Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images

Tetsuji TAKADA[1] and Hideki KOIKE[2]

[1] SONY Computer Science Laboratories
Muse Bldg. 3-14-13 Higashigotanda, Shinagawa-ku, Tokyo 141-0022, JAPAN
zetaka@computer.org
[2] Graduate School of Information Systems, University of Electro-Communications
1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, JAPAN
koike@acm.org

Abstract. There is a trade-off between security and usability in user authentication for mobile phones. Since such devices have a poor input interfaces, 4-digit number passwords are widely used at present. Therefore, a more secure and user friendly authentication is needed. This paper proposes a novel authentication method called "Awase-E". The system uses image passwords. It, moreover, integrates image registration and notification interfaces. Image registration enables users to use their favorite image instead of a text password. Notification gives users a trigger to take action against a threat when it happens. Awase-E is implemented so that it has a higher usability even when it is used through a mobile phone.

1 Introduction

As mobile phones become widely used in various situations, a suitable method for user authentication is strongly required because they are often used as a user terminal for e-commerce and mobile banking. We currently, however, only have the option of using text-based authentication, such as user ID and password. This, however, is undesirable because of the trade-off problem between security and usability. It is better to use a longer password to ensure security. This, however, brings about usability issues such as the difficulty of remembering, recalling and inputting passwords. In particular, the difficulty of inputting passwords is critical in mobile phones because of the tedious input interface. In my mobile phone, for example, string "zetaka" requires 11 times of key typing. A simplified password, therefore, has been used such as a 4-digit number. However, we think that this type of authentication does not qualified enough to meet security requirements for e-commerce and mobile banking.

This paper proposes a novel authentication method for a mobile phone called "Awase-E". We assume that it will be used with a mobile phone with a digital camera. It uses photographic images taken by the users instead of text-based passwords. We also integrate two kinds of user interfaces into current authentication frameworks so that it not only improves usability but also enhances its security.

2 Awase-E: Image-based Authentication with Image Registration and Notification Interfaces

Awase-E is an authentication system using photographs instead of passwords. It, moreover, integrates image registration and notification interfaces into current authentication frameworks(**Fig. 1**).

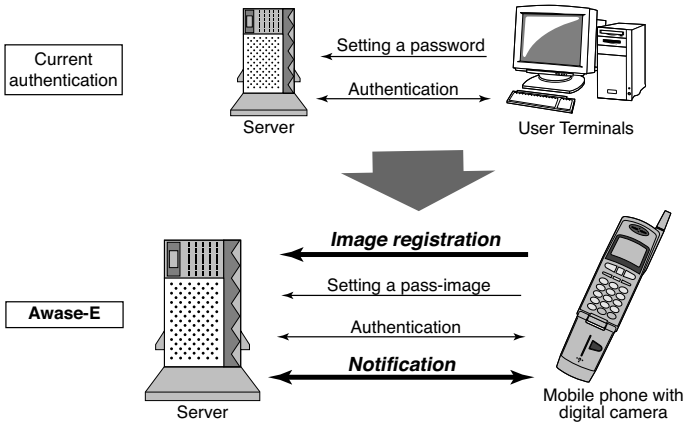

Fig. 1. Transition between Current and Proposed Authentication Framework

The image registration interface enables users to add their favorite images to the authentication system. As a result, this makes it possible for users to use their favorite image as a "pass-image". Almost 20 million users currently have mobile phones with digital cameras in Japan. Most of them send photos by E-mail with a few key clicks on the spot. The image registration interface is implemented using this function. It is implemented separately from a pass-image setting in order to ensure the security against impersonation attempts. This function simply enables users to add a photo to the system and a registered photo does not automatically become a pass-image. In other words, not all registered images become a pass-image. A user must set at least one pass-image before authenticating oneself using Awase-E.

The notification interface gives users a trigger to handle a threat practically. It notifies users of the occurrence of all kinds of events related to the authentication process. For example, Awase-E sends an E-mail to the user who has registered a photo. The E-mail has a URL. The web page that is linked by that URL contains the photo that a user has just registered. A user can thus confirm the registered photo immediately through a web page. If a user receives such an E-mail even though the user had not registered the photo, it means that someone has registered it masquerading as a legitimate user. A legitimate user, therefore, quickly knows when an intrusive attempt has been made. From these scenarios, we would strongly recommend using Awase-E with mobile phones to ensure a user's prompt awareness of a security breach.

Awase-E keeps an event history of past usage for certain periods for the purpose of auditing the user's authentication usage. A user can investigate the history through a web page. It enables users to check the authentication usage even if a user has lost their mobile phone.

Awase-E is implemented through both E-mail and Web. Prerequisite requirements for a user terminal is that it has access to the above two network service types. This means that it is also possible to use Awase-E from computers.

The detail of the authentication process is shown in **Fig. 2**.

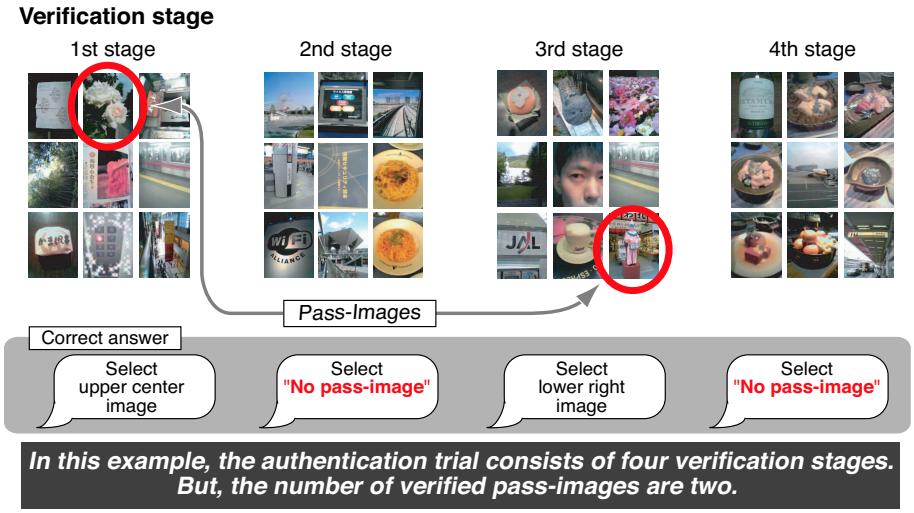

Fig. 2. A Detailed Authentication Process in Awase-E(N=4, P=9)

One authentication trial consists of **N** times of verification stages. Awase-E, of course, authorizes a user as a legitimate user only if all verifications are successful. In each verification stage, Awase-E shows **P** pieces of images on the screen, a user must select a pass-image correctly from them. Only one pass-image is included in each verification image set. The reason for this is to reduce the possibility that a randomly selected attacker's answer would be a correct answer. We call an image that is not a pass-image as a "decoy image". The location of each image in the image set is randomly determined. This means that the location of both pass-image and decoy images can change each time. It is also possible that there is no pass-image in an image set. In this case, the user must answer "no pass-image".

Awase-E is an easier method for users to complete the authentication process than before, even when using a mobile phone. The numerical keys on a mobile phone are uniquely correspond to each of the images on the screen at any given stage. This enables users to choose any image in the screen with one click. In using Awase-E, it is possible to authenticate oneself by just $\mathbf{N} + 1$ times of key types. Moreover, Awase-E does not need to input any text in authenticating oneself because it uses an E-mail address as a user ID.

3 Considerations

There are some related works which make an attempt to improve the problem of password-based authentication and the experimental results clearly indicate that image-based authentication has an advantage over password or PIN-based authentication[1, 2] especially in regards to the human interface aspect. It is easier for a user to memorize an image than a text. It is also easier to identify an image than recalling a text. However, previously proposed systems make use of images that are only provided by the system[3]. These system-assigned images have little relation to the users, and it is possible that a user will forget it as time goes on, even though it is an image.

Awase-E, then, uses photographs that are taken by users for authentication. Moreover, Awase-E enables users to add their favorite images to the system and to use them as pass-image in an easy way. This feature greatly reduces the load of memorizing and recalling the secret information over using system provided images. The reason is these images are closely related with the user's experience. This means that the user tends to remember the images subconsciously when the user looks at it. Using photographs also make it easier to generate and select a pass-image. We think that these advantages result in motivating users to change their pass-image more frequently. This is a feature that has not been realized in any current authentication methods. Another benefit of image registration is that it increases the number of total images in the authentication database. An image-based authentication, theoretically, has a vast information space for secret information. It is, however, practically limited by the number of total images that the system has in its database[1, 2]. In Awase-E, the database for images continues to expand as time passes.

Awase-E also introduces the case that there is no pass-image in generating a verification image set. This feature has two merits. One is that it reduces the number of pass-images that a user must remember. and therefore reduces the memory load on users. Of course, the case of a user selecting all"no pass-image" is not allowed for security reasons. The other advantage is that it also enhances the security level against "Intersection Attack"[1] which is a specialized attack method to this kind of image-based authentication. The reason is that this kind of attack can only occur when a pass-image is included in the image set in all verification stages.

The notification interface gives users the information of an occurrence of an attack through E-mail and the web. In other words, it gives a trigger to users to take a response against it. If a user is aware of an attempt that an attacker impersonates yourself, a user should add a new photo and change their pass-image to a new one. Current security assessments of existing authentications are evaluated by statistical methods only. It is clear that Awase-E has the same security level of **N**-digit number passwords. We think, however, the evaluation method ignores the aspect of users in authentication. It is difficult to rectify the well-known problem that "a user is the weakest link in the security chain". Awase-E provides a notification interface to address this issue. We expect that this type of alerting mechanism has a positive effect on changing the user's view

against computer security. The reason is that every user will probably encounter a malicious attempt in the near future. We believe that notification will become important in order to ensure the security level in any authentication system, and mobile terminals will become an essential device that can receive these notifications immediately on the spot.

The number of verification stages in Awase-E is variable. Awase-E, therefore, provides a flexible authentication framework that can handle various situations. For example, to emphasize security over usability, you could configure Awase-E such that a user must verifies 5 sets and must select a pass-image in 4 of the sets. On the contrary, if you put weight on usability over security, you can configure the process such that the user verifies only 3 sets and must select a pass-image in 1 of the sets.

From these considerations, we believe that Awase-E provides a better authentication framework that addresses both security and usability issues. In other words, Awase-E satisfies both security and usability issues at higher level than existing authentication methods.

4 Conclusion

In this paper, we proposed a novel authentication method called "Awase-E" that is used with mobile phones with digital cameras. We integrate image registration and notification interfaces into image-based authentication. Image registration enables users to use their favorite pictures as pass-images. And the notification interface gives users a trigger to take appropriate action against malicious attempts.

Awase-E is easily operable even when used through a mobile phone. Using a favorite picture as a pass-image reduces the memory load on users regarding secure information and is less memory-intensive than simply using system-assigned images. The notification function enables users to take appropriate action by themselves. In other words, it provides users with a method of ensuring the security of their own right. This feature is important in order to keep the user from being the weakest link in the security chain. We think that Awase-E realizes a higher level of coexistence in both security and usability than previous user authentication methods.

References

1. R. Dhamija and A. Perrig: Deja Vu: A User Study Using Images for Authentication, 9th Usenix Security Symposium, pp. 45–58, Aug (2000).
2. A.D.Angeli, M.Coutts, L.Coventry and G.I.Johnson: VIP: a visual approach to user authentication, Proc. of the Working Conference on Advanced Visual Interface (AVI2002), pp. 316–323, May (2002).
3. A. Perrig and D. Song: Hash Visualization: a New Technique to improve Real-World Security, In International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC), (1999).