Research and Implementation of Single Sign-On Mechanism for ASP Pattern*

Bo Li, Sheng Ge, Tian-yu Wo, and Dian-fu Ma

Computer Institute, BeiHang University, P.O Box 9-32 Beijing 100083

Abstract. Software Services based Application Service Provider pattern is an important method in constructing enterprise applications, which integrate business systems with different authentication mechanism. So there are questions such as repeated authentication and authorization, difficulties in authorization management, difficult to describe security information interoperability. This paper proposes a method, which stores information in a uniform format, accesses it in a standard interface and exploits account federation, authentication proxy, and authorization proxy to transfer authentication and authorization results. As a result, we design and implement a single sign-on system by this method.

Keywords: ASP, Single Sign-on, LDAP, SAML

1 Introduction

Under the Internet environment, ASP platform and service is becoming the trend of E-business. Portal-based ASP platform can provide or integrate various information systems, such as OA, Email Systems, and cooperative platforms and so on. Not only does the ASP provide a standard interface for User, but provide a standard connection point for application providers.

Application always has its own authentication and authorization mechanism Heterogeneity of which result in problems [1]. ①users must remember independent accounts and login repeatedly. ②User information and security policy are unrelated, which makes the user management complicated and unsafe. ③Because of heterogeneous security mechanism, it is impossible to transmit authentication results to finish a cooperative job. Thus, to integrate the user information and security policy standardize authorization process and set up SSO system among applications becomes the key in ASP development.

So far, much SSO-related work has been done. Such as MS .Net Passport [2] and Liberty [3], but they can't meet new requirement of authorization management and sharing security information

This paper proposed a SSO solution base on LDAP [5] and SAML [6]. LDAP stores and manages user information and security. SAML descript and transmit the authentication results in a standard way.

* This paper is supported by China Education and Research Grid (China Grid) and the National High Technology Development Program of China under Grant No.(2001AA113030, 2002AA116050 and 2003AA115420).

H. Jin, Y. Pan, N. Xiao, and J. Sun (Eds.): GCC 2004, LNCS 3251, pp. 161–166, 2004.

2 Single Sign-On Technology

2.1 Traditional SSO Techniques

SSO technology provides a convenient way to access applications in distributed environment. The MS .Net Passport use Cookie and redirection to implement central authentication and distributed authorization. But it lack of standard protocol to exchange authentication. Liberty 1.0 establishes the authentication chain and theoretically can extend allied sites infinitely. Because it supports SAML, it brings good interoperability. But complicated architecture and authentication chain management are the shortcoming. So it's hard to solve the SSO problem in ASP with traditional SSO technique.

2.2 LDAP Directory

LDAP is Lightweight Directory Access Protocol. Directory organizes user and applications information within distributed LDAP defines standard methods to access directory; new schema can be costumed according to requirement; distributing: directory information tree (DIT) can be divided into child trees to represent management domains.

In ASP environment, Dynamic changes of applications result in security information management complexity. With above characteristics, LDAP can simplify security information integration and management.

2.3 SAML

SAML 1.0 (Security Assertion Mark Language) was mainly designed to share security information for authentication and authorization services. SAML is based on XML, so it is a good choice for ASP environment to descript and share the authentication and authorization results among many heterogeneous security systems.

3 Design Principle of SSO System

3.1 Conceptual Model

Based on LDAP and SAML, this paper proposes a SSO mechanism for the ASP service model (figure 1). LDAP integrate security information within a security domain and ensures unified storage, access, central authentication and authorization; SAML can share security information among heterogeneous applications among ASPs. Definitions in this ASP-Oriented SSO mechanism are as follows:

Definition 1: An ASP application platform is depicted by a set containing five items $\{DS, LS, P_{AE}, P_{AO,} P\}$.

DS means domain security server, responsible for the central authentication and authorization.

LS means LDAP server, centrally store the user information and security policy within an ASP platform.

P_{AE} means the authentication proxy, which authenticates the user's identity to the legacy applications on the behalf of the user.

P_{AO} means the authorization proxy, which controls the users' access and sends the authorization information to the new developed applications.

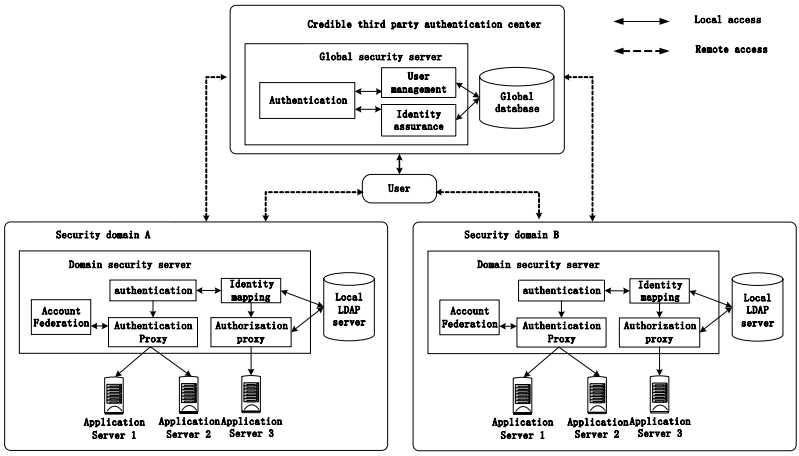

Fig. 1. ASP oriented single sign-on mechanism.

P represents the application systems deployed in an ASP, P_L refers to the legacy systems and P_N refers to the new developed application.

Definition 2: (Identity Assurance), illustrated as the figure 2, if A and B are two security domains in the distributed environment then the Identity Assurance is: if U has been authenticated in domain A, when U wants to access B, A can assure U's identity to B on behalf of U. This procedure makes it possible to share the user's identity among domains. The identity assurance is the core SSO mechanism.

Definition 3: (Identity Mapping), if A is a security domain and U is a global user, then the Identity mapping refers to the procedure of mapping the global identity to local identity of certain domains.

Definition 4: (Account Federation), user federate their identity in the ASP platform with their identities in each applications within the ASP platform, then store them for transmit automatically.

Definition 5: (Authentication Proxy), after user has logged on ASP platforms, if he want to access legacy applications, the account will be transmitted by the account federation information automatically.

Definition 6: (Authorization Proxy), when deployed applications to the ASPs, the manager will customize access control policy. If the user has been authenticated by the ASP, then Authorization Proxy will create and send authorization assertion automatically to the execute module to parse the authorization result.

3.2 SSO Mechanism Within ASP

There are two types of applications in a security domain, legacy system and newly developed applications In this SSO system, we establish account-federation relationship for every legacy systems and send the authentication information automatically. As to newly deployed application, a common authentication module provided by the SSO system will do the job on the behalf of users. The Web application A represents

an legacy application P_L, the Web application B represents a newly developed application P_N, then the single sign on in within ASP domain is as below:

1. User logged on the ASP platform and provided DS_A the account-federation information.
2. DS_A authenticated the user and stored the account- federation information in LS_A. Then this user attained a single identity and a federation – relationship.
3. The administrator of P_N customized the authorization policy, including roles and permissions; the administrator of DS_A assigns the role to the user, so the user have the corresponding permissions.
4. When User U wanted to access P_L, the authentication module of P_L requested the acount information of U, according to the established account-federation, and DSA returned the account to P_N.
5. The authentication module of P_L authenticated the user's identity.
6. When the user wanted to access P_N, according to the established security policy, DS_A constructed an authorization assertion by SAML and returned it to P_N.
7. P_N executed the SAML authorization assertion.

Through this mechanism, ASP platform cannot only support account-federation and storage for the legacy systems, but can customize access control policy for the newly developed systems. Thus, we can achieve central authentication and access control.

3.3 SSO Mechanism Among ASP Platforms

Within the enterprise alliance, to finish a transaction users need to access many applications distributed in many enterprises. The key problem is sharing and transferring the authentication and authorization results among ASPs. For example, ASP_A and ASP_B represent two independent security domains. After they release and exchange their own trust policy, a new credible relationship is established.

1. Users access ASP_A, which redirect user to authentication center (AC) to log on globally.
2. Users log on AC, AC create Http Session, SAML authentication assertion and ticket based on the authentication result (reference to the assertion) for the user.
3. AC redirect the user to ASP_A with the ticket issued by AC, which prevents repeated attack.
4. ASP_A request integrated SAML authentication assertion by ticket, AC return the assertion to the authentication module of the ASP_A.
5. Authentication module of ASP_A authenticate the identity of the user according to the SAML authentication assertion issued by AC.
6. User access ASP_B, ASP_B redirect user to AC.
7. Make use of the Http session, AC create the SAML assertion and ticket for the user, then redirect the user to the ASP_B with the ticket issued by AC.
8. ASP_B request integrated SAML authentiation assertion from AC, then AC return the assertion to the authentication module of the ASP_B.

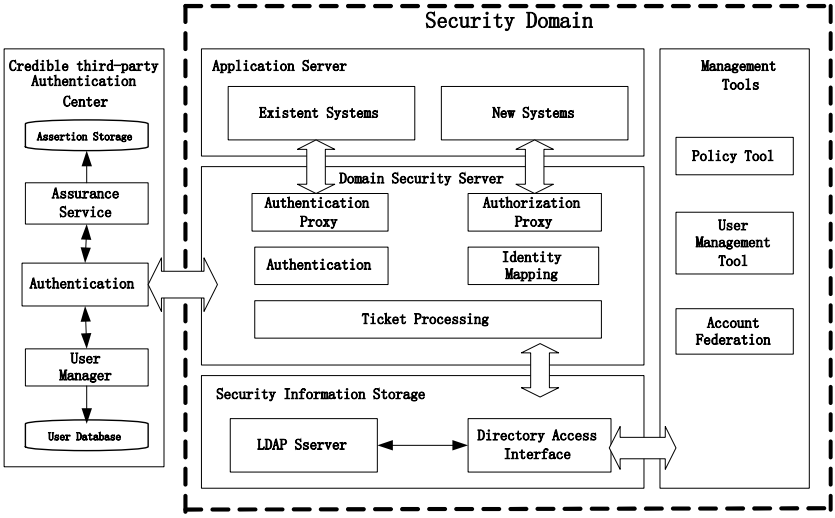

Fig. 2. Architecture of the single sign-on system for ASP pattern.

9. Authentication module of ASP_B authenticate the identity of the user according to the SAML assertion, thus the user only log on once to the AC,then he can access ASP_A and ASP_B seperately.

In above mechanism, credible third-party authentication center send authentication and authorization result by assertion and ticket to guarantee user's identity to other platforms.

4 Implementation of Single Sign-On System

In this paper, we implement a single sign-on system for ASP Pattern, (Abbreviation is ASPSSO), According to the design target, this paper design four core parts to construct the system: security information storage, domain security server credible, third-party authentication center and configuration tools, the architecture is showed as figure 2:

1. Security information storage: Introduce LDAP to centrally store user's accounts and security policy in a domain. LDAP access interface, capsulate the API to access LDAP.
2. Domain security server: Authenticate the users and map the global identity to the local identity, create the account federation for users, automatically transmit the account to the legacy application, send the authorization assertion to the new deployed application.
3. Credible third-party authentication center: Authenticate the global user, create and manage SAML authentication assertion, issue ticket relative to the assertion, respond to request of assertion.
4. Configuration tools: Customize account federation information, access control policy, and the identity mapping policy of the users.

5 Security Analysis

When user access through the single sign-on system, the system may be exposed to security attacks, the security guarantee is important. This paper analyzes security r characteristic, which can avoid several kinds of security attack:

1. Wiretap attack Code: and decode to the SAML assertion, which can make the result of authentication and authorization confidential and integrate.
2. Playback attack: Set the period of the validity of assertion, decrease the valid time of attacker, and make the assertion invalid after has been accessed once.
3. Attack of tamper message: Because we use SOAP to transmit SAML result, we extend SOAP by WS-Security standardization, in this way the SOAP message can include the signature element to guarantee the integrity of message.
4. Disguise attack: We extend SOAP message with the authentication element to prove message sender's identity, which prevents the attacker to disguise as a legal site.
5. Hostile corporation site attack: By setting the effect region of SAML assertion to prevent the hostile use of the ticket.

6 Conclusion

In order to meet the new security requirement of E-Business, this paper propose a kind of Single Sign-on means for ASP Pattern. The characteristics are as follows: ①though LDAP, the system can centrally manage the user information and security policy in a standard interface. ②though SAML, the system has standard description and transmission of authentication and authorization result. ③unified authentication and authorization, simplified complexity of authorization management: ④By Web Service, implement a reliable third party authentication center, which is interoperable and portable. ⑤the system has good security and

Problems such as reliability and performance in large-scale concurrent access should be taken into account.

References

1. Build and implement a single sign-on solution [J]. Sep.30th 2003. http://www-106. Ibm.com/developerworks/java/library/wa-singlesign/? Ca=dgr-lnxw914CASsso
2. Microsoft Corporation. Microsoft .NET Passport Technical Overview.2001 [J].
3. Jeff Hodges, Sun Microsystems, Inc. Liberty ID-FF Architecture Overview [S]. 14 April 2003.www.projectliberty.org/specs/ draft-lib-arch-overview-v1.2-04.pdf.
4. Network Working Group. Lightweight Directory Access Protocol (v3)[S]. 1997. RFC2251.http://www.ietf.org/rfc/rfc2251.txt? number=2251
5. Hallam-Baker P, Maler E.Assertions and Protocol for the OASIS Security Assertion Markup Language [S]. 2002,5. http://www.oasis-open.org/committees/ security/docs/Cs-sstc-cor e-01.pdf