Poster: Authentication by web browsing history

Chisa Kuroda, Mizuki Kobayashi, Mioko Watanaze, and Manabu Okamoto
Kanagawa Institute of Technology
Shimo-ogino 1030, Atsugi-shi
Kanagawa, Japan

***Abstract*—Almost all web services require user authentication. Several methods can be employed to authenticate users, such as passwords, biometric identification, IC cards, and PKI certification. The web services can select the most suitable method. In this paper, we propose a method that authenticates the user by confirming his/her history of visited web sites. Web services can perform more secure authentication than normal methods as a kind of risk-based authentication. No further action for authentication is required of a user or his/her device; the user can enjoy web surfing as usual while his/her actions are used for authentication.**

Keywords—authentication; web browsing history; life log

I. INTRODUCTION

Suppose you intend to begin web surfing. You start your computer, launch your browser, and access web sites one after another. You visit SNS first, and then connect to web mail. From there, you connect to blog services and a video-sharing site. Your surfing actions and visited sites typically do not change from day to day.

We herein present a means of authentication based on regular daily web-browsing actions. This risk-based authentication method involves user authentication based on browsing history.

II. RELATED WORK

Risk-based authentication [1-4] is a non-static authentication system. If the system perceives some kind of danger or unusual behavior of the user, it enables the application to challenge the user for additional credentials, such as a secondary password, whereas a static username and password may suffice for lower-risk situations. Risk-based authentication consists of using contextual information, such as an IP address, and historical information, such as keyboard strokes or mouse dynamics. However, such information belongs to hardware devices or the keyboard and mouse. Therefore, if a user frequently changes his/her device or location, it is not efficient.

III. PROPOSED METHOD

In this paper, we propose an authentication method that employs a user's site-visiting history. With this method, users can be authenticated by not only passwords but also their web-surfing histories. We use a single-sign-on method and identity providers (IdP). We refer to the service that authenticates the user by this method as the service provider (SP).

We assume that a user has accounts with IdP and SP. In addition to passwords, SP requires another authentication method for security. SP trusts IdP and enables authentication of the user on behalf of SP.

In preparation, the user first registers his/her usual daily actions, as shown in Figure 1. Details of these actions are beyond the present scope. We assume that a user provides a text list to SP; however, this may be performed in various ways. For example, IdP could possibly automatically record it.

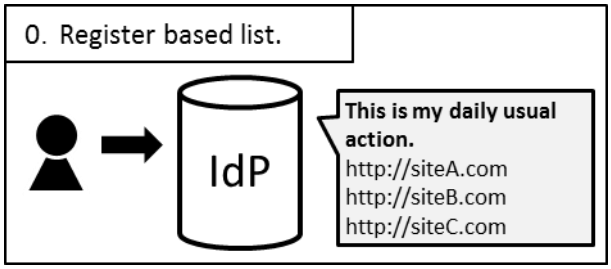

Fig. 1. Registered typical daily actions.

When the user wants to receive certifications and uses SP, he/she starts the computer and connects to IdP, which authenticates the user based on its authentication policy.

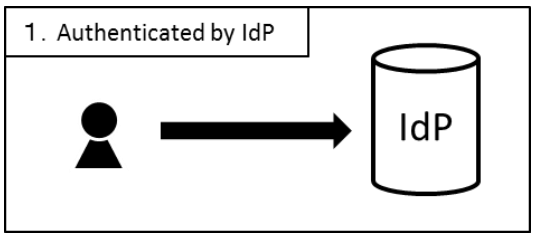

Fig. 2. Authentication by IdP.

The user begins web surfing. Here, the user visits "siteA.com." The HTML on the top page of siteA.com includes an image from IdP. For example, the HTML of the top page includes a tag, such as <img src=http://idp.com/history.jpg>, as shown in Figure 3. The image file is obtained from IdP, and IdP receives the HTTP request to obtain the image and HTTP referrer of the request parameter. Here, the HTTP referrer becomes the requested domain. In this example, when the user visits siteA.com, it obtains an image from IdP. Therefore, the HTTP referrer becomes siteA.com, and IdP can register the user's site-visiting history with this HTTP referrer.

Accordingly, web sites that support our method must add this image tag in the HTML of the top page. It is a very simple tag, such as "img src." After the user is authenticated by IdP, the site can obtain the image. When a user has not yet

authenticated by IdP, it provides a "No image yet" notice. The web site places the image on the HTML and a user can see it.

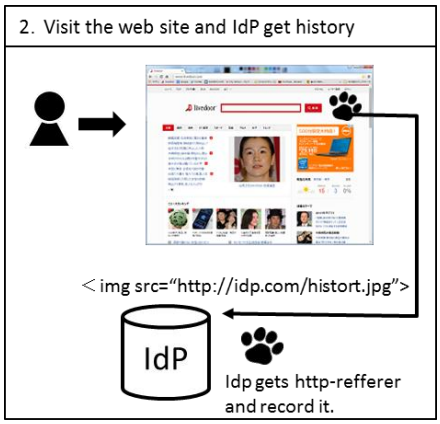

Fig. 3. IdP obtains a user's history.

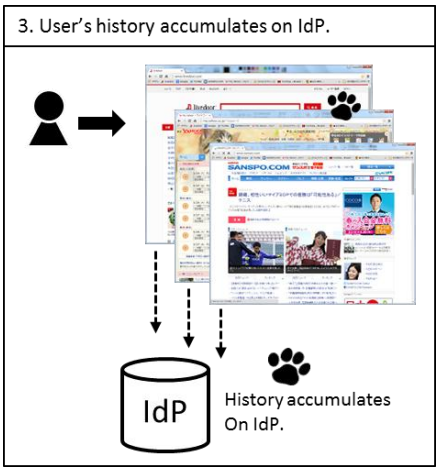

Fig. 4. User's history accumulated on IdP.

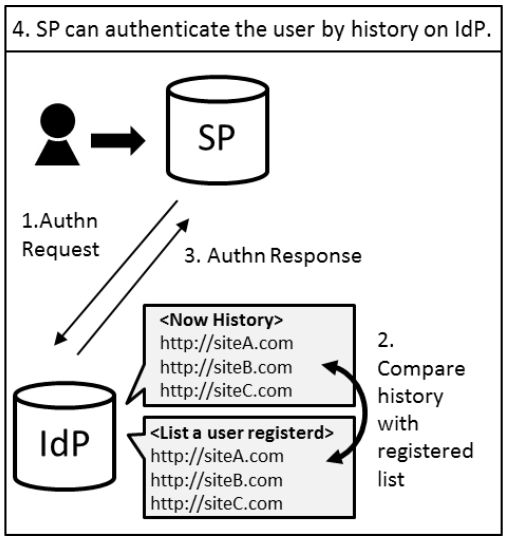

Fig. 5. Authetication by history.

A user continues web surfing, and IdP obtains his/her history, as illustrated in Figure 4. In this case, a user is going to employ SP and connects to it. Our method employs a single-sign-on protocol, such as OpenID [5]. According to that protocol, SP requests authentication from IdP. IdP compares the user's current history with his/her registered history and calculates the synchronization rate. IdP can provide an authentication response to SP with the user's identity, including this synchronization rate information.

We can apply some method in this enabling of the synchronization rate between IdP and SP. For example, IdP can precisely determine whether an authentication is valid. In other words, IdP can only provide 0% (not valid) or 100% (valid) as the user's synchronization rate. As another example, IdP can provide a set synchronization rate, such as 75%, and SP can evaluate it based on its policy.

Furthermore, IdP can provide an authentication response, including the user's history, and SP can assess that history. At that time, the user must register his/her daily history list for SP and the user's current history is provided to SP. This is not security-focused because browsing history is very personal information. We therefore assume that personal information is centralized on IdP.

IV. Proposed System Advantages

A user must first log into IdP. If a user has not logged into IdP, then the user's history cannot be registered by anyone; therefore, his/her personal information is not leaked.

If an attacker intends to impersonate a user, the attacker must not only steal the user's password but also record the user's entire browsing log, which is much more difficult.

A secondary password is sometimes used for risk-based authentication; however, a secondary password is not typically used and is therefore apt to be forgotten. Nevertheless, one's typical daily web surfing practices are rarely forgotten. Furthermore, browsing history authentication requires no special device or action; accordingly, this approach can be used at any time and place.

V. Conclusion

In this paper, we proposed a risk-based authentication system using web browsing history. SP can join this system only by supporting the single-sign-on protocol. Moreover, web services that support this system need only to add a simple image-acquiring HTML tag.

References

[1] N. N. Diep, S. Lee, Y.-K. Lee, and H.J. Lee, "Contextual risk-based access control," *Security and Management*, pp. 406-412, 2007.

[2] G. Tubin, "Emergence of risk-based authentication in online financial services: you can't hide your lyin' IPs," *Whitepaper #V43:15N, TowerGroup*, May 2005.

[3] M.S. Obaidat and D. T. Macchairllo, "An on-line neural network system for computer access security," *IEEE Transactions on Industrial Electronics*, Vol. 40, No. 2, pp. 235-242, April 1993.

[4] T. Enokido and M. Takizawa, "Purpose-based information flow control for cyber engineering," *IEEE Transactions on Industrial Electronics*, Vol. 58, No. 6, pp. 2216-2225, June 2011.

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