Poster: Authentication with Plural Servers in the Correct Order

Yuki Kuamazawa, Akane Ito, Manabu Okamoto
Kanagawa Institute of Technology
Shimo-ogino 1030, Atsugi-shi
Kanagawa, Japan

***Abstract*—For enhanced security, in addition to passwords, biometric identification, IC cards, and PKI certification can also be utilized. Further, multi-factor authentication, which uses plural certification to facilitate a single login, can also be utilized. In this paper, we propose a new multi-factor authentication system in which, not only is it necessary to receive certifications from plural authentication servers, but it is also necessary for the user to receive each certification in a specific correct order. This order is decided by users beforehand, and single sign-on protocols are used to exchange authentication requests and responses between servers.**

Keywords—authentication; multi-factor authentication; single sign-on

I. Introduction

Virtually all Service Providers (SPs), such as SNS, Webmail, and E-commerce sites, need to authenticate users. Most SPs use only passwords for authentication. However SPs handling money or personal information, such as e-banks, need stronger security than the password method. Key loggers and shoulder hacking are just two of the many threats to the password method. Furthermore, passwords can be stolen or guessed by attackers. Therefore, this method is dangerous.

Two-factor [1] or multi-factor authentication can be used to provide more enhanced security measures. For example e-bank SPs that utilize these methods can distribute a one-time password token machine for users and when that user login to the SP he/she needs to input both a normal password and the one-time password displayed on the machine. However, passwords or token machines that belong to the user may also be stolen, and attackers can easily use the stolen item and information to impersonate the user.

In this paper we propose multi-sign-on using multiple identity providers (multi-IdPs). In this method, even when all secret certifications are stolen, attackers will still experience difficulty impersonating the correct user.

II. Related Work: Multi-Sign-On

Multi-sign-on using plural IdPs on SSO protocols is proposed in [2]. In the proposed method, the SP needs no special functions and devices to enable multi-sign-on. IdPs can provide authentication certification for plural SPs, and users who wish to use the SP access the plural IdPs for authentication. In other words, plural SPs share the IdPs' authentication method. This method is very effective and reduces development costs. Fig. 1 illustrates this scenario.

However, virtually all IdPs utilize passwords for authentication, and so, even in multi-sign-on scenarios, users still need to input a separate password for each IdP. This is a burden and so users are apt to use the same passwords for all IdPs, which is dangerous because an attacker can then easily login to the SP with a common stolen password. In such a scenario, multi-sign-on would be ineffective.

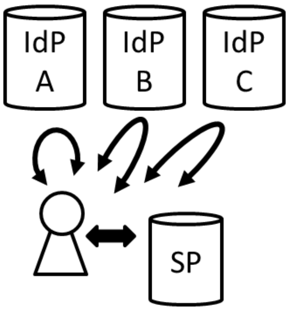


Fig. 1. Multi-sign-on using IdPs.

III. Proposed Method

In this paper we propose a new multi-sign-on system using plural IdPs on SSO protocols. In the proposed system, users must be authenticated by plural IdPs in a specific order registered by the user beforehand. We assume that a user has accounts with plural IdPs and an SP, with each IdP having an authentication method for user authentication. Even if all the IdPs use an ID/password method, the proposed system still provides enhanced security.

The proposed system operates as follows. First of all, the user registers his/her desired IdP order with the SP. For example, if the IdPs are A, B, and C, he/she can register an order such as {C, B, A}. The order is confidential and is known only by the user and the SP. Fig. 2 illustrates the operation of the proposed authentication system and Fig. 3 shows the sequence of actions carried out. Authentication via the proposed system proceeds as follows:

1. The user accesses the SP that he/she wishes to use.
2. The user selects the IdP that he/she wishes to be authenticated with and moves to that IdP. Naturally, the user knows the correct order that he/she registered

beforehand and so he/she selects IdPs in accordance with that order. For example, if he/she registered the order as {C, B, A}, he/she would access IdP C first.

3. The user is authenticated by the IdP based on its authentication policy.
4. The IdP provides a certificate of authentication for the SP. The SP receives the certification, checks it, and registers the order of the IdP that authenticated the user.
5. The user repeats steps 2, 3, and 4 until the sequence of IdPs is complete.

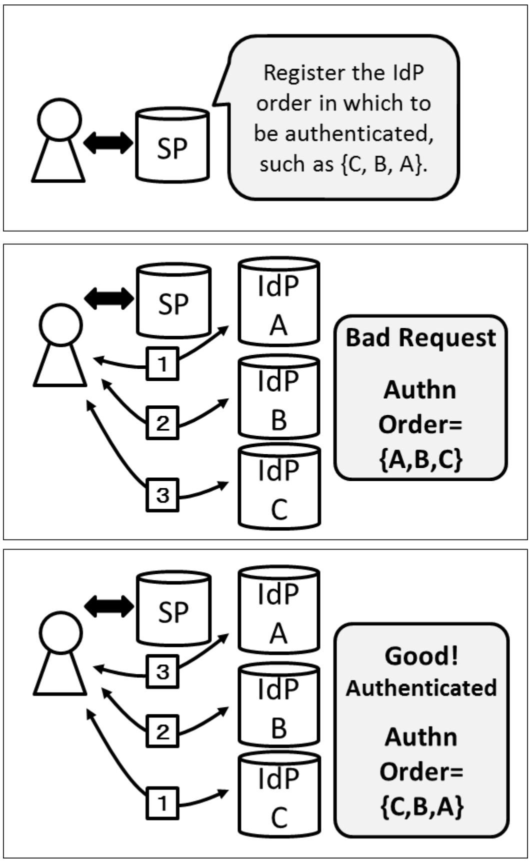


Fig. 2. Operation of the proposed authentication system.

For example, in Fig. 2, the user has registered the order of IdPs as {IdP C, IdP B, IdP A}. If the user is then authenticated by IdPs in the order {A, B, C}, the SP will not accept the authentication because the registered order is different. Only when the order of IdPs is exactly the same as the order registered beforehand is the user authenticated by the SP and can then use the services of the SP. In Fig. 2, only when the user is authenticated in the order {C, B, A}, can he/she use the SP.

In the sequence shown in Fig. 3, the SSO protocol OpenID [3] is used to exchange authentication information between SPs and IdPs. Using SSO, SPs can easily get authentication results. OpenID is used in real services widely. The sequence in Fig. 3 is based on the actual operation of OpenID. Fig. 4 shows an example user interface in a browser. When the user presses the “Not yet” button, he/she moves to the IdP corresponding to the button. However, the login button remains disabled until the user has obtained all certifications in the correct order.

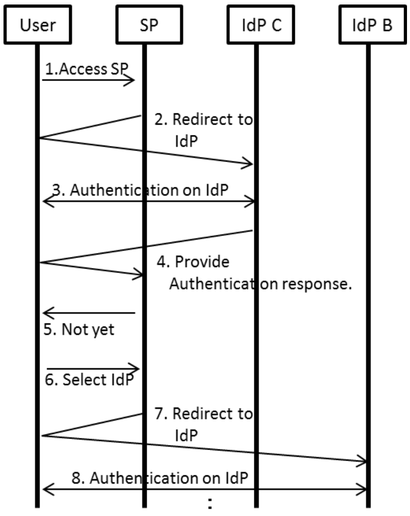
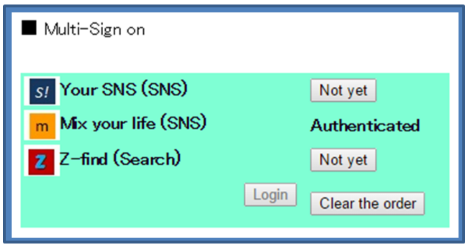


Fig. 3. Sequence of actions in the proposed system.


■ Multi-Sign on

Your SNS (SNS)	Not yet
Mix your life (SNS)	Authenticated
Z-find (Search)	Not yet
Login	Clear the order

Fig. 4. User interface of the system in a browser.

IV. Advantages of the Proposed System

In this system, even if all secret certifications are stolen, attackers will still have difficulty correctly authenticating with the SP without knowledge of the correct order.

Obviously, an attacker can try all combinations of IdPs. For example, in Fig. 2, the attacker can try all six combinations: {A, B, C}, {A, C, B}, {B, A, C}, {B, C, A}, {C, A, B}, {C, B, A}. To reduce the attacker’s chances of success, we can use many IdPs. For example, a user may use 10 IdPs and select only five of them, resulting in the attacker having to make the attempt 10 × 9 × 8 × 7 × 6 = 30240 times. Furthermore, if the number of IdPs is small, after a set number of failed attempts, the account can be locked for a fixed length of time, a log recorded, and a report sent to the user.

V. Conclusion

In this paper, we proposed a multi-sign-on system in which users have to be authenticated with plural IdPs in a set order registered by the user beforehand.

References

[1] D. DeFigueiredo, “The case for mobile two-factor authentication,” IEEE Security and Privacy, vol. 9, No. 5, pp. 81-85, 2011.

[2] T. Ishizuka, M. Okamoto, “Multi-sign-on; authentication collector,” IEEE Security and Privacy, Poster, 2014.

[3] OpenID, http://openid.net/foundation/.