An Overview of maintaining security in Web services

S.Anjugam P.Visalakshi,
[1, 2]Asst.Professor (Senior Grade)
[1, 2]Department of Computer Applications
SRM University, Kattankulathur, Chennai.
Tamil Nadu, South India

Abstract

Web Services are a loosely-coupled, language-neutral,platform- independent way of linking applicationswithin organizations, across enterprises, and across the Internet. With web services we can exchange data between different applications and different platforms. While we are exchanging the data, the unauthorized entities should not be able to access the information within the message. In this paper, we discuss the areas of security and how to maintain that security. It also describes the benefits of the web services and the standards which are used on the web services.

Key Words: Web service components, Benefits of Web service,and Web Services Security.

I Introduction

A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processableformat (WSDL).Other systems interact with the web service in a manner prescribed by its description using SOAP message, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

A Web service is an abstraction notion that must be implemented by a concrete agent. The agent is the concrete piece of software or hardware that sends and receives messages.

- **Overview of Engaging a Web Service**

There are many ways that a requester entity might engage and use a web service. In general, the following steps are required , as illustrated in figure-1.

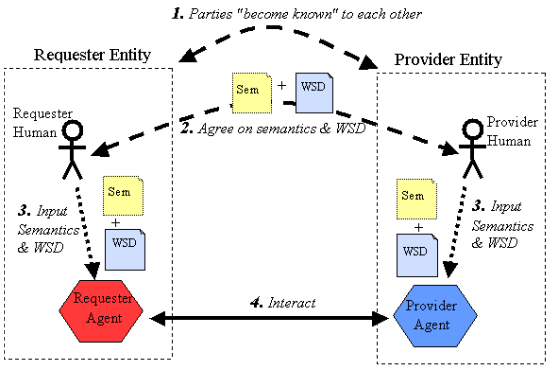

Fig-1: Web Service

1. The requester and provider entities

Become known to each other or at least one becomes know to the other.

2. The requester and provider entities somehow agree on the service description and semantics that will govern the interaction between the requester and provider agents.
3. The service description and semantics are realized by the requester and provider agents
4. The requester and provider agents exchange the messages, thus performing some task on behalf of the requester and provider entities

II- COMPONENTS OF WEB SERVICES

The basic Web services platform is XML + HTTP . All the standard Web servicesworks using the following components:

- **SOAP (Simple Object Access Protocol)**

SOAP is an XML-based protocol for exchanging information between computers. It is a communication protocol between applications, standard format for sending messages to communicate via Internet. It is platform independent, Language independent, simple and extensible

- **UDDI (Universal Description, Discovery and Integration)**

UDDI is a specification for a distributed registry of Web services, platform independent and open framework. It can communicate via SOAP, CORBA, Java RMI protocol.

It is an open industry initiative enabling business to discover each other and define how they interact over the Internet.

- **WSDL (Web Services Description Language).**

It is an XML based protocol for information exchange in decentralized and distributed environments.

Iii Benefits of Web Services

- **Exposing the function on to network**
  Web services allows us to expose the functionality of our existing code over the network. Once it is exposed on the network, other application can use the functionality of our program.
- **Connecting Different Application**
  Web services allows different applications using different languages to talk to each other and share data and services among themselves. So, Web services is used to make the application platform and technology independent.
- **Standardized Protocol**
  Web services uses standardized industry protocol for the communication.
- **Loosely Coupled Applications**
  Web services are self-describing software modules which encapsulates discrete functionality. Web services can be developed in any technologies(like C++, Java, .NET, PHP, Perl etc.) and any application or Web services can access these services. So, the Web services areloosely coupled application and can be used by application developed in and technologies.
- **Web Services are Self Describing**
  Web services are self describing applications, which reduces the software development time.
- **Automatic Discovery**
  Web services automatic discovery mechanism helps the business to easy find the Service Providers. This also helps our customer to find our services easily.
- **Business Opportunity**
  Web services has opened the door to new business opportunities by making it easy to connect with partners.

IV – WEB SERVICES SECURITY

In securing Web Services, there are five fundamental areas to consider: Message Level Protection, Message Privacy, Parameter Checking, Authentication and Authorization.

- **Message Privacy**

The Message privacy deals with the confidentiality of a message. The Confidentiality is concerned with protecting the privacy of the message contents. A message is considered to have remained confidential if no service or agent in this message path not authorized to do so viewed its contents. The message header contains the information of XML Signature and Token , shown in the figure-2

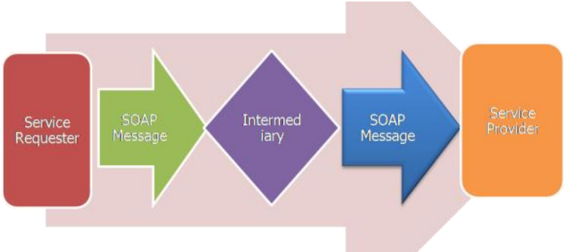

Fig-2: SOAP message in Transit

To ensure confidentiality an encryption scheme must be implemented. Once the message has been received by anentity (intermediary) it is decrypted in its entirety.

The XML Encryption standard provides the necessary framework for accomplishing this task. The XML Encryption allows for the encryption of any combination of the message body, header, attachments and sub-structures.

When a message or part of a message is encrypted, the encryption information can be made available in the message header. This information is useful for complex services since each Web Service in the claim will need to know how to decrypt the section of the message relevant to their services. This information should not be the actual key to decrypt the message.

For example, when a requester encrypts a message body and XML signature information in the header, it may then specify in the header that it has used the providing service's public key. A public key allows for the encryption of data but only the private key may decrypt the data. Once the provider receives the message it sees that the message has been encrypted using its public key. The provider then decrypts the message using its private key.

XML Encryption allows multiple different keys to be used with in a message to encrypt different sections, elements of the message.

- **Message Level Protection**

Message Level Protection has to do with message integrity. Integrity means ensuring that a message's contents have not changed during transmission. This means being able to detect when a SOAP message (message) has been modified from its original state and the ability to guarantee that the contents have not been modified. This is done by creating a message digest.

To ensure message integrity, a technology is required that is capable of verifying that the message received by a service is authentic in that it has not been altered in any manner since it first was sent. XML-Signature provides piece of information that represents a digital signature. This signature is tied to the content of the document so that verification of the signature by the receiving service only will succeed if the content has remained unaltered since it first was sent.

The figure-3 illustrate the XML-Encryption can be applied to parts of a soap header, as well as the contents of the SOAP body. When singing a document , the XML-signature can reside in the SOAP-header.

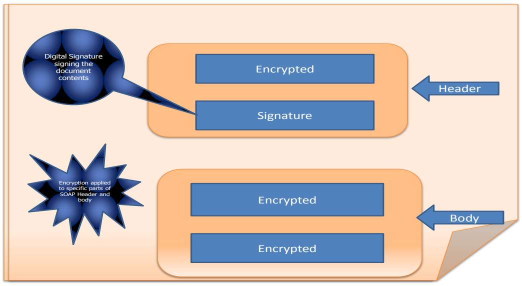
Digital Signature signing the document contents
Encrypted
Signature
Header
Encryption applied to specific parts of SOAP Header and body
Encrypted
Encrypted
Body

Fig-3: A digitally signed SOAP message containing encrypted data.

There are several Token options for signing a message. These options fall under one of two categories; they can either be endorsed or unendorsed.

(1) **Endorsed**: An endorsed token is one which the claims of the token can be validated by a trusted authority. An example of this kind of Token is a X.509 certificate.

(2) **Unendorsed:**An unendorsed Token is one which the claims may not be validated by a trusted authority. An example of this kind of token is a username-password Token.

- **Message Validity**

Message Validity is ensuring that the contents of a message are appropriate to the service and that they are well formed. Checking the contents of a message can be subdivided into two categories; Verifying data types and checking for malicious code. Verifying that the data types passed to an operation are those which the services are expecting is straight. Checking for malicious code within the message is not so straight forward.

Malicious code within a message ca appear as part of the XML message or as parameters to be passed to operations. XML viruses and XML worms are commonly passed within the contents of any XML document or message. Even after verifying that the parameters within a message are appropriate for the operation(s), their may be malicious code present.

Ensuring that a message is well-formed is another step in Message Validity. Since the messages are in XML, it is possible that a message contains a circular-reference. A circular-reference may appear maliciously or through poor programming. Circular-references cause a system to encounter a run-out-of-memory error and shutdown. When done maliciously this is known as a denial-of-service attack. Proper parsing of a message will catch nested loops.

- **Authentication**

Authentication requires that a message being delivered to a recipient prove that the message in fact from the sender that it claims to be. In other words, the service must provide proof that its claimed identity is true.

In its simplest form, authentication could be a username and password combination. However, this is only possible if there is already a relationship between the requester and provider. Because of the distributed nature of web services, a requester may be previously unknown to the provider.

When an unknown requester authenticates it sends information about themselves to the provider. This information is known as credentials.For the unknown requester, the authentication can be achieved through a trusted authority, who issue certificates which can be used for authentication. A provider can evaluate the certificate and contact the trusted authority for verification.

However, there may be an intermediate service contacting the provider on behalf of the requester and once established the requester and provider will communicate.

- **Authorization**

In organizations, highly sensitive data and information must be protected with access control systems. These control systems allow defining and controlling which users are authorized to access specific applications and data but prohibit the access of unauthorized users.

Authentication is the granting of rights, which includes the granting of access based on access rights. Once authenticated, the recipient of a message may need to determine what the requestor is allowed to do.

An access control implementation compares access control information such as the rights of the requestor with the policies or permission needed to access the resource. If the rights of the requester dominate the control policy; then access can be granted; otherwise access is denied.

The two most common access control implementations are ACL(Access Control List) used in the Unix environment for file and directory security and RBAC (Role Based Access Control) which consists of objects, operations, permissions, roles, users and system and Administrative functions(System functionality, administrative operations and reviews) .

V Conclusion

Using web services we can exchange data between different applications and different platforms. While exchanging the data, the unauthorized person can access the information within the message. Hence, to secure the Web Services,we have to consider five fundamental areas: Message Level Protection, Message Privacy, Parameter Checking, Authentication and Authorization. This paper has presented an overview of how to securethe Web Services in all those areas. InFuture , we will develop a security tool for Web Services.

References

1. YUE Kun+, WANG Xiao-Ling, **"Underlying Techniques for Web services : a survey",** Department of computer science and Engineering, Fudan University, Shanghai, China.
2. Thomas Erl, " Service-Oriented Architecture – Concepts, Technology and Design", PearsonEducation,Inc.
3. Richard S.Patterson, John A.Miller, University of Georgia, " Security and Authorization Issues in HL 7 Electronic Health Records: A Semantic Web Services Based Approach",International Journal of Web Services research.
4. KarthikeyanBhargavan, CeedricFournet, Andrew D.Gordin, & Riccardo Pucella,"TulaFale : A security Tool for Web Sevices", Microsoft research.
5. WebServices, www.w3schools.com/webservices
6. Web services Security – www.tutorialpoint.com/webservices
7. SOA and Web Service – www.roseindia.net/web services
8. Webservices – http://msdn.micosoft.com/en-us/library/