IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-6, Issue-4 E-ISSN: 2347-2693

A Survey on Security Issues in Web Services

Satyam Akunuri[1*], Subbarao Perugu[2], Rajendra Prasad B[3]

[1] Computer Science and Engineering , Sreenidhi Institute of Science and Technology, Hyderabad, India
[2] Computer Science and Engineering , Sreenidhi Institute of Science and Technology, Hyderabad, India
[3] Computer Science and Engineering , Sreenidhi Institute of Science and Technology, Hyderabad, India

Corresponding Author: satyamakunuri@gmail.com, Tel.: +919177656326

Available online at: www.ijcseonline.org

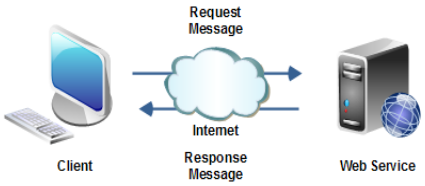
Received: 20/Mar/2018, Revised: 28/Mar/2018, Accepted: 19/Apr/2018, Published: 30/Apr/2018

***Abstract*—** Web Service is a collection of software components which provide the services over the web. Web services are playing a key role in a wide range of modern business applications. The nature of loosely coupled connections and open accessibility may cause several security issues. Recently, a number of new standards and protocols have been introduced. When deploying a web service, security is one of the major issue that need to be addressed. In this paper, we discuss the possible threats to web services and recommend preventive measures**.**

***Keywords*—** WSDL, SOAP, REST, HTTPS, X.509

I. INTRODUCTION

Web Service is a program that can be accessed remotely by using different XML based languages. The service can be described in a standard XML document i.e WSDL (Web Service Description Language). All services that are described in WSDL can be invoked to access those services.



The web services can be developed in either of the following ways. Web services can be implemented in the form of Simple Object Access Protocol (SOAP) based in which an XML message frame work designed to exchange the structured information. We can also develop REST(Representational State Transfer)ful web services. It describes set of design rules for creating stateless service are called resource service which are identified by their URIs. The characteristics of web services are Publish, Find and Bind.

II. WEB SERVICES SECURITY (WSS)

Web services are used by an increasing number of companies as they provide services to customers and business partners through the Internet. Security is an important feature of web service. Since almost all web services are exposed to the network, there is always a chance of security threat to the web service.

Web services security includes the following aspects

Peer Authentication: It is a process of uniquely identifying the end users or processes.

Access Control: It is the process that granting access to specific resources and operations based on authenticated user's entitlements.

Privacy: It is the process of making sure that the information remains private and confidential. It can be achieved through encryption and decryption process.

Integrity: Making sure that the information remains same during the transmission. Integrity for data in transmission is typically provided by using hashing techniques and digital signatures.

2.1 Security Challenges for Web services

The web services are:

- Loosely coupled
- Based on passing of readable and self-describing business messages in XML
- Easily bypass network firewalls
- Expose business service through APIs
- Enable multi-hop composite applications

III. WSS REQUIREMENTS

Web service security at Message and Transport levels.

Message level security: This can be applied when security is essential to a web service application. It uses basic HTTP authentication in which user name and passwords are verified or authenticate a client to the secure end point. This can be embedded in HTTP request that is carried by SOAP message.

When the service provider receives the HTTP Request, the credentials are verified at server end. Message level security used to assure confidentiality by encrypting message components, integrity through digital signatures and authentication by requiring username, X.509 or SAML tokens.

Transport Level Security: Transport level security provides the basic authentication; it can be enabled or disabled from message level security independently. The security at transport level is minimal. It uses SSL (Secure Socket Layer) that runs along with HTTP. HTTP is insecure protocol where all messages sent between two ends over a unsecured network. To make secure HTTP we can apply transport level security. SSL provides authentication, data protection and cryptographic token support for secure transmission. To enable this service port address must starts with on URL from https://.

IV. DEPLOYMENT CONSIDERATIONS

To prevent against the issues identified above, a number of Web services and HTTP Standards have been drawn up

4.1 W3C XML Encryption

WS-Security serves as a container for a variety of elements, each of which provides a partial security solution. The elements defined in the specification are as follows

a) <Security> —The enclosing tag
b) <UsernameToken>—The username and password
c) <BinarySecurityToken>—contains binary data such as X.509 certificates and Kerberos tickets
d) <SecurityTokenReference> -provides for the external storage of claims (privileges)

4.2 W3C XML Signature

a) <ds:Signature>
b) <xenc:EncryptedKey>

4.3 Web Services Security Tokens

Used to help the receiver of the message to identity and verify the sender. Security tokens give a mechanism for conveying security information within SOAP message, and the token itself is represented in XML.

The following security tokens are supported:

a) Username Tokens: used to identify the requestor by "username", and an optional password.

b) X.509 Tokens: X.509 digital certificate help to authenticate a SOAP message or to identify a public key with a SOAP message that has been encrypted

c) Kerberos Tokens: Allows a service to authenticate the Kerberos ticket and interoperate within existing Kerberos domains.

4.4 Security services through HTTPS:

Usually one-sided authentication challenge at play in websites, with the client challenging the server but not the other way around, shows up in Tomcat's configuration file, TOMCAT_HOME/conf/server.xml. Here is the entry for HTTPS:

```
<Connector port="8443" protocol="HTTP/1.1"
SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false"
sslProtocol="TLS"/>
```

The clientAuth attribute is set to false that indicate Tomcat does not challenge the client. If the clientAuth attribute were set to true, then Tomcat would challenge the client's user agent; a setting of true might be of interest for web services in particular. In this configuration file, there is no setting for a serverAuth because the default client behaviour is to challenge the server.

4.5 Container-Managed Security

Tomcat web server provides container-managed authentication and authorization. The domain plays a central role in the Tomcat approach. A domain is a collection of resources, including web pages and web services, with a designated authentication and authorization facility**.** A realm is an organizational tool that allows a collection of resources to be under a single policy for access control.

Configuring Container-Managed Security under Tomcat

Tomcat approach to security is also declarative rather than programmatic; i.e, details about the security Realm are specified in a configuration file rather than in code. The configuration file is the web.xml document included in the deployed WAR file.

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app>
....
</security-role>
<security-constraint>
<web-resource-collection>
<web-resource-name>Users-Roles Security</web-resource-name>
<url-pattern>/tcauth</url-pattern>
</web-resource-collection>
<auth-constraint>
<role-name>satyam</role-name>
</auth-constraint>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
<login-config>
<auth-method>BASIC</auth-method>
</login-config>
```


….
</web-app>
In the revised web.xml, there are four points of interest:
• The resources to be secured are specified as a web-resource-collection . In this case, the collection includes any resource available through the path /tcauth, which is the path to TempConvert service deployed in a WAR file. The security thus covers the service's two encapsulated operations, f2c and c2f . This path includes the WSDL, as the URL for the WSDL ends with the path /tcauth?wsdl .
• Access to resources on the path /tcauth is restricted to authenticated users in the role of bigshot. If Fred is to invoke, say, the f2c method, then Fred must have a valid username/password and be authorized to play the role of bigshot.
The HTTP authentication method is BASIC rather than one of the other standard http methods: DIGEST, FORM, and CLIENT-CERT. Each of these will be clarified shortly. The term authorization is used here in the broad sense to cover both user authentication and role authorization.The transport is guaranteed to be CONFIDENTIAL, which covers the standard HTTPS Services of peer authentication, data encryption, and message integrity. If a user tried to access the resource through an HTTP-based URL such as http://localhost:8080/tc/tcauth, Tomcat would then redirect this request to the HTTPS-based URL https://localhost:8443/tc/tcauth.(The redirect URL is one of the configuration points specified in conf/server.xml.

V. CONCLUSION

Web Service Security is an emerging standard for Web service applications. It defines options for authentication, message privacy and integrity issues. The use of XML Signature and XML Encryption in SOAP headers. As one of the building blocks for securing SOAP messages, it is intended to be used in conjunction with other security techniques. Digital signatures need to be understood in the context of other security mechanisms and possible threats to an entity. Web services security is still relatively new in terms of their practical implementation, web architects and developers need to be careful in how they deploy Web services. In addition to the protective measures discussed in this document, standard recommendations for the security of web applications should also to be followed.

REFERENCES

Books
[1] Stephen Potts, Mike Kopack Sams. Teach Yourself Web Services in 24 Hours. United States of America, Indianapolis, Indiana: Sams Publishing, 2003.
[2] Martin Kalin. Java Web Services: Up and Running. United States of America, CA: O'Reilly,2009.

Journals and Conferences
[1] Aruna.S, "Security in Web Services- Issues and Challenges," International Journal of Engineering Research & Technology (IJERT) Vol. 5 Issue 09, September-2016.
[2] Lee, S., Jo, J. Y., & Kim, Y. (2015, June). Method for secure RESTful web service. In Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on (pp. 77-81). IEEE.
[3] Noor A. Altaani, Ameera S. Jaradat, "Security Analysis and Testing in Service Oriented Architecture," International Journal of Scientific & Engineering Research, Volume 3, Issue 2, 2012.
[4] Balasubramanian, N., & Ruba, A. (2012, August). Security: a major threat for web services. In Advanced Communication Control and Computing Technologies (ICACCCT), 2012 IEEE International Conference on (pp. 104-109).
[5] Masood, A. (2013, November). Cyber security for service ori- ented architectures in a Web 2.0 world: An overview of SOA vulnerabilities in financial services. In Technologies for Home- land Security (HST), 2013 IEEE International Conference on (pp. 1-6). IEEE.
[6] Saravanaguru, R. A., Abraham, G., Ventakasubramanian, K., & Borasia, K. (2013).Securing Web Services Using XML Signa- ture and XML encryption. arXiv preprint arXiv:1303.0910.
[7] Hassan Reza, and Washington Helps, "Toward Security Analysis of Service Oriented Software Architecture," Proceedings of the 2011 International Conference on Software Engineering Research and Practice, Vol. II, 2011.

Authors Profile

Mr. Akunuri Satyam, Assistant Professor, Sreenidhi Institute of Science and Technology, Hyderabad He Perused B.Tech in CSE, from Kakatiya University and M.Tech from JNTUH. He has 10 Years of Experience in Teaching and handled various subjects in Computer Science Stream. He has presented papers and has participated in number of seminars and conference in different levels. He can be reached at satyamakunuri@gmail.com
.

Mr. Perugu SubbaRao, Assistant Professor, Sreenidhi Institute of Science and Technology, Hyderabad He Perused B.Tech in CSE, and M.Tech from NITS. He possess 4 Years of Experience in Teaching and has handled various subjects in Computer Science Stream. He has expertise in theory of computation and compiler design concepts.He has attended number of seminars and conference in different levels. Reach him at subbaraoperugu@gmail.com

Mr. Rajendra Prasad Banavathu, Assistant Professor, Sreenidhi Institute of Science and Technology, Hyderabad.He Perused B.Tech in CSE from CR Reddy College of Engineering and M.Tech from JNTUK. He possess 3 Years of Experience in Teaching and has handled various subjects in Computer Science Stream. He attended conferences at various levels. Reach him at rajendranayakpb@gmail.com

