Design of Web Service Single Sign-on Based on Ticket and Assertion

Yebin Chen
Internet of Things Technology Institute/School of Software
Nanchang Hangkong University
Nanchang,China
chenhb46@163.com

Baozhu Wu
Department of Information Engineering
Gongqing College of Nanchang University
Jiujiang,China
bblstone@126.com

Bing Xia
Human Resources Department
Nanchang Hangkong University
Nanchang,China
sunnyxb@gmail.com

Lianghong Shi
Department of Science and Technology
Nanchang National High-tech Industrial Development Zone
Nanchang,China
stonelbb@sina.com

***Abstract*—The system that integrating the information systems by using web services should provide a unified identity authentication single sign-on scheme for heterogeneous platforms. This paper introduces the characteristics of Kerberos based single sign-on and SAML based single sign-on. A single sign-on scheme which combines the advantages of the two schemes is designed based on analyzing the advantages and disadvantages of the two schemes. The architecture and the designing approach are also presented. And an application is introduced to analysis the operating process of implementing the scheme. Finally, the security is analyzed.**

Keywords Ticket; Assertion; Single Sign-On; Web Service

I. INTRODUCTION

With the increasing popularization of e-commerce, e-government and information systems, the application of single system can't meet the requirements of government and enterprise customers. They are yearning for a kind of method that can resolve multi-system integration development and access system resources in the form of share. Web services can integrate different applications and resolve the issue that integrating multi-system due to it has the advantages of loosely-coupled, language-independent, platform-independent, and cross-region. However, the frequently login and verify is needed when the user access the systems which adopts their own user management and authentication measures. So, it has the disadvantages of inconvenient to the user, large system resource consumption, and low executive efficiency. A kind of scheme is urgently needed to solve the problem. SSO (Single Sign-On) is a kind of secure technology to access the network. The essence of SSO is that the user can access a group of applications related to the entry point the user has signed on [1].

There are many kinds of SSO model at present, such as .Net Passport and Liberty Alliance. A centralized method is adopted to process the cross-region issue in SSO by .Net Passport. The site the user wants to access must support the Passport. Once the user access the site, the login server is redirected first. However, the technology that web service supported Passport single point authentication is not mature. The Liberty Alliance formulates a Specification and advocates an authentication mechanism that includes multiple kinds of identity authentication to meet the requirement of security in different systems. It supports non-centralized authentication and interoperation, and so can overcome the defect that the authentication can be done only after the user communicates with the service center. However, it also exits some defects, for example, it needs full trust between entities, centralizes an IDP (Identity Provider) certification. Even so, it is a better implementation scheme of SSO compared with .Net Passport. There also exist some more matured models, such as Kerberos, and SAML 2.0 which is approved by OASIS to solve the problem of SSO design.

This paper designs a novel SSO scheme based on identity federation. The sign on, access, authority checking, and authority control can be accomplished by adopting the ticket based centralized structure of Kerberos, on the basis of assertion statement verification of SAML, and combining the underlying token tracking forms.

II. RELATED WORKS

A. Traditional SSO

The procedures of user identity authentication in traditional systems are usually as follows: firstly, the user input the user information. Then, the system verifies it. If it is correct, the information is saved by Cookie. And the user information is verified through Cookie when the user login another system. However, this kind SSO must assure that the user information is identical in different systems. So, it leads the waste of system resource. Furthermore, there exists a big security trouble due to

978-1-4577-0536-6/11/$26.00 ©2011 IEEE

the illegal user can access the system illegally through false URL which can be obtained by reading Cookie easily.

B. Kerberos-based SSO

Kerberos is a key exchange standard defined by IETF (Internet Engineering Task Force). The SSO in Kerberos is implemented via key distributed center (KDC) distributing the ticket and authenticating the user uniformly. Its core is ticket [2], and the work principle (shown in Fig.1) is that it sends a request includes user information to KDC if the user signs up initially. The Ticket-granting Ticket (TGT) is returned to the user once KDC receives the request. Then, the user request the service ticket (ST) from KDC by submitting TGT. Finally, the user obtains the corresponding services by submitting the ST to the application server.

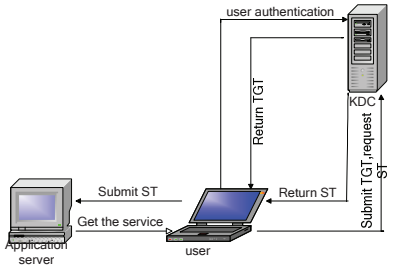

Figure 1. Work principle of Kerberos

C. SAML-based SSO

OASIS (Organization for the Advancement of Structured Information Standards) approves the development of SAML (Security Assertion Markup Language) which is an XML based language. SAML is a protocol and platform independent mechanism (also defined as SSO) for controlling access to the resources for authenticated principals [3]. Assertion is the core of SAML. It provides three kinds of information, there are authentication, attribute, and authorization decision-making.

The SP (services provider) firstly takes responsible for identity authentication when the user access the services which are provided by the SP via browser. The IDP and SP exchange the information once the user request the SSO service. Then, IDP creates SAML statement of the user and sends it to the SP. The SP verifies the validation of SAML to implement the function of SSO and logout [4].

D. SSO Combined Kerberos with SAML

Centralized user identity authentication management and the function of information bidirectional authentication are adopted by the Kerberos based SSO model. It not only reduces the burden of system maintenance, but also improves the security greatly. However, the transfer of ticket information, the encryption and decryption of the ticket are very complex. Furthermore, the user information will be leaked easily if it is transferred between the low version browser and web server.

SAML is an XML based language, it has the characteristics of cross-platform, cross-language, heterogeneous systems, so the information can be transferred easily. The user information is authenticated by transferring the Artifact in the form of assertion statement in SAML based SSO model. The security can be guaranteed due to the Artifact is disposable. However, it is easily attacked by unauthorized users due to lack of mutual authentication.

The SSO scheme designed by combining Kerberos and SAML can get better performance. It combines the advantages of each model. The advantages of the scheme are: bidirectional authentication of the ticket in Kerberos can improve the security of SAML based SSO. The SAML provides media for the ticket transfer. Furthermore, the potential information leakage can be avoided by assertion statement in SAML.

III. THE DESIGN OF WEB SERVICE SSO BASED ON TICKET AND ASSERTION

A. Architecture

The web service SSO based on ticket and assertion mainly includes three modules: user login, ticket authentication, and assertion management. The user login module takes responsible for one-time authentication; it mainly includes the transmission of the user information. The bidirectional authentication which can assure security and real-time is implemented by combining the idea of Kerberos protocol in ticket authentication module. The assertion management module manages the authentication by using a series of decision language based on the main idea of SAML to guarantee the valid user access the service in security. Fig. 2 shows the architecture of ticket and assertion based SSO.

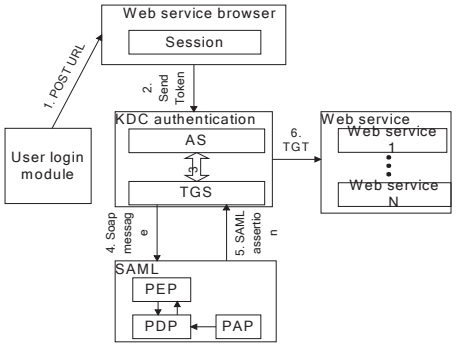

Figure 2. The architecture of ticket and assertion based SSO

The login process can be described as follows:

(1) The user information is sent to web service browser in the form of URL through POST method by user login module

(2) Web service browser records the login session and sends user information to KDC authentication center by means of Token.

(3) AS (Authentication Service) process the user request when the information is sent to KDC authentication center to determine whether the user is legal. The result is returned to TGS ticket. And the ticket submits the corresponding TGT to SAML center in the form of SOAP (Simple Object Access Protocol) message.

(4) The received ticket information is decided whether illegal or not by PEP (Policy Enforcement Point), PDP (Policy Decision Point), and PAP (Policy Access Point). Then SAML assertion is returned to the ticket.

(5) Whether the submitted TGT is valid or not is determined after the TGS has received the SAML assertion. The corresponding server ticket is returned if it is valid.

(6) The user login the web services according to the legal ticket, and take various application operations.

B. The Design of the Scheme

The ticket and assertion based web service SSO mainly includes four major functional designs. There are: login module based on Ajax, Token, the mutual authentication of the ticket, and SAML assertion. Login module is designed by using Ajax (Asynchronous JavaScript and XML), and it makes interactive web operation more convenient. The ticket can be encapsulated well due to the model is implemented by using an object-oriented language—Java. In web service, the ticket protocol is described by using WSDL (Web Services Description Language), and the ticket is sent by embedding into the SOAP protocol in order to achieve the goal of mutual authentication and to get better security.

1) Login module implemented by Ajax

Web development implemented by using Ajax is an important technology. Ajax uses XHTML and CSS, uses DOM to implement dynamic display and interaction, uses XML and XSTL to exchange and process the data, uses XMLHttpRequest to access asynchronous data, and uses Javascript to bind and process all the data [5]. And the page can be locally refreshed well. It will turn to the corresponding web service page after the verification of identity information. The key code of designing login by Ajax is described as follows.

```
Var url = "login.action"; / / definition of jump address
xmlHttpReq. open ("GET", url, true);
xmlHttpReq.onreadystatechang function(){};//implement jump
xmlHttpReq.send (NULL);
```

The user information is transferred to the server for verifying through Ajax engine. And it is stored by session.

2) Session

Session is a storage space maintained by application server. In this paper, session is implemented by using a class named Token. Whether the user has the right to login is determined according to the identification information stored by Token when the user accesses the service. The Token class contains the following methods: token.account, token.function, token.opernumber, and MD5.account, etc. token.account maintains some identification information which is stored when the user login. Token.function is used for indicating whether the user has the privilege to use the function. It is used by combining a default number which is generated by the system. Token.opernumber presents an operation number the user have privilege to access. MD5.account is used for encrypting the identity information to avoid leakage.

Session is taken as a server mechanism, it uses a structure that similar to harsh table to storage information makes the user identification storage more helpful. Furthermore, it encrypts the user information, the method, and the number makes the information protection more convenient.

3) Mutual Authentication of the ticket and the design of SAML assertion

In Kerberos, a secure bridge is being built between the client and the server by providing central authentication service and encrypting the method via traditional symmetric key algorithm [6]. The core of SAML is assertion. Assertion is a statement without needing proof, it can provide a series of decision schemes to authenticate the information [7]. In practical, SAML can generate and release three kinds of security assertion: authentication assertion, attribute assertion, and authorization decision assertion. The ticket in Kerberos operated bidirectional by adopting assertion is effective.

The ticket and assertion based web service SSO mainly includes three phases: the exchange of authentication service, authentication service, and application service. Each phase can be divided into request and response. The relations of the request and response in three phases are shown in figure 3.

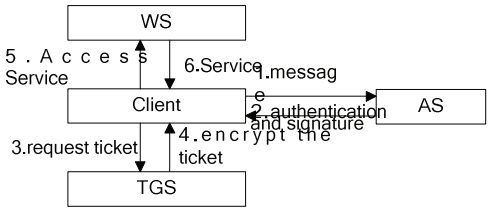

Figure 3. mutual authentication the ticket and model of the SAML assertion

There are mainly six steps in figure 3. There are:

Step 1. C→AS: The client sends a message which includes user information to the server. The message is encrypted by dynamic password in the server.

Step 2. AS→C: The message is decrypted by using private key in authentication service center. Then the authentication service center authenticates the information by querying the information from the database. The AS signature is sent to the client only when the authentication is succeed.

Step 3. C→TGS: The signature verification is encrypted and sent to the ticket granting service (TGS) for requesting the ticket when the client gets the signature.

Step 4. TGS→C: The message is decrypted according to the acquired public key when it is received. The ticket with TGS signature is sent to the client if the verification is valid.

Step 5. C→WS: The signature ticket received from TGS and the attribution information of local host such as computer name, address, and request time is sent to the web server.

Step 6. WS→C: Web server verifies whether the received signature ticket is valid. If it is, the identity information is stored so that the user can access the required web services.

The main function of SAML is reflected in step 4 and step 5 during mutual authentication of the ticket. It is helpful to avoid the information leakage and malicious attacks owing to the user identification information is transferred via browser in the form of disposable ticket. The SAML assertion and the ticket which is taken as a request object of SAML are sent to the AS during authentication. Then the user information which

is stored in the form of assertion is sent to PDP and PEP by AS for decision control.

The design of the ticket in SAML mainly includes three parts: the creation of assertion, the creation of the ticket, and the transmission and reception of the ticket value. Java as an object-oriented language can solve the problem of assertion and ticket initialization well. The ticket information can be described by WSDL in web service, and can be transferred by embedding into SOAP file. The key code of designing the three parts is shown as follows:

(1) the creation of assertion:

```
public class assertion extends Assertion { // encapsulation the
                                          //assertion to a class
CreatAssertion (note method) // the creation of assertion
... ...}
```

(2) the creation of the ticket:

```
public class ticket extends Ticket {
String ticketKey;
public void sendTicket (as parameters) // the transmission of the ticket
public void receiveTicket () //information of the received //ticket
... ...}
```

(3) the assertion of the ticket in SAML

Message definition in WSDL:

```
<message:name="ticketKey">
<part name="account" type="reg:ArrayAccount"/> //user account
<part name="opernumber" type="xsd:string"/> //user operation
                                            //number
<part name="requesttime" type="xsd:timeInstant"> //request time
... ...</ Message>
```

Assertion identifier in SAML:

```
<samlp:Request><samlp:AssertionTicket>encrypted digital </ samlp:
AssertionTicket></samlp:Request>//encrypt message and send it
... ...
```

The summary design code of the web services SSO is shown above. It mainly includes the assertion and ticket initialization, a ticket message definition in SAML, and the encryption of the assertion ticker during transmission.

C. Application Analysis

The SSO designed in this paper is applied in an integrated system of broadcasting and television. The system includes the integrated resource of three heterogeneous systems, there are digital television system, broadband system, and call center system. The services of each system can be accessed mutually to guarantee data synchronization. Charge service in broadband system and the expenditure service in digital television system should be used by expenditure statistical analysis service in call center system. The function that access the data of analyzing charge report forms in call center system must be used by charge service in broadband system and the digital television expenditure service in digital television system. So, SSO is needed. Using ticket and assertion based SSO to login the heterogeneous systems can avoid the complexity of login multiple times and guarantee the security of the information. The concrete operating process in the system includes login, request the Token, the mutual authentication of the ticket, SAML decision, access the web services.

IV. EVLATION

During web services SSO process, confidentiality, data integrity, non-repudiation, and availability are the attributes of security properties [8]. This paper analyzes the security of the designed SSO mainly from the following aspects: confidentiality, data integrity, and non-repudiation.

Confidentiality means the message that the user is sending will not be intercepted. The SSO designed in this paper adopts post to transmit the information which is encrypted by MD5 can guarantee the confidentiality. The XML-based SAML is used to transfer the ticket. And XML has the characteristic of scalability, so the encryption technology can be introduced to encrypt the important information.

Data integrity represents the data will not lose easily during transmission, and will not revise or delete by some unsafe factor. The ticket is asserted by using SAML, the information can be encapsulated during request or response, and digital signature is used for avoiding the information to be modified malicious guarantee the data integrity. Furthermore, the ticket is authenticated mutually ensures non-repudiation.

V. CONCLUSION

The design idea of SSO is that only login once can access multiple web application relate to the entry point that the user has signed on. Ticket and assertion based SSO combines the advantage of Kerberos and SAML ensures the authentication more validation by adopting mutual authentication. During authentication, SAML can provide standard mechanism for authentication and authorization, and it provides security and interoperability for information transmission and authentication.

REFERENCES

[1] Manshan Lin, Heqing Guo, “Present Situation and Development of single sign-on technology,” Journal of Computer Applications, 2001, Vol 24, No.6,pp.248-250

[2] Jason G. Kerberos. The Definitive Guide[M]. Sebastopol: O'Reilly Media, 2003.

[3] XML Security: Ensure portable trust with SAML, http://www.ibm.com/developerworks/library/x-seclay4/index.html?S_TACT-105AGX52 &S_CMP=cn-a-x/, 2009.

[4] Wang Xiuyi, Wang Lingyan,Han Jihong and Chen Qingrong,. “Security Research on a SAML-based Single Sign-on implement mode,” .Microcomputer Information, 2007, Vol 23, No.8-3, pp.81-83

[5] Ryan Asleson, Nathaniel T. Schutta, Foundations of Ajax. Beijing: Posts & Telecom press, 2006

[6] Tiehua Wen, Shiwen Gu, “An improved method of enhancing Kerberos protocol security,” Journal of China Institute of Communications, 2004,Vol 25, No.6, pp.76-79

[7] Suriadi,Ernest Foo,Audun Josang, “A user-centric federated single sign-on system,” Journal of Network and Computer Applications, 2009,Vol 32, No.2, pp.388-401

[8] Hengda Ma, Pengfei Li, Xuexiong Yan, “The security of web services[M]”. Beijing: Publishing House of Electronics Industry, 2007