STUDY ON IMPROVING WEB SECURITY USING SAML TOKEN

Venkadesh M M.tech, Dr. A. Chandra Sekar M.E., Ph.D. MISTE

1Research Scholar
Bharath University
Chennai 73, India.
venkadeshkumaresan@yahoo.co.in

2Professor - CSC Department
St. Joseph’s College Of Engineering
Jeppiaar Nagar, Chennai – 600119.
drchandrucse@gmail.com

Abstract: Web service is the most important word which is most commonly used by all computer professionals. Web services are mainly used for communicating different platform within a network connection. Web services are created based on SOA architecture. SOA platform is most popularly used in distributed systems. When using in distributed system security becomes prominent. This study is carried out on improving web security using SAML tokens. SOA principles and SAML are used in this study.

Keywords: Web Services, SAML, XML, HTTP, SOAP.

1. Introduction

Let us explain the concept of web services with the following example. Let us consider we have an software application use in some service centre which is not web enabled and it does not support any other platform. But it is considered to be a powerful tool for all services. In older days it becomes costly to convert it is accessible for all platforms. After the concept of web services came into force it become easier to access by different platform and was easily web enabled. Due to web services we have the advantage of less time and less cost management. SAML is a XML (Extensible Markup Language) based data format. It is used for transferring security information from client to server. SAML is developed by the Security Services Technical Committee (SSTC) of OASIS (Organization for the Advancement of Structured Information Standards). The versions of SAML used till now are SAML 1.0, SAML 1.1 and SAML 2.0.

In this paper we have discussed about web services in section 2. In section 3 we have studied about the SAML concepts. In the following section 4 we have detailed about the newest version SAML 2.0 and its components such as assertion, protocols, binding. In section 5 we have discussed the advantages of SAML. In section 6 and 7 we have conclusion and future enhancements. Finally in section 8 we have references.

2. Web Services

Web services are usually identified by Uniform Resource Locator (URL). Web services are a connection of two or more electronic devices in a network to transfer messages between them. Web services connection is made through World Wide Web. A remote computer using any platform can communicate the server with different platform using web service. Web service makes the user access platform independent. Web service has the capacity to convert any existing applications into web applications. Web services are XML based system that exchange information using the internet. The open standards on which web services are built on are TCP/IP, HTTP, Java, HTML and XML. The components used in web services are:

1. SOAP (Simple Object Access Protocol)
2. UDDI
3. WSDL (Web Services Description Language)

The user can communicate different sources in different platforms. Web services are not specific for any one programming language or operating system. Web services communicate with different platform within less time since all data are in XML. XML is used in web services for tagging the data and SOAP is used for the exchange or transmits of data. UDDI (Universal Description, Discovery and Integration) describes the services and stores the services. WSDL shows the list of services stored or available.
3. SAML Concepts

Security Assertion Markup Language is short known as SAML. It is based on XML and used to exchange security information between client and server. It is very flexible and extensible protocol. SAML exchange is done between the security domains. SAML used for web services security, single log-out and account linking. It unites entity’s identity to facilitate single sign-on. It mainly uses attribute based authorization. The major roles of SAML are:

1. Identity Provider/Asserting Party.
2. Service provider/Relying Party
3. User

Asserting Party is the system entity which gives authentication to the service provider about the user i.e. it sends SAML assertions to the relying party. It creates, maintains, manages and exchanges user identity. Juniper software is a best example for Identity provider; it gets the user name and password. Relying Party is the system entity which provides services for the users. It receives SAML assertion and gets the user identity and makes user access the service. SAML assertion is the token created by the asserting party based on the request made by relying party. SAML makes dynamic integration possible in today’s business environments.

3.1 SAML Work Flow

SAML is said to be a very normal framework since it is widely used. It is a main protocol which discusses fully about how single-on users work. SAML creates trust relationship between identity providers and service providers. SAML work flow starts from when the user requests the service from the Service provider. The service sends request to the Identity provider. The Identity provider request some information such as username, password or login id from the user. After receiving the details given by the user the Identity provider sends the response to the Service provider to allow the user to access the service. SAML does not specify any method of authentication to the Identity provider. SAML is one of the most secure methods or single sign-on.

4. SAML 2.0

The newest version of SAML is SAML 2.0. It is the major revision of SAML 1.1. It is used due to its intellectual property and protocols to secure web services and made accessible for all enterprise cloud applications. It provides stable and full featured federated identity security infrastructure. SAML 2.0 uses some existing standards which are given below:

1. XML (Extensible Markup Language)
   • XML Schema
   • XML Signature
   • XML Encryption
2. HTTP (Hypertext Transfer Protocol)
3. SOAP (Simple Object Access Protocol).

4.1 SAML Protocol Components

The figure 3 shows the SAML Protocol components. The main components of SAML protocol are:

1. Assertions
   - Authentication Assertion
   - Attribute Assertion
   - Authorization Decision Assertion
2. Protocols
3. Binding
4. Profile

![Figure 3]

4.1.1 Assertions

Assertion is an XML data format. It is used to authenticate and authorize the users. It gives all security information about the users and also special security information such as contact no., address etc.

Example of authentication assertion

```xml
<saml: Assertion
   AssertionID="128.9.167.32.12345678"
   Issuer="IRCTC"
   <saml: AuthenticationStatement
      AuthenticationMethod="password">
      <Saml: Subject>
         <saml: NameIdentifier
            SecurityDomain="IRCTC.com"
            Name="venkat" />
      </Saml: Subject>
   </saml: AuthenticationStatement>
</saml: Assertion>
```

Example authorization decision assertion

```xml
<saml: AuthorizationStatement
   Decision="Permit"
   Resource="http://irctc-hotels/welcome.htm">
   <Saml: Subject>
      <saml: NameIdentifier
         SecurityDomain="IRCTC"
         Name="venkat" />
   </Saml: Subject>
</saml: AuthorizationStatement>
</saml: Assertion>
```

User is at: http://irctc.com
Clicks on a link it takes her to http://indian-hotels.com
It really takes her to inter-site transfer URL: https://source.com/intersite?dest=indian-hotels.com
The best example for inter-sire transfer this is LDAP, LDAP is a software tool which is storing user name password and URL. If user name and password match with existing user id then only we can able to move to the destination page.

4.1.2 Protocols

Protocol means it is an approved format of data to exchange/transmit data between two parties i.e. Asserting party and Relying party. In SAML we are sending data after the verification of the user identity. Protocols show or give detailed format of how to get the security details of the user. Protocols mainly use request and response protocols. The user after registering the identity request protocol is send to the identity provider and it sends response protocol if the user identity matches with the data received.
4.1.3 Binding

Binding is the process of associating the object with some identifiers. SAML Binding is the process of mapping SAML protocols onto the standard messaging format. SAML 1.1 specifies only one binding. It specifies SAML SOAP binding. But SAML 2.0 specifies the following bindings:

1. SAML SOAP Binding (similar as in SAML 1.1)
2. Reverse SOAP (PAOS) Binding
3. HTTP Redirect (GET) Binding
4. HTTP Post Binding
5. HTTP Artifact Binding
6. SAML URI Binding

4.1.4 Profiles

The SAML 2.0 is listed with the following profiles

1. SSO Profiles
   - Web Browser SSO Profile
   - Enhanced Client or Proxy (ECP) Profile
   - Identity Provider Discovery Profile
   - Single Logout Profile
   - Name Identifier Management Profile
2. Artifact Resolution Profile
3. Assertion Query/Request Profile
4. Name Identifier Mapping Profile
5. SAML Attribute Profiles
   - Basic Attribute Profile
   - X.500/LDAP Attribute Profile
   - UUID Attribute Profile
   - DCE PAC Attribute Profile
   - XACML Attribute Profile

SAML 1.1 uses only one profile for single sign-on. Even though SAML 2.0 lists all these profiles the most primary case used is Web Browser SSO as in SAML 1.1. The figure shows the SAML 2.0 use case Web Browser SSO. Here Asserting party is indicated as source site. Relying party is indicated as destination site. Browser is the user.

5. Advantages of SAML

The advantages of SAML are:

1. Portable trust i.e. User authentication occurs inside the firewall so multiple application passwords are not required.
2. Cross Domain Single Sign-on.
3. Authentication of data i.e. It properly manages the identity to the Identity provider.
4. SAML is independent of any particular security or user database format i.e. it is neutral to all platforms.
5. Reduced administrative cost for service providers.
6. Improved online service for end users.
7. There is no need to synchronise or maintain user information between directories.

6. Conclusion

This study deals about the web services and its security management using SAML tokens. It gives details about the newest version of SAML and its components and deals with its advantages.

7. Future Enhancements

In future environment we shall concentrate on improving the web security using the advanced concept of SAML and implementing the web browser single sign-on.
8. References