Journal of Southeast University (English Edition) Vol. 23, No. 3, pp. 465 – 468 Sept. 2007 ISSN 1003—7985

Scalable single sign-on system

Huang He[1] Shan Zhiguang[2] Huang Dongquan[3]

([1]College of Software, Beihang University, Beijing 100083, China)

([2]Department of Informatization Research, State Information Center, Beijing 100045, China)

([3]Department of Foundation Courses, Xuzhou Air Force Academy, Xuzhou 221000, China)

Abstract: To address the scalability and identity federation problems of the traditional single sign-on system, the proposed scheme divides the security systems into different security domains. Each security domain has its own security servers and service providers, and there are trust relationships between different security domains for identity federation. The security server is responsible for authentication and authorization inside the domain, and offers identity federation capability for different domains. The security assertion markup language (SAML) assertion is used as security token in the system for authentication, authorization, and identity federation. The design of the proposed single sign-on process is based on web service security framework and multiple security domains, and the authorization is always deployed in the local area inside the service provider's security domain, which enables web service clients, both inside and outside their security domains, to access the services in a simple, scalable, standard and secure way.

Key words: security systems; architecture; web service; single sign-on; identity federation

Single sign-on service enables a user of a distributed system who may potentially use a variety of different application services spread over different end-systems needs to sign on, i. e. authenticate himself, only once to the system as a whole, and the results of that authentication are automatically propagated to the end-system as required. This is very important to the future software architecture where web service, the service-oriented architecture (SOA) and grid provide the infrastructure for the users and service providers.

The existing single sign-on systems[1–3] are based on the idea that a central server, such as Microsoft passport. com, Liberty identity server, is used to offer the identity authentication for the users. This may cause the scalability problem when users and services in the system increase. In addition, some of the existing single sign-on systems are quite complicated. Many redirection operations are needed between clients and servers thus it takes many steps for a client to complete the single sign-on process.

A scalable single sign-on system for web services is proposed in this paper. Unlike Liberty[3] and other existing single sign-on systems, the proposed scheme divides the system into different zones, which are called security domains in this paper. There are three entities in each security domain: web service client, security server and web service provider.

1 Architecture of the Proposed System

Fig. 1 shows the architecture of our proposed single sign-on system. There are multiple security domains, and each domain has a security server for authentication, authorization and identity federation.

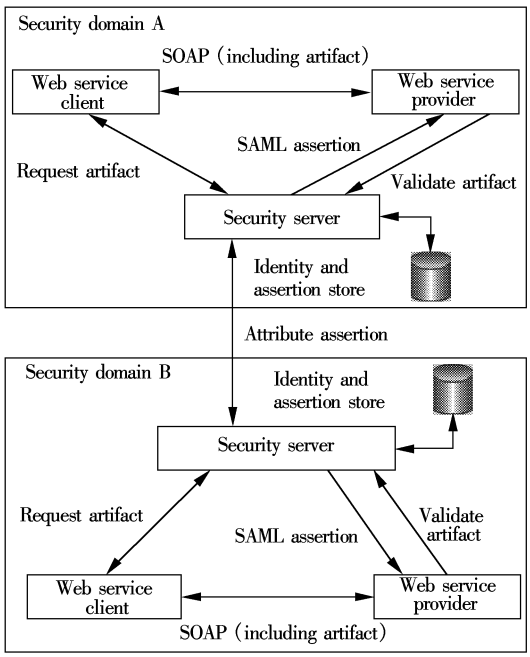

Fig. 1 Architecture of our proposed system

The SAML assertion is used as the shared, stand-

Received 2007-05-18.

Foundation item: The National Natural Science Foundation of China (No. 60673054).

Biography: Huang He (1970—), male, doctor, lecturer, huanghe@buaa. edu. cn.

ard security token for web service. The SAML assertion allows web service clients and web service providers in different security domains to securely communicate identity information that can be used for the purposes of authentication and authorization. In addition, the flexibility of the SAML assertion allows web services providers to support different authorization models while only having to handle a single security token format.

The authentication and authorization mechanisms work in a standard way defined by WS-trust specification[4], where a web service client interacts with the security server to request a security token for use in simple object access protocol (SOAP) messages. In addition, a web service provider interacts with a security server to validate security tokens that arrive in a SOAP message.

When a web service client intends to access the services inside its domain, it logs into the security server within the domain and obtains a security token (artifact in Fig. 1). Later, the client uses the token to access the web service, and when the web service provider obtains the token, it will send the token back to the security server to validate it. If the token turns out to be a valid one, the security server determines the authorization for the requested resources and then the client can access the service he wants.

If a user tries to access a service provider outside its domain, the security server communicates using SAML assertion with another security server in the corresponding security domain. Then the security server determines the authorization of the requested resource according to the trust relationship between the different domains and the SAML assertion (attribute assertion) from the domain in which the client is located, and the authentication process is also executed in the security server within the client's domain.

2 Design of Single Sign-on Process

2.1 Single sign-on inside security domain

There are four kinds of security tokens in our proposed single sign-on system: the authentication assertion, attribute assertion, authorization assertion and artifact.

As shown in Fig. 2, in the system, a web service client accesses the services within the clients' security domain by the following steps:

① Client logs into the security server within the clients' domain through authentication techniques such as ID/password.

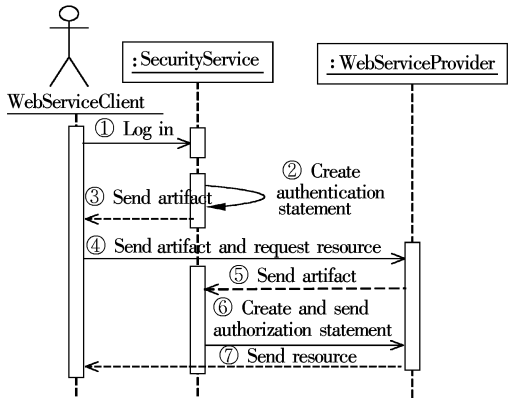

Fig. 2 Single sign-on process within domain

② Security server authenticates the client's identity and creates an authentication assertion and an artifact (a credential) for the client.

③ Security server sends the artifact to the web service client.

④ Web service client sends a SOAP message, which contains the client's artifact, to the service provider.

⑤ Web service provider creates a session to save the client's information and then sends the artifact back to the security server for authentication.

⑥ Security server resolves the artifact and uses it as an index to find out the corresponding authentication assertion of the client. In addition, the security server checks out the access control lists and decides the authorization assertion for the client according to its authentication assertion. Finally, the authorization assertion is sent to the service provider, which decides if the client has the right to access the corresponding resources.

⑦ Web service provider checks the authorization assertion and sends the resources to the client.

2.2 Single sign-on between security domains

When a client tries to access a web service which is located outside the clients' security domain, the following steps shown in Fig. 3 are needed.

① to ③ are the same as that described in 2.1.

④ The client requests service to the service provider in security domain B, and sends a SOAP message, which contains the client's artifact, to the service provider in domain B.

⑤ The web service provider in security domain B creates a session to save the client's information and then sends the artifact to the security server in domain B for authentication.

⑥ The security server in domain B resolves the client's artifact, and determines out that the client is

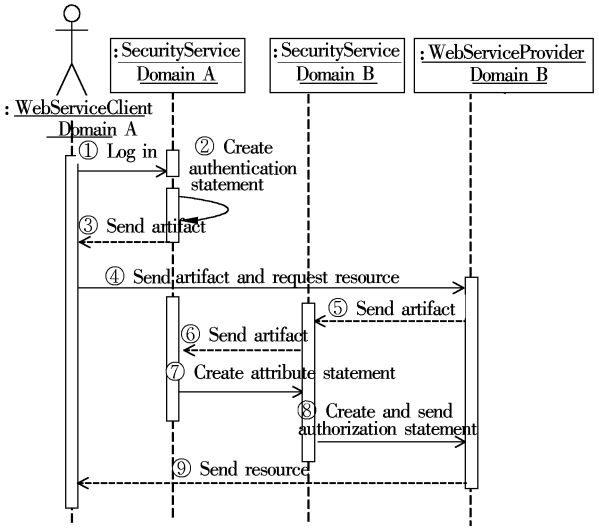

Fig. 3 Single sign-on process between domains

from domain A. Then it sends the artifact back to the security server in domain A.

⑦ The security server in domain A discovers the client's authentication assertion according to the artifact, and then creates the attribute assertion, which contains the necessary attribute information according to domain B's requirements. The attribute assertion is sent to the security server in domain B.

⑧ The security server in domain B checks the trust relationship between domains A and B, the attribute of the client, and the access control lists in domain B, and then creates the authorization attribute for the client. The authorization assertion is then sent to the service provider in security domain B.

⑨ The service provider in domain B sends the corresponding resources to the client in domain A, according to the authorization assertion.

2.3 Identity federation

The process of identity federation enables trust and allows the integration of identity information between different security domains. In the proposed single sign-on scheme, the attribute assertion is the security token for identity federation.

Authentication is required to verify the identity (conveyed as a security token) of the user in one security domain before creating a different security token that is trusted by the partner security domain. As mentioned earlier, in our proposed single sign-on system, authentication is always processed inside the client's domain. Trust establishment between different domains enables a security server to trust the users outside its security domain. In effect, trust between different domains is established through the exchange of security tokens. The X.509 based XML signature[5-6] is used to authenticate the security token between different security domains, and the trust establishment between different domains is implemented through the attribute asserting.

A user may have different identifiers and different roles in different security domains. Identity mapping facilitates the ability for a security token to contain the correct user identity information used in different security domains. This identity information can be retrieved either from the existing token itself or from a lightweight directory access protocol (LDAP) directory in our system. Identity information includes attribute values, and the information is used to personalize the user experience or to make authorization decisions within the service. User identity mapping is deployed according to the policy of the trust relationship between different security domains.

3 Conclusion

Single sign-on is one of the key technologies in web services and grid applications. The proposed single sign-on scheme divides the security system into different security domains, in which each domain has its own security server for authentication and authorization, and thus the system is scalable. The artifact and other three kinds of SAML assertions are used as security tokens in the system for authentication, authorization, auditing, and identity federation. The single sign-on process works in a standard way defined by web service security framework, and the identity federation is provided in a simple and secure way in the system, since the authorization is always deployed in the local area inside the service provider's security domain.

References

[1] Hallam-Braker P, Maler E. Assertions and protocol for the OASIS security assertion markup languages (SAML) [EB/OL]. (2002-04-19) [2007-05-08]. http://www.oasis-open.org/committees/security/docs.

[2] Erdos M, Cantor S. Shibboleth-architecture draft v05 [EB/OL]. (2002-05-02) [2007-05-08]. http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf.

[3] Pfitzmann B, Waidner M. Analysis of liberty single-sign-on with enabled clients[J]. *Internet Computing*, 2003, **7**(6): 38-44.

[4] Yu Xiulan, Chen Xiaoyan, Fang Xing et al. Web services security in data service delivery platform for telecom[C]// *Proceedings of the E-Commerce Technology for Dynamic E-Business*. Washington DC: IEEE Computer Society, 2004: 374-377.

[5] Jeong Jongil, Shin Dongkyoo, Shin Dongil. An XML-based automated authentication profile for home network based on OSGi framework[C]//*International Conference on Consumer Electronics*(*ICCE* '06), *Digest of Technical Papers*. IEEE Consumer Electronics Society, 2006: 99 - 100.

[6] Zhao Gang, Zheng Dong, Chen Kefei. Design of single sign-on[C]//*Proceedings of the E-Commerce Technology for Dynamic E-Business*. Washington, DC: IEEE Computer Society, 2004: 253 - 256.

一种可扩展的单点登录系统

黄 河[1] 单志广[2] 黄冬泉[3]

([1] 北京航空航天大学软件学院,北京 100083)
([2] 国家信息中心信息化研究部,北京 100045)
([3] 徐州空军学院基础部,徐州 221000)

摘要:为解决传统单点登录系统的可扩展性和身份联合问题,将系统划分为不同的安全域,每个安全域具有域内的安全验证服务器,并且不同的安全域之间具有信任关系以支持身份联合. 安全服务器负责域内用户的验证和授权,同时为不同域之间的用户提供身份联合. 系统使用 SAML 断言作为安全令牌以完成验证、授权和身份联合过程. 单点登录过程的设计基于 web 服务安全框架和多安全域,并且授权总是在服务提供者所在的域内实施,因此无论对于域内还是域外用户,系统提供了一种简单、可扩展、标准并且安全的访问 web 服务的方法.

关键词:安全系统;体系结构;web 服务;单点登录;身份联合

中图分类号:TP393