A Cross-IdP Single Sign-On Method in SAML-Based Architecture

Tzu-I Yang[1], Chorng-Shiuh Koong[2], and Chien-Chao Tseng[1]

[1] National Chiao Tung University, Department of Computer Science, Hsinchu, Taiwan
[2] National Taichung University of Education,
Department of Computer and Information Science, Taichung, Taiwan
{tiyang,cctseng}@cs.nctu.edu.tw, csko@mail.ntcu.edu.tw

Abstract. Security Assertion Markup Language, which is an XML-based framework, has been developed to describe and exchange authorization and authentication information between on-line business partners. One of the major applications is used to achieve single sign-on through different cloud services. SAML has provided the basic assertion of security that allows the user to surf hybrid clouds of the enterprise. The identify provider, which in charge of the management of the user information, can help users access these services effortlessly. However, the user anonymity of SSO from different identify providers is still an open issue even in SAML 2.0. In this study, we propose a SSO architecture for hybrid cloud to achieve identity federation cross-IdP using SAML, which provide the user an enterprise-crossed, services-integrated, backward compatible, and anonymity-maintained environment.

1 Introduction

With the rapidly growing of Internet techniques, cloud computing becomes the mainstream, which can provide all kinds of services. Because various services may come from different cloud servers, users may be asked to login again and again to provide valid credentials. In order to integrate differences and provide a mature and high quality environment, single sign-on (SSO) is introduced to solve this kind of problem. SSO is a property of access control with multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them.

SAML is an XML-based solution, which has developed, by the Security Services Technical Committee of the standards organization, the Organization for the Advancement of Structured Information Standards (OASIS), for exchanging user security information between enterprises and service providers. It supports W3C XML encryption and service provider initiated web single sign-on exchanges. It can be imagined that after logging in at Yahoo home page, the user could use its mailbox, auction, photo album services, without providing credentials again. However, users may have to login many times to use the services while the various services are subordinate under different IdPs. In addition, it is hard to convince these enterprises to share authentication schemes since it may cause the security anxiety. The commercial

James J. (Jong Hyuk) Park et al. (eds.), *Future Information Technology*,
Lecture Notes in Electrical Engineering 276,
DOI: 10.1007/978-3-642-40861-8_10,

conflict and the resource limitation may also prevent the construction of the global IdP from being carried out.

In this study, we proposed a cross-IdP SSO method in SAML-based architecture, which provide the user a federation cross-IdP environment with the features of backward compatibility and personal anonymity. The message transfer from different IdPs can also prevent from malicious parties since the SAML V1. x has already supported PKI-based protocol. The related works will be briefly presented in section 2, and the proposed architecture is described in section 3. We have the discussion in section 4, and we conclude the features and future work in section 5.

2 Related Works

The solutions of Federation system are usually based on a Federated Identity Model (FIM) [1], with the property of authentication and authorization, and provide the ability of interoperability securely between heterogeneous information systems. SSO is one of the FIM functions whereby a single action of user authentication and authorization can permit a user to access all services, which the user has access permission without the need to enter multiple passwords. The other advantages of SSO systems are the security and anonymity. The users' privacy can be retained because there is only one authentication portal, which receives and stores users' credentials. The applications only receive information about whether they may let the user in or not. Also, the user authenticates only once, which means the transfer of sensitive information over the network can be limited.

There are mainly three implemented models: SAML [2], OpenID [3] and Microsoft CardSpace [4]. SAML is the most mature and comprehensive technology and has undergone standardization in 2002 (SAML 1.1) as well as in 2005 (SAML 2.0), respectively [5]. SAML defines a XML-based solution to perform SSO which allows users to gain access to website resources in multiple domains without re-authentications. To achieve SSO, the domains need to form a trust relationship before they can share an understanding of the users' identity. Following the specification of SAML, IdP is required for most of the SAML-based architectures. Alternative solutions [6] present approaches without an IdP by applying X.509 certificates for authentication only. However, the intermediate server is required to manage both the authentication and authorization processes between clients and SP. To support more commercial situations in the real world, we must enable the users also to achieve SSO under many Certificate Authorities.

One of the most common examples is the university campus. It may support various backend authentication mechanisms like Kerberos, LDAP and relational database. Although there exist researches [7, 8] that can be applied to the real circumstances, they may still lack of the demands of flexibility and scalability. The flexibility may involve the dynamic joined student associations, academic exchanges and department anniversary, which may join and leave frequently in a period of time. The scalability may involve the resource sharing among different campuses, universities and even with the industries.

3 Our Proposed System Architecture

In this study, we provide system architecture to achieve the cross-IdP identity federation. In this chapter, we exhibit the scenario, explain the concepts and provide the related algorithms.

3.1 Scenario

One of the most complicated environments is the university campus which involves various kinds of services and commercial services. Students who may register in two universities since they provide various kinds of curriculums. Many campuses also provide virtual money, which means students can pay for goods by using their student IDs (Figure1). Assume the user register with the name Gobby in NCTU for master degree, he may want to pay for the tuition or shop at the department store with different identity Bill. One scenario is that he has logged in at one of the web sites, he does not want to authenticate again and then can access these services or use the student ID to pay for bills, which may locate at different webs or locations. Another example of the usage is that if the user want to join the conference which does not belong to one of the members of the federation. These kinds of SPs may occur dynamically, which is hard for traditional SSO architecture to cooperate with these SPs. In accordance with these scenarios, the topology of different systems must be maintained and managed dynamically. Hence, to provide the backward compatibility and maintain the spirit of SSO, we introduce the new virtual role, named Manager, the detail is provided as follow.

3.2 System Components

There are three main roles in our proposed system includes Service Provider (SP), Identity Server (IdP) and Manager. Since all IdPs should provide authentication schemes for different services in original SAML-based architecture, we can recognize the IdPs as the portal sites which provide various kinds of services. Traditionally, a user may be asked to login the website many times if the SPs that he has visited is subordinated by different IdPs. To provide the basic facility of federation, IdPs must share the user criminal which leads to the tense of users' privacy leakage. On the other hand, users who have several accounts for different web sites may also cause the ambiguity of federations. Therefore, we introduce a new role, Manager, to handle

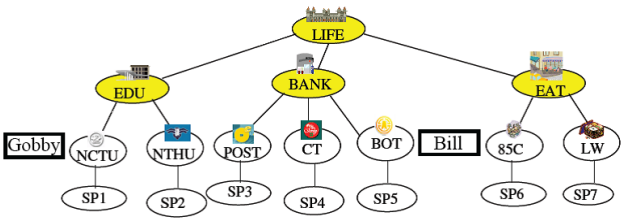

Fig. 1. Layered Concept in Actual Commercial System

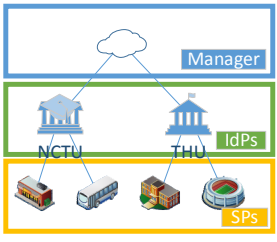

Fig. 2. System Components

the communication between different IdPs. Figure 2 demonstrates the component hierarchy. By using user Link_ID, which is similar to the pseudonym, can help Manager to cooperate different IdPs in a seamless way. One of the major contributions of our architecture is the anonymity since the IdPs only maintain the local identities. While communicating with other IdPs under the federation architecture, the user can be identified through the Link_ID, which is automatically created by the correspondent IdP (i.e. Manager) and the privacy information will not be exchanged through different IdPs.

3.3 Manager

In order to achieve identity federation, we define a third-party architecture, the Manager, to maintain users' identities. The Manager records the corresponding identities at different IdPs for the user by using account linking table (ALT), which can help different IdPs communicate with the global Link_ID with different identity of the same user. It provides privacy-preserving characteristic for a user during a web SSO exchange .The process of associating a Link_ID with another Link_ID at a partner is called account linking afterward. The user privacy can be guaranteed since the IdPs only maintain the local identities, which means there is no extra private information exchanged between different IdPs.

Figure 3 shows the example of ALT. Assume the user register on one of the IdPs, and the user wants to use the services on another website with different identities, he can log in at IdP_1 using his Gobby account and use another account Bill at IdP_2. Because the Manager will maintain the ALT, which helps the user use different account from different web sites at the same time. Besides, the Link_ID can also be different which provide the anonymity since these IdPs cannot get the local identities from each other.

3.4 Global Path Finding

The architecture defines that a user at an IdP wants to visit another IdP by following the tree path rather than peer to peer. Deliberate that the source IdP and destination IdP might not be below the same manager, so how to know the position of the destination IdP must be solved. Managers must record the nodes of its upper layer and lower layers. Briefly, in a path, a manager stores the Link_ID of the left neighbor along with the Link_ID of the right neighbor for every user. The global path of an IdP is encoded

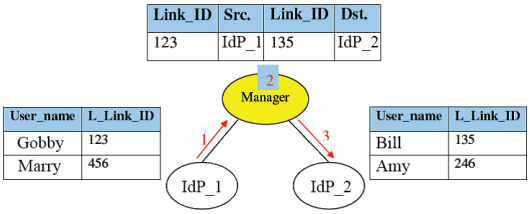

Fig. 3. Account Linking Table in the Manager

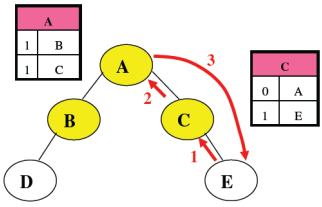

Fig. 4. An example of globa path finding

in a sequence of strings, which can indicate the position and relationship of the IdP. For the purpose of expansibility, the global path string is coded dynamically. (Figure 4) gives an example, the global path of IdP E should be coded "A_C_E", it indicates that E's manager is C and C's manager is A, and so on. The construction start with E sends a request to its Manager to get its global path. C receives the request and then appends C. The path code becomes "C_E". C looks up its table to know that it is not the top layer, then C keeps on sending the request to the upper layer. While A receives the request and appends A, the path code becomes "A_C_E". A refers to its table knowing there is no more upper layer, then sends back code path "A_C_E" to E. An IdP site can ask its global path upward gradually as above and stores the path code in the local site. Each IdP asks upward periodically and updates its path code when the topology changed.

3.5 Core Algorithm of Manager

When getting the global path of the destination IdP, the source IdP will send the string and the request of identity federation to its manager. After receiving, the manager will compare the string with its name to determine whether its name appears or not. If it appears, the fact expresses that the target IdP is under its subtree surely and the manager should send the request downward. Otherwise, the manager sends the request upward. Each manager, which receives the request of identity federation, will look up its ALT to determine whether a previous federation has been established for the user. If a previous federation has been established then continue to transmit forward according to the Link_ID, otherwise the manager needs to generate a Link_ID and record it to establish a new account linking entry. Due to the limitation of the paper pages, the algorithm of managers will provide in the future works.

4 Discussions

We also implemented the whole system and deployed in an university of north Taiwan. However, due to the limitation of paper pages, we strictly go analyze and discuss the proposed architecture.

4.1 Security

All information that delivered is Link_ID rather than real credentials. The source IdP and destination IdP neither know the ID used on the other side. It provides privacy-preserving characteristic for users. Besides, the malicious IdPs can be omitted since SMAL 1.x had already provided the PKI-based protocols, which means that all the exchanged messages can be encrypted and verified by using the SSL protocol.

4.2 Expansibility

The expansibility property can be discussed in vertical and horizontal ways. Each Manager must record the nodes of its upper layer and lower layers. We can take advantage of it to insert or delete SPs under different IdPs (Manager). Assume that a relationship exists as (Figure 1). Someday all three groups want to cooperate in demand,

and then the manager LIFE will be constructed in need to integrate them. If a new alliance, e.g. Play alliance, wants to join the exist federation, it can simply vertically add to the BANK alliance tree as a subordinate or horizontally add to the LIFE alliance.

4.3 Robustness

In the section, we would consider the influence when a manager is destroyed in the business system. Most probably account link in the node would not be operated. But it can work without involving the crashed node, including account linking. Besides, we consider another situation. That is, there is a petition to a certain manager and the connected was interrupted. The Link_ID which is generated previously would not disappear. After connecting successfully, the Link_ID can be used for another federation.

5 Conclusion

In this study, we proposed a method that can provide users an enterprise-crossed, services-integrated, backward compatible, and anonymity-maintained environment by introducing the concept of pseudonym based on SAML. All identity federations are established by Managers and dispersed evenly, and the communication between these Managers (IdPs) are secured by using PKI-based SSL. Comparing to the traditional SSO, regardless of sorting and storages may be required, it is more efficient and applicable. In the future, we will focus on developing a secure and efficient method to rebuild the destroyed Managers, because the recovery of previous federations may be required.

References

1. Bhatti, R., Bertino, E., Ghafoor, A.: An integrated approach to federated identity and privilege management in open systems. Communications of the ACM 50, 81–87 (2007)
2. Lockhart, H., Mishra, B.: Security Assertion Markup Language (SAML) 2.0 Technical Overview (2005)
3. Recordon, D., Reed, D.: OpenID 2.0: a platform for user-centric identity management. Discovery, 11–16 (2006)
4. Bhargavan, K., Fournet, C., Gordon, A.D., Swamy, N.: Verified implementations of the information card federated identity-management protocol. In: Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008, pp. 123–135 (2008)
5. Maler, E., Reed, D.: The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Security & Privacy Magazine 6, 16–23 (2008)
6. Fugkeaw, S., Manpanpanich, P., Juntapremjitt, S.: A Robust Single Sign-On Model Based on Multi-Agent System and PKI. In: Sixth International Conference on Networking (ICN 2007), pp. 4–9 (2007)
7. Akiyama, T., Teranishi, Y., Okamura, S., Sakane, E., Hasegawa, G., Baba, K., Nakano, H., Shimojo, S.: A Report of Campus-Wide IT Authentication Platform System Development in Osaka University. In: 2007 International Symposium on Applications and the Internet Workshops, p. 35. IEEE (2007)
8. Shen, J., Zhu, C.: Design and Implementation of Single Sign-on Using Yale-CAS. Computer Technology and Development (2007)