by World Wide Web Consortium (W3C).***The layers of semantic web architecture are described as below**:-



Semantic Web Architecture in layers
Figure-4

In the above architecture our main emphasis is on Query processing. For query processing we have to understand the working of layers related to RDF, Querying, Ontologies , Rules and Unifying logic. The major thing we have to understand for RESOLVE is the fact that when this particular semantic web services uses their knowledge base for fetching the data which needs high security considerations. The main element of RESOLVE is shown below in the figure:



OVERALL WORKING OF RESOLVE

Figure-5

The RESOLVE is neither a Web service nor an Agent. It is an application which works in a distributed environment. It will work as gateway in between the Agent and the Semantic Web Services. The major components of the Resolve are as below:

4.1. Central Control Unit (CCU)

This particular Unit supervises the request as given by the Agent and also works as the first interface for the Agent. The

Supervision is meant for categorizing the type of information inquired by the Agent. Categorizing is essential for performing the initials task. CCU also generates the token$_1$ for the complete RESOLVE processing. It generates the token according to the categories. It also supervises the flow of the Messages in a sequence. This CCU also passes the token and request to the Decision Engine.

4.2. Conversion Module

It is bidirectional in nature. Since this ontology is written in OWL for a semantic web service, which though is allowed as a valid content language by FIPA but is not as expressive as SL, so there is a need to translate this ontology from OWL to SL. The CU feeds this ontology to the OWL to FIPA ontology translator, which returns the FIPA Ontology equivalent of the OWL ontology fed as an input. This is done with the help of matchmaking service that returns a reference or handle of that service to the CU. This handle enables the CU fetch the service profile of the service and its ontology, without which semantic understanding is unattainable.

4.3. Decision Engine

This is the Module which decides which particular Agent inquiry needs more attention regarding the security aspect. The decision is totally based on the knowledge base. If suppose the inquiry needs to fetch the database field which is highly confidential in nature. Then this particular Decision Engine will take decision and pass it to the RESOLVE Cryptography Mechanism and the semantic web service with the proper token$_1$.

4.4. RESOLVE Cryptography Mechanism

This is the Mechanism which is responsible for selecting a cryptography algorithm according to the information provided by the Decision Engine. This particular mechanism generates a key and sends it to the Cryptography Convertor along with the Token$_2$ with the cryptography tag in it. This particular Mechanism also has the responsibility to send this token$_2$ and key to the Original requestor (the application or the website) which initiated the Agent who wants required information. This mechanism sends this to the Original Requestor independently so that after receiving the information from the Agent the Requester can decipher it.

4.5. Cryptography Convertor

This is the module which after receiving the information and token$_1$ from the semantic services encodes it according to the information and token$_2$ provided by the RESOLVE Cryptography Mechanism. Then this information is passed to the Agent.

4.6. Tokens

In this RESOLVE system we use two types of tokens, Token$_1$ and Token$_{2.}$ Token$_1$ is used for maintaining the flow and Token$_2$ is used for the cryptography purposes. In this scenario the Agent got the information in the Encoded form and there is nothing in the information to decipher it. When the Agent give the information back to the Original requestor then this information will be changed according to the token$_2$ and the key given by the RESOLVE Cryptography mechanism. Then the original registered requester uses this information for further semantic services data. The main theme behind this system is all the semantic web security services will function same as before; we are just covering the complete information into a packet which is secured by RESOLVE.

5. Comparison of RESOLVE with the current Scenario of Semantic Web Services

In the current scenario semantic web services are using all the security specification as described in the Heading 3 of this paper. RESOLVE will not change in this current situation but it only adds another covering of security. RESOLVE will only work when the Decision Engine decided that the information which is required is highly confidential in nature. If it is not then only token$_1$ will pass and there will be no extra RESOLVE security covering.

6. Future Scope of Work

We have to develop Quiet efficient Algorithms for Decision making. RESOLVE has to modify more so that ontology can easily be described. Some efficient Cryptography algorithms should also be cultivated so that it can meet out the needs of RESOLVE Cryptography Mechanism.

7. ACKNOWLEDGMENTS

The authors would like to express their cordial thanks to
Mr. Anshul Pandey (Research Engineer Intel, USA) and
Mr. Chandresh Verma (Project Manager, Satyam) for their valuable advice.

8. REFERENCES

[1] Greenwood, D., Calisti, M., Nagy, 2005, J.: Semantic Enhancement of a Web Service Integration Gateway, AAMAS SOCABE Workshop,Utrecht, Netherlands

[2] Greenwood, D., Calisti, M., 10-13 October, 2004, An Automatic, Bi-Directional Service Integration Gateway, IEEE Systems,Cybernetics and Man Conference; the Hague, Netherlands

[3] Laukkanen, M., Helin, H., July 2003. Composing workflowsof semanticweb services. In Proc. of the 1st International Workshop on Web Services and Agent Based Engineering, Sydney, Australia.

[4] Richler, M., Kersten, G., Strecker, S., 2003, Towards a Structured

[5] Web Services Architectures, W3C Working Draft 14 May 2003: http://www.w3.org/TR/2003/WD-ws-arch-20030514/

[6] B. Atkinson, G. Della-Libera, S. Hada, M. Hondo, P. Hallam-Baker, J. Klein, B. LaMacchia, P. Leach, J. Manferdelli,H. Maruyama, A. Nadalin, N. Nagaratnam, H. Prfullchandra, J. Shewchuk, and D. Simon, 2002. http://www-106.ibm.com/developerworks /webservices /library/ws-secure/.

[7] M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon. Xml-signature syntax and processing rules. http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/, August 2001.

[8] http://www.w3.org/TR/2003/WD-ws-arch-20030514/

[9] http://www.w3.org/TR/ws-arch/

[10] Guangtao Xue, Qunhua Pan, and MingLu Li, "A New Semantic-based Query Processing Architecture," 2007 international Conference on Parallel Processing Workshops (ICPPW 2007), September 10-14, 2007.

[11] Dongwon Lee, Wang-Chien Lee, and Peng Liu, "Supporting XML Security Models using Relational Databases:A Vision," Lecture Note In Computer Science, Springer-Verlag Berlin Heidelberg, Vol. 2824, Berlin Germany,September 8, 2003, pp. 267-281.

Shubha Singh received her Master degree in Computer Applications from Agra university in year 2002 and M.Tech in computer science in year 2007. She has worked as associate in govt project at IIT, Kanpur. Presently she is working as Asst. Prof. in Compute Application Deptt. At KIT ,Kanpur.She has more than 8 years teaching experience. Her areas of interest includes DBMS,Networks and Operating Systems. Her research papers related to Computer Security and semantic web are published in several international journals.

Pradeep Rai received his bachelor degree in computer Science & Engineering from KNIT, Sultanpur in the year 2002 and M.Tech in computer Science in the year 2008. Currently he is working as Asst. Prof. in CSE Department at KIT, Kanpur. His area of interest includes VPN, wi-fi networks, network Security. His many research papers related to Computer Security are published in several international journals.

Dr. Raghuraj Singh received his
B. Tech degree in Computer Science & Engineering
From Harcour Butler Technological Institute, Kanpur India, in 1990, M.S. degree in Software Systems from the Birla Institute of Technology & Sciences, Pilani, India, in 1997, and Ph.D. degree in Computer Science & Engineering from the Uttar Pradesh Technical University, Lucknow, India, in 2006. He is currently a Professor in the Computer Science & Engineering Department at the Harcourt Butler Technological Institute, Kanpur, India. His research interests include software architecture, software reliability/quality assessment, Object-oriented design measurements, and software testing. He is a member of IETE, ISTE, and IE.