Awase-E: Photo-based User Authentication System

Hideki Koike†, Tetsuji Takada‡, Takehito Onuki†
†Graduate School of Information Systems, University of Electro-Communications
1-5-1, Chofugaoka, Chofu, Tokyo 182-8585, Japan
‡Information Technology Research Institute, National Institute of Advanced Industrial Science and Technology
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591, Japan
Email: koike@acm.org, zetaka@computer.org, nukky@vogue.is.uec.ac.jp

INTRODUCTION

To minimize vulnerability in character-based password systems such as 4-digit PIN or alphanumeric password, image-based authentication, where the user selects pre-defined images (referred to as *pass-images*) from multiple images displayed on screen, are being proposed [2, 3, 4]. These systems are focusing on a human aspect rather than mathematical security. Researchers of image-based authentication state that they would minimize a human's cognitive load by effectively using the human cognitive ability to recall images. They state that "an image once seen is easy to recall."

Although we basically agree with this subjective argument, we have noted that few quantitative evaluations has been done to prove it [1]. Is it true that images are easier to remember or recall than character-based passwords, particularly over a long period of time? Another issue in image-based authentication is an implementation issue. Previous research proposed ideas or developed prototype systems for experiments. However, they did not tackle practical issues such as how we register photos, how we select pass-images, and so on.

The goals of this research are (1) to propose a new framework for image-based authentication, (2) to design and implement a practical authentication system using the Web and a mobile phone with a camera, and (3) to conduct user experiments in order to quantitatively discuss advantages of the proposed method as compared to traditional character-based authentication as well as other image-based authentication systems.

AWASE-E: PHOTO-BASED AUTHENTICATION SYSTEM

We developed a photo-based user authentication system, named "Awase-E" using the Web and a mobile phone equipped with a camera[4] (Figure 1). Figure 2 illustrates a sample authentication sequence of Awase-E. One authentication trial consists of **N** times of verification stages. Awase-E authorizes a user as legitimate if all verification stages are successful. At each stage, Awase-E shows **P** pieces of images on the screen, and the user has to select the correct pass-image among them. Figure 2 shows an example of the authentication scheme with **N**=4 and **P**=9.

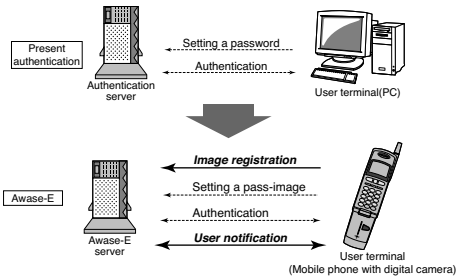

Figure 1: Four modules in Awase-E and comparison with current authentication

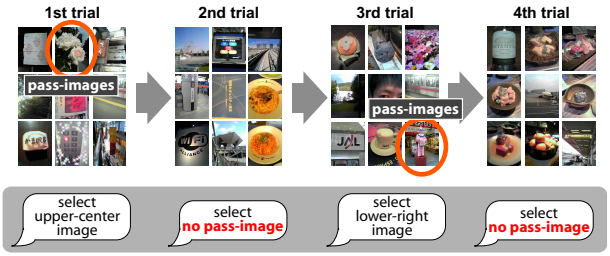

Figure 2: An example of one authentication sequence of Awase-E.

An each verification stage, the image set includes less than one pass-image. Images that are not pass-images are called "decoy images." The location of each image in the image set is randomly determined by the system. This means that the location of a pass-image and decoy images change every time. The user has to answer his/her pass-image if he/she finds one. If there is no pass-image in the image set, he/she has to answer as "no pass-image," which is always presented in each verification stage. At least one pass-image appears in one verification sequence (i.e., in 4 stages in this example), and the system does not allow an answer with all "no pass-images."

EXPERIMENTS ON LONG-TERM MEMORY

In order to evaluate how easy it is to remember and recall photos, even if they were used for a long period of time, the

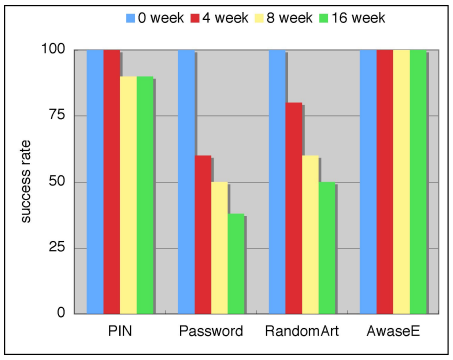

Figure 3: The change of success rates in four authentications in experiment.

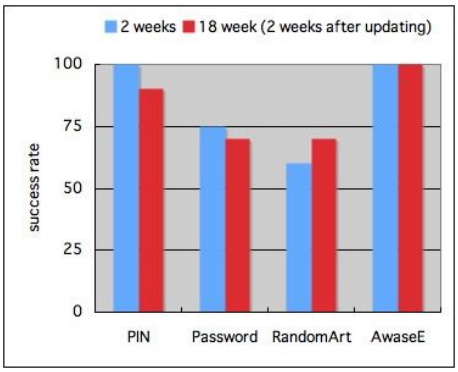

Figure 4: The change of success rates before and after updating password/pass-images in experiment.

following experiments were conducted.

As the character-based authentication methods, we chose a 4-digit password (*PIN*) and an alphanumeric password of more than 6 characters (*Password*). As the DejaVu-like image-based authentication systems (*Random Art*), we used the same authentication mechanism as that of Awase-E. However, the system used 100 computer-generated abstract images instead of photos. Each subject had to choose 4 images as pass-images from these abstract images. In Awase-E, 1200 photos were pre-registered, and subjects were required to register 4 photos taken by themselves.

Ten university students, all in their twenties, male, and belonging to the same laboratory, were involved in the experiment. They were all familiar with PINs and alphanumeric password through using ATMs or PCs in their daily lives. However, they had no experience in using any image-based authentication systems. The authentication experiments were done 0 (i.e., the initial authentication), 2, 4, 8, and 16 weeks after the subjects set their secret information (i.e., password or pass-images) to each authentication system. Just after the authentication on the 16th week, the subjects were asked to update their secret information. Then, after 2 weeks, they were asked to authenticate. Each authentication was done in our presence, and therefore the subjects could not use any memos having secret information. The subjects were allowed up to 3 trials for each authentication.

Figure 3 shows the success rate of four authentication methods after 0, 4, 8, and 16 weeks in experiment. This result shows that the success rate of Awase-E was the highest, and it was 100 percent within 3 trials after 16 weeks. On the other hand, over 60 percent of the subjects and 50 percent of the subjects forgot their passwords/pass-images after 16 weeks in Password and in Random Art, respectively.

Figure 4 shows the success rate change when the subjects were forced to update their secret information. The subjects were asked to update their secret information just after the authentication at the 16th week. The graph shows the success rate at 2 weeks after setting the initial password and the success rate at 2 weeks after updating their password. From this graph, it is notable that the success rate of traditional password became lower but that of the image-based authentication did not.

Discussion

Awase-E shows a high authentication success rate after 16 weeks. This implies that the use of photos and show-and-recognize authentication makes it possible for humans to remember secret information for a long period of time. At the same time, it shows that even when authentication is not used frequently, it is possible to provide more stable authentication. The minimum interval of authentication was 2 weeks, and this is probably less frequent than the use of an ATM in our daily lives.

People might wonder why Password showed such low scores in Figure 3. This was because the subjects did not use their familiar passwords in the experiment. They have familiar passwords for their daily life, and they use them to log in to a PC or use online services. However, these passwords are *real* secret information for them and they did not want to use real information in the experiment. Since they had to use unfamiliar passwords, they forget these passwords very easily.

One of the interesting result is the success rate change after updating the secret information. We first expected that the success rate would decrease in any authentication because the subjects might confuse the old passwords/pass-images and the new ones or they might fail to remember the new ones since they had become familiar with the old ones in 16 weeks.

REFERENCES

1. A. D. Angeli, M. Coutts, L. Coventry and G. I. Johnson: VIP: a Visual Approach to User Authentication, Proc. of the Intl. Conf. on Advanced Visual Interface (AVI2002), pp. 316–323, 2002.
2. R. Dhamija and A. Perrig: Deja Vu: A User Study Using Images for Authentication, 9th USENIX Security Symposium, pp. 45–58, 2000.
3. T. Pering, M. Sundar, J. Light, and R. Want: Photographic Authentication through Untrusted Terminals, IEEE Pervasive Computing, Vol.2, No.1, pp. 30–36, 2003.
4. T. Takada, H. Koike: Awase-E: Image-based Authentication for Mobile Phones Using User's Favorite Images, Proc. of 5th Intl. Symposium, Mobile HCI 2003, Springer, pp. 347–351, 2003.