Poster: Single Sign-on Using Portable IdP on USB Flash Drive

Takahiro Ishii
Kanagawa Institute of Technology
Shimo-ogino 1030 Atsugi-shi
Kanagawa, Japan. Student

Atsushi Inoie
Kanagawa Institute of Technology
Shimo-ogino 1030 Atsugi-shi
Kanagawa, Japan, Assistant professor

Manabu Okamoto
Kanagawa Institute of Technology
Shimo-ogino 1030 Atsugi-shi
Kanagawa, Japan, Associate professor

***Abstract*—Single sign-on (SSO) is a mechanism whereby a single action of user authentication enables a user to access web services without entering multiple passwords. But, the SSO is not used much now, because almost all portal sites become Identity Providers (IdPs) and we have to use too many IdPs. That is, it is no longer a "single" sign-on. In this paper, we propose an SSO using a very personal portable IdP that we can carry on a USB flash drive.**

Keywords—single sign-on; authentication; USB

I. INTRODUCTION

Single sign-on (SSO) is one of several authentication methods. A user can be authenticated by a single action when that user uses plural service providers (SPs). Although standard SSO methods have been proposed, such as OpenID [1] and SAML [2], SSO is not yet familiar. To use SSO we need to access an Identity Provider (IdP) and the IdP must have some business merit. By using SSO, the IdP can acquire a number of accesses, gain ad revenue, or lead users to other services. So, every large site wants to become an IdP. As a result, we have to use plural IdPs, which are not "single" sign-ons.

In this paper, we propose an SSO method using a portable IdP on a USB flash drive. The IdP is very personal. In this method, we need only our personal IdP for SSO. The IdP on the USB flash drive is very safe; because the user always has his USB, no information on the IdP goes out.

The USB flash drive is very convenient and its memory has increased in size, e.g., 8,16,32 Gbytes. So, we can put an HTTP server on it and we can use the server for the IdP of the SSO.

II. RELAYED WORK: SINGLE SIGN-ON

Single sign-on is a standard technique of user authentication. One technique, OpenID is an open standard. When a user uses an SP (called the Relying Party (RP) in OpenID), the RP redirects the user to the IdP (OpenID provider (OP)) and the OP authenticates the user and brings him to the OP with an authentication response. The OP then confirms the response and authenticates the user. SAML is also a standard of SSO. SAML uses XML assertion in its authentication response. SAML maintains strong security and creates a trusted circle.

Both in OpenID and SAML, all users have to visit the IdP (or OP) and log in before using the SP, as shown in Fig. 1. The IDP can act as an identity service, and thus it can obtain some business advantages. The IdP can display advertisements on the login page for SSO. In addition, the IdP can develop various services as a portal site.

Consequently, a plural IdP provides an SSO service and then users have to use the plural IdP in parallel. This is not a "single" sign-on situation, and so it is a problem for SSO.

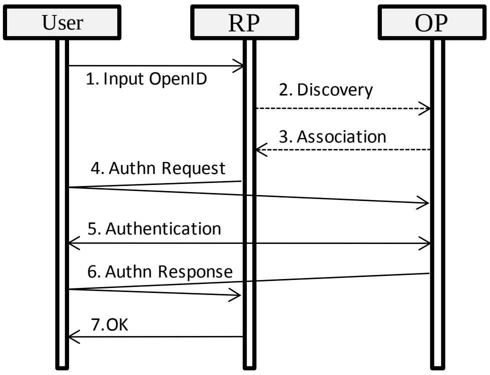

Fig. 1. OpenID sequence.

III. PROPOSED METHOD

In this paper, we propose an SSO method using a portable IdP on a USB flash drive. The size of HTTP server software, such as XAMPP [3], is approximately 300 M bytes and can easily fit on a USB flash drive. Therefore, we can carry the HTTP server anytime.

We place the HTTP server on a USB flash drive and make it an active IdP. The user connects the USB to a PC and launches the HTTP server software. That IdP is used only for the user who is the owner of the USB flash drive.

Fig. 2 shows an example of the sequence. We assume that OpenID is used for SSO. The sequence of SSO is exactly the same as the ordinary SSO method except the IdP is on a local host.

One advantage of this method is that we can appoint an IdP easily. In past methods, it was difficult for the SP to appoint an

IdP. So, the SP shows a list of IdPs for users on the SSO login page of the SP and the user selects one IdP. The IdP list is long, and it is difficult for the user to pick up one IdP in this long list. In this method, the SP can appoint an IdP by 127.0.0.1 (localhost). This action is very easy. The SP needs only to add one SSO link in the HTML of the login page, as shown in Fig. 3.

Furthermore, the HTTP server on the USB flash drive is useful for SSO without SSO standards. In an example of OpenID or SAML, the SP needs to create software to adapt to the standard method. This is a burden for a simple SP. But we can solve this problem by using the IdP on the USB flash drive.

The SP adds a submit button called "SSO by IdP". It is just a link to 127.0.0.1 (localhost) with a form with a hidden type that shows that the SP wants an ID/password. The SP uses "return_to" tag to show the return URL of the SP from the local IdP.

The IdP gets tags from the SP and extracts the ID/password in the IdP database. Extracting the ID/password is very easy because only one user (the owner of the USB flash drive) is on the IdP. The local IdP makes up a new form in the HTML and sets that action URL as "return_to". At that time, the ID and the password on the form are filled in as default values. The user only pushes the button, and the SP gets the ID/password by the customary form action. Fig. 4 shows this sequence.

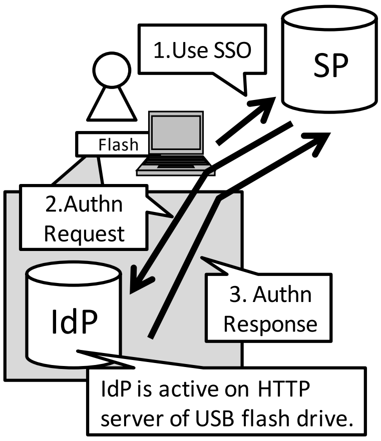

Fig. 2. Proposed method.

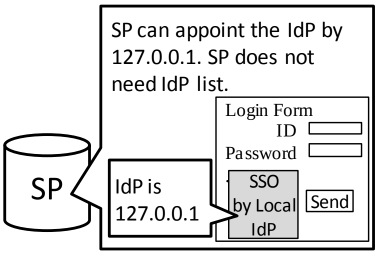
SP can appoint the IdP by 127.0.0.1. SP does not need IdP list.
Login Form
ID
Password
SP
IdP is 127.0.0.1
SSO by Local IdP
Send

Fig. 3. SSO form on SP.

IV. Advantages

In this section, we describe the advantages of our method.

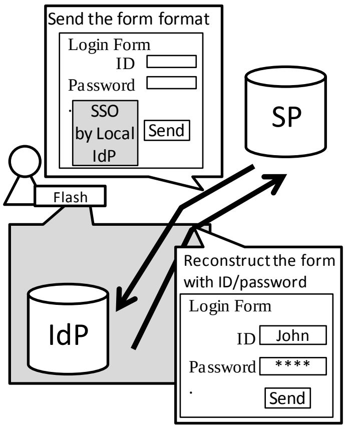

Fig. 4. Simple form login.

A. Usability

In this scheme, users need only a USB flash drive on which the HTTP server is installed. The SP has to do add just one link in the HTML, and it is very easy to appoint the IdP because it is 127.0.0.1. So, the SP does not need the IdP lists. We can use the USB flash drive anywhere on any PC and then we can use SSO ubiquitously. For example, we can use this method on a public PC, such as a PC in a business room of a hotel.

B. Efficiency

The SSO sequence is exactly the same as that for the standard method. The user can input an ID/password only on his personal IdP. This is then a "single" sign-on. The SP appoints 127.0.0.1 (localhost) as the IdP and then does not need the IdP list. In addition, when we cannot use the standard SSO method, we use the HTTP server as the IdP on the USB flash drive. At that time, the HTTP server on the flash drives acts as auto fill-in software and makes the forms with the ID and password as default values. The SP can get the ID and password by customary form actions.

C. Security

Since the SSO sequence is exactly the same as that for the standard method, the SSO security is the same as the standard. We use a personal IdP, and then it is not online anytime and there is no attack from cracker. Therefore, the ID/password is not leaked. Furthermore, some of USB flash memory is able to lock the drive. Using the USB password is required, and so another user cannot obtain the password of a user who has lost his USB.

V. Conclusion

In this paper, we propose an SSO using a portable IdP on a USB flash drive. Although it is a very personal IdP, the user can use the SSO ubiquitously.

References

[1] OpenID, http://openid.net/foundation/.
[2] OASIS SAML, http://www.oasis-open.org/committees/security.
[3] XAMPP, http://www.apachefriends.org/en/xampp-windows.html.