Can Users Remember Their Pictorial Passwords Six Years Later?

Thomas S. Tullis
Fidelity Investments
82 Devonshire St., V3B
Boston, MA 02109 USA
Tom.Tullis@fmr.com

Donna P. Tedesco
Fidelity Investments
82 Devonshire St., V3B
Boston, MA 02109 USA
Donna.Tedesco@fmr.com

Kate E. McCaffrey
Fidelity Investments
82 Devonshire St., V3B
Boston, MA 02109 USA
Kate.McCaffrey@fmr.com

CHI 2011, May 7–12, 2011, Vancouver, BC, Canada.
ACM 978-1-4503-0268-5/11/05.

Abstract
Previous research had shown that pictorial passwords, where users recognize their target images among distractors, have potential for improving the usability of authentication systems. A method using personal photos provided by the users as their targets, shown among highly similar distractors, showed the most promise for both accuracy and security. But the longest time period that had been tested between successive login attempts was only about one month. We wanted to see what happens when six years have elapsed. We recruited some of the same participants from the previous study and tested their ability to select their target photos six years later. We found that 12 of 13 participants successfully authenticated themselves. The overall accuracy rate was 95.6%, demonstrating that most users can remember these pictorial passwords even over long periods of time.

Keywords
User authentication, pictorial passwords, photos, photographs, longitudinal study, pictures

ACM Classification Keywords
H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

General Terms

Human Factors, Security.

Introduction

Remembering passwords has become a major issue for many people. As online activities such as banking, shopping, and research have increased, so too have the number of passwords that users must remember. For example, in a study that gathered information from over 500,000 users [1], the average person had 25 different online accounts they need passwords for. Each of these people had an average of 6.5 passwords, each of which was reused at 3.9 sites. Difficulty remembering passwords has apparently prompted many users to adopt extremely simple and weak passwords. An analysis of the top passwords from the hacked Gawker website [2] found that the most popular password was "123456", followed closely by "password". However, as privacy concerns have increased, many sites have begun to require stronger passwords, often with different rules for their construction, causing users to need even more passwords.

Alphanumeric passwords may be the most common form of security, but they are certainly not the only option. Researchers have tried to develop secure authentication methods that take advantage of the strengths of the human brain rather than taxing it. One promising line of research has investigated the use of graphical or pictorial passwords (e.g., [3],[5]).

In our previous research [5], we investigated several different approaches to pictorial passwords, where users must identify their target photos within arrays of distractor photos. For that study, participants submitted 5 – 18 photos that they would have to recognize as their "password". Participants were asked to submit photos of personal significance to them, but which others would not easily associate with them (e.g., avoiding recognizable photos of themselves). These were the "target" photos.

After entering their user ID, participants attempted to recognize their personal photos to authenticate themselves. In the final experiment of that study, participants were shown five consecutive screens of sixteen photos each. Each screen contained one target photo and fifteen "distractor" photos. After a user clicked on a photo for the screen, the next screen appeared with no feedback as to whether the first click was correct. A success or failure was indicated to users only after they completed clicking on photos for all five screens.

As one way of testing the security of this approach we also asked participants to try to "break in" as other participants in the study. All of the participants worked at Fidelity Investments, in some cases having worked together for many years.

We found that the best combination of accuracy and security was when the distractors were tailored to each target photo—i.e., the fifteen distractors shown with a given target were chosen to be very similar to it rather than simply a random set of distractors. All of the participants in that study were able to successfully authenticate themselves by selecting their target photos, even after 30 days had elapsed.

We recently began to wonder how well these same participants would be able to recognize their target

photos now that six years have passed since that previous study. Although six years is probably an extreme amount of time between successive logins to a given site, it is easy to imagine cases where a year or more might elapse (e.g., a site for submitting your annual taxes). In our previous study, the longest time lapse was only one month. Testing the long-term memorability of these pictorial passwords was the purpose of the current study.

Method

Somewhat to our surprise, we found that fourteen people who had provided photos for our 2005 study still worked at Fidelity. This is slightly more than the number of participants in the last reported experiment from the previous study because a few more people completed the study after that paper was published.

We contacted each of these people and asked, somewhat mysteriously, if they would be willing to participate in a short usability study. Since we did not want the participants to try to find (and study) the photos they had submitted for the previous study, we did not initially explain the purpose of this "usability study". Thirteen of them were willing to participate.

The study was conducted in our Usability Lab. Participants were not told the nature of the study until the beginning of the session. None of the participants had seen or used their photos for authentication since the previous study, which was conducted almost exactly six years earlier.

The procedure was basically the same as in the "Tailored Distractors" condition from Study 3 of the previous study [3]. Participants attempted three trials each to authenticate by recognizing their target photos among tailored distractors. Figure 1 shows an example of the five screens for one trial seen by one of the participants in the study.

Participants were then given three chances to try to break in as another participant in the study. They were shown a list of the participants in the study and their user ID's. Participants were able to use the break-in trials as they wished: they could attempt to break in as the same person three times, or try to break in as two or three different people across the three trials.

Results

Twelve of the thirteen participants successfully authenticated by recognizing their pictorial passwords. (As in the previous study, participants were given up to three trials to successfully authenticate.) The overall accuracy rate per trial was 95.6% correct. As shown in Figure 2, accuracy for each participant (the percent of their targets that they recognized) ranged from 73% to 100%. Nine of the twelve participants correctly identified all five of their target photos on all three of their trials. Three failed on their first trial but then succeeded on their second and third trials. One participant (P3) failed on all three trials, even though his overall accuracy was 73%.

On the average, participants took 37 seconds per trial (five screens). In our previous study [3], participants took an average of 21 seconds per trial. Not having used the photos for authentication in six years obviously slowed the participants down.

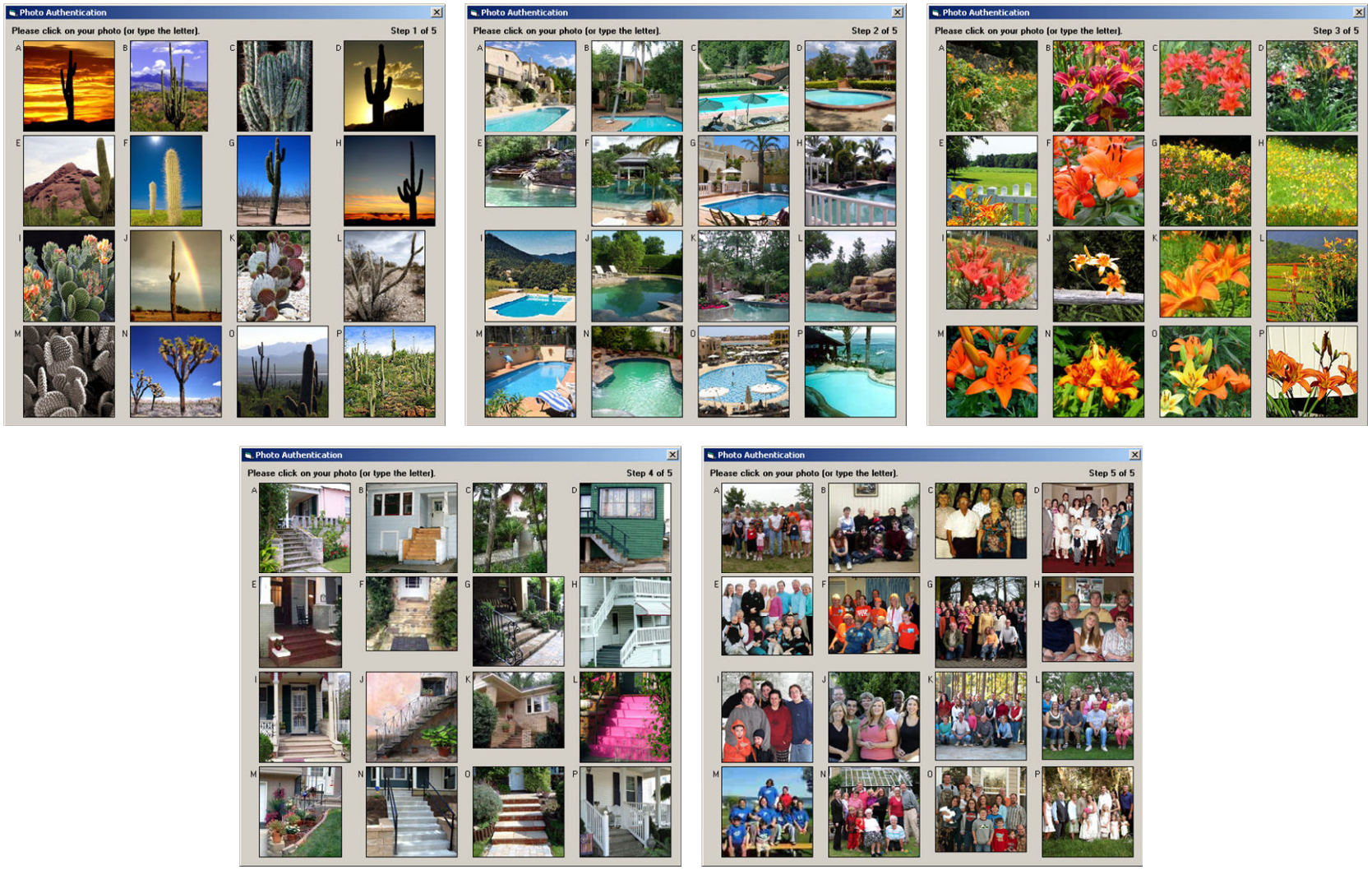

figure 1. An example of the five screens seen by one participant on one trial. On each of these screens, one of the sixteen photos had been provided six years earlier by the participant. The other fifteen photos were highly similar distractor photos chosen by the experimenters. Participants had to correctly identify all five of their photos to successfully authenticate themselves.

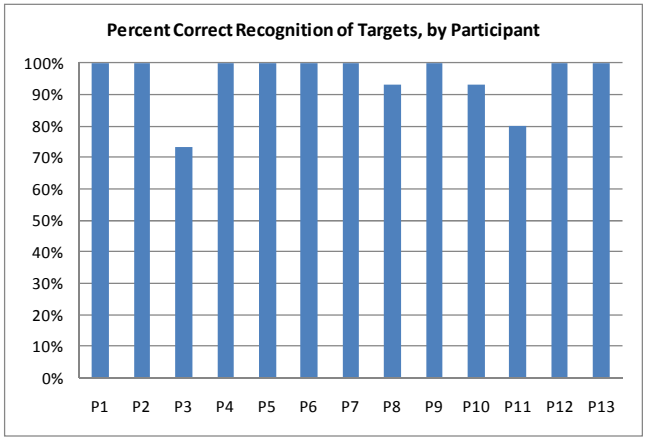

figure 2. Percentage of their 15 target photos (5 per trial x 3 trials) that each of the participants correctly recognized.

During the attempted "break-in" trials, none of the participants succeeded in breaking in as another participant in the study. They failed on every trial. Overall, their accuracy rate per trial was 20.5%, or about 1 out of 5 targets correctly identified. (This is almost exactly the same as the break-in accuracy from our previous study.) Accuracy per participant, as shown in Figure 3, ranged from 0% to 53%.

Keep in mind that all of the participants in this study work at Fidelity Investments, mostly in the same department. Some have known each other for 15+ years. Consequently, their ability to correctly guess an average of one target photo per break-in trial is perhaps not surprising.

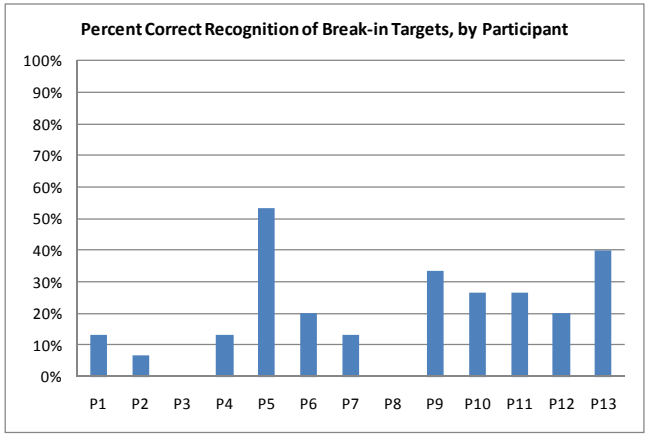

figure 3. Percentage of the 15 target photos that participants correctly guessed on attempted "break-in" trials.

Discussion

The majority of the participants were successful in recognizing their target photos even though six years had passed since they last used the photos in this manner. Only one participant failed to recognize all of his photos. In talking to this participant, we learned that most of the photos he had originally provided were not ones that he took; some were photos he had found on the web and thought were interesting. Consequently, the photos were perhaps not as personally significant to him as the other participants' photos were to them.

Whether the level of "break-in" accuracy found in this study (20%) is acceptable for a given application obviously depends upon the level of privacy and security required for that application. Security of this method could be increased by increasing the number of distractor photos per screen (e.g., using a 5 x 5 grid of

photos) or the number of screens (e.g., six). Alternatively, this method could be used as a way of recovering a textual password, similar to the way "challenge questions" are commonly used.

In this study, we hand-picked the distractor photos that were shown with each target photo. Obviously, this is not a method that could be used in a real implementation of this technique. Future research should focus on practical methods for identifying similar distractor photos. One possible method could be to require users to provide textual tags describing their photos at the time of submission (e.g., "cactus", for the first example in Figure 1). These tags could then be matched against the tags for photos in a large collection of distractor photos. This could perhaps be used in conjunction with pattern recognition algorithms to detect photos with a similar visual appearance. For verification of the similarity of the distractors, the user might be shown a set of candidate distractors at the time of submission, perhaps asking the user to identify the distractors that are the most similar to their photo.

This type of pictorial password probably would not be appropriate for frequently used passwords (e.g., a LAN password) since it is slower to use than a typical alphanumeric password. For example, in a study of various keyboard designs for entering strong-security alphanumeric passwords [4], participants took an average of 9 seconds to enter the password using a traditional QWERTY keyboard. This is significantly faster than the 37 seconds in the current study or even the 21 seconds in our previous study.

However, in cases where a significant amount of time might elapse between uses of the password, this type of pictorial password using personal photos is very promising. Digital cameras, including cameras in cell phones, have become almost ubiquitous since our previous study, so providing photos for a system like this would be relatively easy for many people. One of the keys to the long-term recognition of the photos appears to be the personal significance of the photos. At the same time, they need to be photos that others would not be able to readily recognize and associate with that user, which could become more challenging with the rapid growth of photo-sharing via social media.

References

[1] Florencio, D. and Herley, C. A large-scale study of web password habits, *Proceedings of the 16th international conference on World Wide Web*, May 8-12, 2007, Banff, Alberta, Canada.

[2] Seward, Z. M., and Sun, A. The Top 50 Gawker Media Passwords. *The Wall Street Journal*, December 13, 2010.

[3] Takada, T., Onuki, T., and Koike, H. Awase-e: Recognition-based image authentication scheme using users' personal photographs. *Innovations in Information Technology*, 2006, pages 1-5, Nov. 2006.

[4] Tullis, T., Mangan, E., and Rosenbaum, R. An Empirical Comparison of On-Screen Keyboards. Human Factors and Ergonomics Society 51st Annual Meeting, Baltimore, MD, October 1-5, 2007.

[5] Tullis, T. S., and Tedesco, D. P. Using personal photos as pictorial passwords, *CHI '05 extended abstracts on Human factors in computing systems*, April 2-7, 2005, Portland, OR, USA.