Authentication Using Graphical Passwords: Basic Results

Susan Wiedenbeck
Jim Waters

College of IST
Drexel University
Philadelphia, PA, 19104 USA
susan.wiedenbeck@cis.drexel.edu
jw65@drexel.edu

Jean-Camille Birget

Computer Science
Department
Rutgers University
Camden, NJ, 08102 USA
birget@camden.rutgers.edu

Alex Brodskiy
Nasir Memon

Computer Science Department
Polytechnic University
Brooklyn, NY, 11201 USA
abrods01@utopia.poly.edu
memon@poly.edu

Abstract

Access to computer systems is most often based on the use of alphanumeric passwords. However, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters. We have designed a new and more secure graphical password system, called PassPoints. In this paper we describe the PassPoints system, its security characteristics, and the empirical study we carried out comparing PassPoints to alphanumeric passwords. In the empirical study participants learned either an alphanumeric or graphical password and subsequently carried out three longitudinal trials to input their passwords over a period of five weeks. The results show that the graphical group took longer and made more errors in learning the password, but that the difference was largely a consequence of just a few graphical participants who had difficulty learning to use graphical passwords. In the longitudinal trials the two groups performed similarly on memory of their password, but the graphical group took more time to input a password.

1 Introduction

Until recently computer and network security has been formulated as a technical problem. However, it is now widely recognized that most security mechanisms cannot succeed without taking into account the user (Patrick, Long, & Flinn, 2003).. A key area in security research is authentication, the determination of whether a user should be allowed access to a given system or resource. Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. Today other methods, including graphical passwords, are possible alternatives. This paper reports on research aimed to design a new kind of graphical password system, empirically test its usability, and compare it to alphanumeric passwords. The significance of this research is the provision of a flexible graphical password system with extensive human factors data to support it.

We refer to the security and usability problems associated with alphanumeric passwords as "the password problem" (Wiedenbeck, Waters, Birget, Broditskiy & Memon, 2005). The problem arises because passwords are expected to comply with two fundamentally conflicting requirements:

1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.
2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

Satisfying these requirements is virtually impossible for users. Consequently, users ignore the requirements, leading to poor password practices (Morris & Thompson, 1978; Adams & Sasse, 1999; Sasse, Brostoff & Weirich, 2001).

This problem has led to innovations to improve passwords. One innovation is graphical passwords, i.e., passwords that are based on images rather than alphanumeric strings. The basic idea is that using images will lead to greater memorability and decrease the tendency to choose insecure passwords. This, in turn, should increase overall password security. Several graphical password systems, described in the next section, have been developed and some HCI evaluation has been done.

In this paper, we describe a new and more secure graphical password system that we have designed. We report on an empirical study comparing the use of this graphical password system to alphanumeric passwords in a longitudinal study. Our primary research question is the following: Are graphical passwords competitive to alphanumeric passwords in security, learning, performance, and retention?

2 Background on Passwords

2.1 Problems with Alphanumeric Passwords

The password problem arises largely from limitations of humans' long-term memory (LTM). Once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. Decay and interference explain why people forget their passwords. Items in memory may compete with a password and prevent its accurate recall (Wixted, 2004). If a password is not used frequently it will be even more susceptible to forgetting. A further complication is that users have many passwords for computers, networks, and web sites. The large number of passwords increases interference and is likely to lead to forgetting or confusing passwords.

Users typically cope with the password problem by decreasing their memory load at the expense of security. First, they write down their passwords (Adams & Sasse, 1999). Second, when they have multiple passwords, they use one password for all systems or trivial variations of a single password. In terms of security, a password should consist of a string of 8 or more random characters, including upper and lower case alphabetic characters, digits, and special characters. A random password does not have meaningful content and must be memorized by rote, but rote learning is a weak way of remembering (Rundus, 1971). As a result, users are known to ignore the recommendations on password choice. Two recent surveys have shown that users choose short, simple passwords that are easily guessable, for example, "password," personal names of family members, names of pets, and dictionary words (Sasse et al., 2001; Brown, Bracken, Zoccoli, & Douglas, 2004). To users the most important issue is having a password that can be remembered reliably and input quickly. They are unlikely to give priority to security over their immediate need to get on with their real work.

2.2 Why Graphical Passwords?

Graphical passwords were originally described by Blonder (1996). In his description of the concept an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated.

Memory of passwords and efficiency of their input are two key human factors criteria. Memorability has two aspects: (1) how the user chooses and encodes the password and (2) what task the user does when later retrieving the password. In a graphical password system, a user needs to choose memorable locations in an image. Choosing memorable locations depends on the nature of the image itself and the specific sequence of click locations. To support memorability, images should have semantically meaningful content because meaning for arbitrary things is poor (Norman, 1988). This suggests that jumbled or abstract images will be less memorable than concrete, real-world scenes. LTM does not store a replica of the image itself, but rather a meaningful interpretation (Mandler & Ritchey, 1977). To retrieve the locations a user will be dependent on the encoding used while learning. A poor encoding will hurt retrieval by failing to distinguish similar objects.

Depending on the graphical password system, at retrieval time users will be presented with either a recognition task or a cued recall task. In a graphical password system based on recognition, the user has to be able only to recognize previously seen images, making a binary choice of whether the image is known or not known. Recognition is an easier memory task than pure, unaided recall (Norman, 1988). In our password system we use an intermediary form of recollection between pure recall and recognition, cued recall. Scanning an image to find previously chosen locations in it is cued recall because viewing the image reminds, or cues, users about their click areas. Psychologists have shown that with both recognition and recall tasks, images are more memorable than words or sentences (Sheperd, 1967; Paivio, Rogers & Smythe, 1972; Standing, 1973). This is encouraging in terms of memory for graphical passwords.

Efficiency is important in password systems because users want to have quick access to systems. The time to input a graphical password by a highly skilled, automated user can be predicted by Fitts' Law (1954). The law states that the time to point to a target depends on the distance and size of the target – greater distance and smaller targets lead result in slower performance. Existing evidence suggests that alphanumeric passwords may be faster to input than graphical passwords (Dhamija & Perrig, 2000). However, the question remains how big the difference may be.

3 Design of PassPoints

3.1 Background on Graphical Password Systems

Here we discuss some graphical password systems based on recognition or cued recall of images. Most existing systems are based on recognition. The best known of these systems are Passfaces (Brostoff & Sasse, 2000; Real User Corporation, 2001) and Déjà Vu (Dhamija & Perrig, 2000). Brostoff and Sasse (2000) carried out an empiricial study of Passfaces, which illustrates well how a graphical password recognition system typically operates. To create a password, the user chose four images of human faces from a portfolio of faces. To log in the user saw a grid of nine faces, which included one face previously chosen by the user and eight decoy faces. The user had to click anywhere on the known face. This procedure was repeated with different target and decoy faces, for a total of four rounds. If the user chose all four correct faces, he or she successfully logged in. Data from this study suggest that Passfaces are more memorable than alphanumeric passwords. A small study of the use of Déjà Vu came to the same conclusion. On the other hand, passwords based on image recognition have a serious disadvantage. Only a small number of faces can be displayed on each screen, e.g., in Passfaces nine faces. An attacker has a 1-in-9 chance of guessing this passface. Consequently, the login process requires repetitive rounds of face recognition. If four rounds are used the chance of guessing the password is $(1/9)^4 = 1.5 \times 10^{-4}$. With a few thousand random guesses an attacker would be likely to find the password. To increase security similar to that of 8-character alphanumeric password, 15 or 16 rounds would be required. This could be slow and annoying to the user.

Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation (Boroditsky, 2002), the user chooses several predefined regions in an image as his or her password. To log in the user has to click on the same regions. The problem with this scheme is that the number of predefined regions is small, perhaps a few dozens in a picture. The password may have to be up to 12 clicks for adequate security, again tedious for the user. Another problem of this system is the need for the predefined regions to be readily identifiable. In effect, this requires artificial, cartoon-like images rather than complex, real-world scenes.

3.2 Design of the PassPoints System

We developed a graphical password scheme based on Blonder's original idea that overcomes its limitations of needing simple, artificial images, predefined regions, and consequently many clicks in a password. Our scheme: (1) allows any image to be used and (2) does not need artificial predefined click regions with well-marked boundaries – a password can be any arbitrarily chosen sequence of points in the image (Birget, Hong, & Memon, 2003). Complex images can have hundreds of memorable points, so for example, with 5 or 6 click points one can make more passwords than 8-character Unix-style passwords. In order to log in, the user has to click close to the chosen click points, within some set tolerance distance, e.g., within .25 to .50 cm from the user's click point. The tolerance is needed because the user's click point literally is a single pixel, which is too precise for a user to click on successfully. The tolerance, which is adjustable in the system, gives a margin of error around the click point, in which the user's click is recognized as correct.

In Wiedenbeck et al. (2005) we compare the password space of PassPoints with alphanumeric passwords, for various parameter settings. The password space is the set of all passwords that are possible for a given password scheme and for a given setting of parameters. For example, for alphanumeric passwords of length 8 over a 64-

character alphabet, the number of possible passwords is $64^8 = 2.8 \times 10^{14}$. In PassPoints if the image size is 1024 x 752 (i.e., roughly the full screen), with a tolerance around the click point of 20 x 20 pixels, and with passwords consisting of 5 clicks, the password space will have size 2.6×10^{16}.

4 Methodology

4.1 Participants

Forty experienced computer users participated in the study. The mean age of the participants was 32.9 years (SD = 10.9), and the range was from 20 to 55 years. The sample included 23 males and 17 females.

4.2 Materials

The system included both graphical and alphanumeric password interfaces. The PassPoints system was instrumented for data collection. The graphical password interface consisted of an image for inputting the password and several buttons (Figure 1). A single image was used in this experiment. It showed a scene of a hotel swimming pool with people moving around it. The colorful image had many objects that could serve as memorable click points. For the purposes of testing the size of the picture was 451 x 331 pixels. The tolerance, around a click point was set to 20 x 20 pixels (a square of area .53 cm^2). The rest of the interface consisted of a background with five buttons and with empty space to present instructions in the experiment. The Submit button was used to submit the password when the user had entered it. The Clear button erased all password points input so far. The Undo button erased only the user's most recent point. The See My Password button allowed the users to view their password during the learning phase and under certain circumstances in the retention phase. The Quit button allowed a user to quit the experiment. All instructions for the participants were given on the screen and feedback on correctness of a password input was given on screen when the user clicked the Submit button. The online testing system also included a questionnaire that asked the user's perceptions of the password system. In the alphanumeric interface a typical password input field was shown in which the user typed a password. The buttons were Clear, Submit, Show My Password, and Quit.

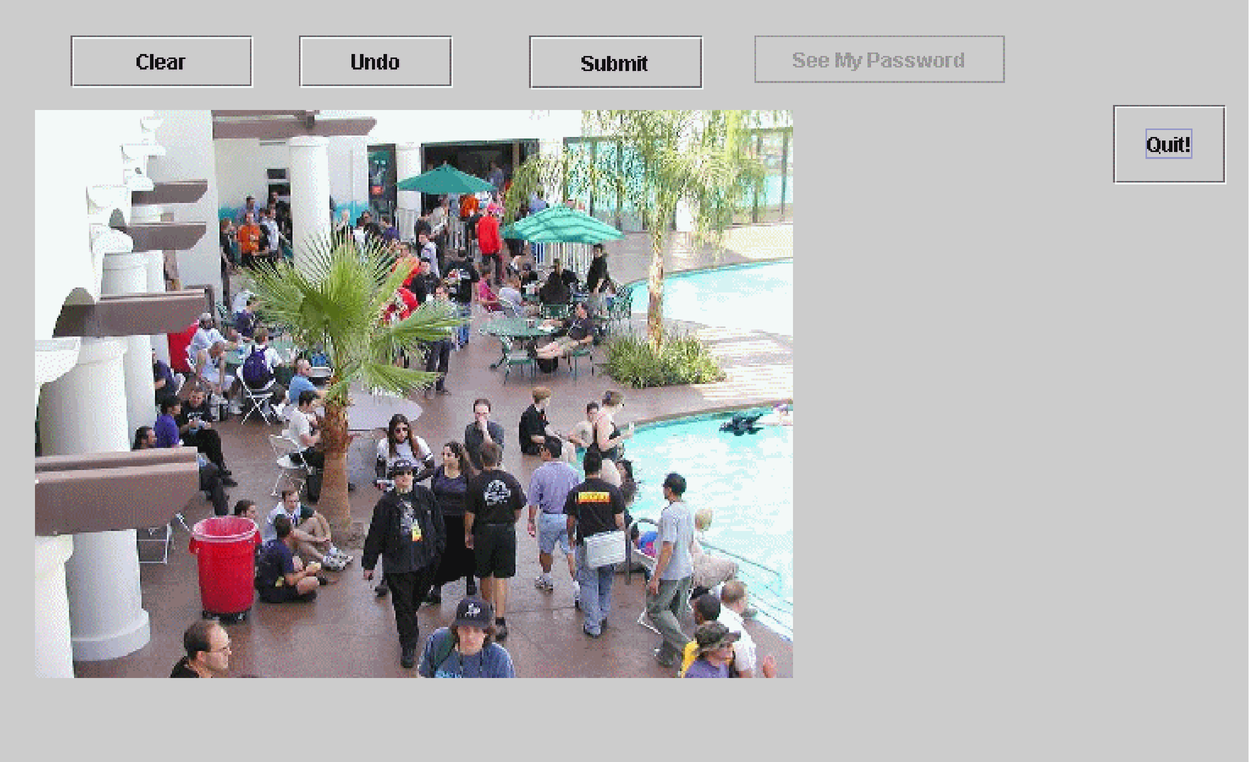

Figure 1. Graphical password interface used in experiment.

4.3 Procedure

A single PC with a high resolution 19 inch monitor was used in the experiment. Testing was done individually. Participants were randomly assigned to the graphical or alphanumeric condition. Each individual participated in three sessions. The first session lasted about 35 minutes. First, the participants were explained the procedures of the experiment Then they chose a graphical password, given instructions on the screen. Graphical password users had to select and enter five distinct points on the picture with no point within the tolerance around any other chosen point. They were told that they would have to remember the points and the order in which they were input. Alphanumeric users had to enter eight characters including at least one upper case letter and one digit. They were also told not to choose a password they had already used. The system enforced that the participants re-enter the password until they chose a valid password. A graphical password of 5 points was used based on our analysis (Wiedenbeck et al., 2005), which shows that in terms of security 5 click points provide a password space as large as or larger than an alphanumeric password of 8 characters. When the participant had created a valid password, the password was displayed as feedback to the participant before going on to the next phase.

In the learning phase the participants entered the password repeatedly until they achieved ten correct password inputs. They received binary feedback on the correctness of each password input. If at any time during the practice participants were not able to remember the password, they could click on Show My Password. After the learning phase, the participant filled out the questionnaire online. This was designed to gather user perceptions and act as a distractor between the learning phase and the first retention trial.

In the retention phase, password retention was measured longitudinally three times: at the end of the first session (R1), one week later (R2), and four weeks later (R3). In these retention trials the participants had only to enter their passwords correctly one time. If the participant entered an incorrect password, the system instructed the participant to re-enter the password. If the participant failed to input the password correctly after four attempts, the Show My Password button was enabled and the participant could view the password, then make another attempt. After the last retention trial, R3, the user again filled out a questionnaire as in the first session and wrote answers to five open-ended questions.

5 Results

Here we report the quantitative result on the password learning and retention phases. We do not report results from the surveys of user perceptions.

5.1 Learning the Password

After choosing a password, participants practiced their password in the learning phase. The criterion for success was 10 correct logins. The participants continued to input the password until the criterion was met. We measured the number of incorrect password submissions and the total time spent in practice. Table 1 shows the means and standard deviations.

Table 1. Means (standard deviations) of number of incorrect submissions and total practice time in the learning phase (alphanumeric N=20/graphical N=20)

	Mode	Mean (SD)
Number of incorrect submissions	Alphanumeric	0.40 (0.68)
	Graphical	4.80 (7.16)
Total practice time (seconds)	Alphanumeric	66.08 (4.92)
	Graphical	171.89 (24.46)

T-tests were used for the analyses. There were significant differences favoring the alphanumeric group in both the number of incorrect inputs t(38)=-.2.73, p<.013 and total practice time t(38)=-4.24, p<.0001. Graphical participants had much more variability in their practice (Table 2). Of the 20 alphanumeric participants 14 had no incorrect inputs, 4 had one incorrect input, and 2 had two incorrect inputs. In the graphical group 8 had no incorrect inputs, 4 had one incorrect input, and 1 had two incorrect inputs. Four of the graphical participants had rather extreme scores with 17 to 20 incorrect inputs. We reanalyzed the date removing these three outliers and found that difference in the number of incorrect inputs was not significant between the alphanumeric and graphical groups (t(34)=-1.85, p<.113).

Table 2. Number of participants making incorrect password submissions in the learning phase.

	Number of Incorrect Submissions								
	0	1	2	3	6	9	17	18	20
Alphanumeric	14	4	2						
Graphical	8	4	1	1	1	1	2	1	1

5.2 Remembering the Password

In the retention phase participants input the password longitudinally three times. In each retention trial the participants had to enter their password correctly only one time. The number of incorrect password submissions and time for the correct submission are shown below (Table 3).

Table 3. Means (standard deviations) of number of incorrect password submissions and time for the correct submission (alphanumeric N=20/graphical N=20)

	Mode	Mean R1 (SD)	Mean R2 (SD)	Mean R3 (SD)
Number of incorrect submissions	Alphanumeric	0.25 (0.79)	2.20 (2.73)	1.75 (2.47)
	Graphical	1.55 (1.57)	2.75 (3.88)	1.50 (2.80)
Time for correct submission (seconds)	Alphanumeric	5.23 (1.66)	9.42 (3.70)	9.24 (3.72)
	Graphical	8.78 (4.40)	24.25 (15.21)	19.38 (17.57)

Two-way, mixed model ANOVAs was used for the analyses of the two measures. The within-subjects factor was retention trial (R1/R2/R3) and the between-subjects factor was mode (alphanumeric/graphical). For the number of incorrect submissions, the effect of retention trial was significant (F(2,76)=6.907, p<.002). The effect of mode was not significant, and likewise the interaction between retention trial and mode also was not significant. A post hoc Tukey's HSD test for specific differences between the retention trials showed that the only significant difference was between R1 and R2 (p<.001), with R1 taking fewer trials than R2. Figure 2 below shows the number of participants who failed to submit a valid password on their first attempt for each retention trial.

We also measured the number of participants who failed to "log in" by the criterion of allowing a maximum of four attempts (Table 4). This measure was introduced because many password systems limit how many successive attempts a person is allowed to make. Participants who had not succeeded after four attempts were considered to have "failed" by this real-world criterion. In fact, we allowed them to continue to try to log in, but we enabled the See My Password button after four failed attempts.

In the analysis of the total time for the *correct* submission, the effect of retention trial was significant (F(2,76)= 21.67, p<.0001). The effect of mode was significant as well (1,38)=39.24, p<.04001). There was a significant interaction between retention trial and mode (F(2,76)=6.67, p<.004). Tukey's HSD showed that there were significant differences between R1 and R2 and between R1 and R3, but no significant difference between R2 and R3. A post hoc Newman-Keul's test for the interaction indicated that in the R2 trial the graphical time was significantly different from all other conditions (p<.05).

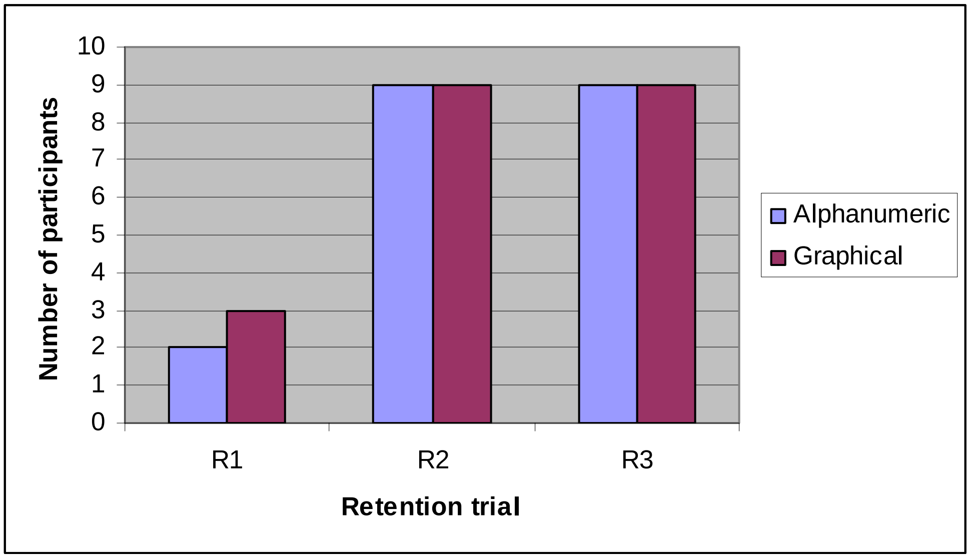

Figure 2. Number of participants who failed to enter their password on their first attempt.

Table 4. Number of participants by retention trial who failed to submit a correct password after four attempts

	R1	R2	R2
Alphanumeric		7	5
Graphical	1	6	3

6 Discussion

A major advantage of PassPoints is its large password space over alphanumeric passwords. The large password space is significant because it reduces the ”guessability” of passwords. Similarly, PassPoints has an advantage in password space over Blonder-style graphical passwords and recognition-based graphical password. But human usability is also an essential consideration. Our human factors testing of the PassPoints system in comparison to alphanumeric passwords yielded somewhat mixed results.

In the learning phase the alphanumeric group took fewer trials to achieve 10 correct password inputs than did the graphical group. This is also reflected in significantly longer total times to input the graphical passwords. Seventy percent of the alphanumeric participants input the password 10 times without any errors, and all alphanumeric participants were able to achieve the criterion with a maximum of two incorrect password inputs. The graphical group took more trials and had more variability. Forty percent of graphical participants achieved input of the password 10 times without any errors, and 70 percent achieved the criterion with a maximum of three incorrect password inputs. Surprisingly, the least successful twenty percent of the group made between 17 and 20 incorrect password inputs. However. It should be clearly noted that most graphical participants did not have serious problems in the learning phase.

We do not consider it a negative outcome that the graphical group made more errors that the alphanumeric group in learning. The graphical participants were using a new password system, completely unknown to them, for their first time. Understanding the password system and how to use it effectively took them time. Indeed, several participants in the graphical password group had significant difficulties in meeting the learning criterion. These participants may have had various problems, e.g., hand-eye coordination, lack of attention to precision in clicking, or poor choice of their graphical password. Whatever the reason for the long trails of incorrect practices, it should be recognized that the alphanumeric group had no equivalent challenges, given their long familiarity and use of alphanumeric passwords.

The most common problem in graphical password input was clicking outside the tolerance around the user's click point. Participants were often close to, but outside, the tolerance. Although at the end of the creation phase they viewed their click points with the tolerance outlined on the image, participants still had difficulty being as precise as required. The participants input their points slowly, so we believe this was not the result of lack of care in input. Rather, it appears that in password creation participants focused on the general area around their click point rather than the precise point. Thus, we believe that this was a memory problem. Graphical password users had to understand how much precision was needed to be successful and then train themselves to remember the password accordingly. For example, they might have needed to remember a password point as "the seat of the chair" rather than simply "the chair."

In the retention phase, the correctness of password inputs differed by trial for both groups. Since the R1 trial took place in the same session as the creation and learning phases, there were few bad inputs. In the R2 trial participants had more difficulty recalling their passwords, regardless of which group they were in. In the final R3 trial there appears to have been some consolidation of the passwords in memory because the incorrect inputs were lower than in R2 (though not significantly) in spite of the long time lapse. The lack of significant differences between the alphanumeric and graphical modes on the correctness of password inputs and lack of interactions between mode and trial, indicate that the main factor in correctness was password memory for both groups. It is encouraging that the graphical group was as to do as well or better than the graphical group, in their first experience with remembering graphical passwords.

The time for the correct input of the password showed that the alphanumeric group was faster in all three retention trials. We expected a longer input time for the graphical group based on the time for mouse movement and selection of the target (Fitts, 1954). However, the large difference between the two groups points to a conclusion that the time difference was mostly a result of think time to locate the correct click region and determine precisely where to click in it. Among the three sessions, the fastest input was in R1, a result that was expected and reflected the high correctness of inputs in R1. It is interesting to note that in R1 the difference in input times of the alphanumeric and graphical groups were not very large, about 3.5 seconds longer in the graphical group. This outcome was achieved with graphical participants who were certainly not automated in the graphical input process. This suggests that with highly skilled users the input time will not be much longer than alphanumeric input times. The increased time for the correct password input in R2 and R3 was quite elevated over R1 for both alphanumeric and graphical groups. This shows the effect of intermittent use on memory for passwords. In addition, the graphical group in R2 was by far the slowest, indicating that participants proceeded slowly and carefully to ensure correct recall and input. Interestingly, in the graphical group, the R3 trial at the end of five weeks was a bit faster (though not significantly) than the R2 trial. This may mean that the graphical participants were becoming familiar enough with their graphical passwords and input procedures to work more quickly.

7 Conclusion

The empirical testing of PassPoints indicates strengths and weaknesses, but is overall encouraging. Graphical users' retention of their password over five weeks was similar to alphanumeric users, perhaps even a bit better, This result is notable because it was achieved in very intermittent use and with very little experience with graphical passwords. In practice users of graphical passwords may exceed alphanumeric password users, given more experience with graphical passwords and the opportunity to use their graphical passwords regularly for some period of time. While graphical users always took more time to input their passwords than alphanumeric users, even so there was evidence that with continuous use graphical passwords can be entered quite quickly.

This work focused on the usability of PassPoints, but its security is also an important issue. PassPoints seems to hold out the prospect of a much more secure system. It is easy to obtain large passwords spaces. Furthermore, in our experiment it appears that users rarely chose points that were within the tolerance around the click point of another participant. That is, people were not strongly drawn to a few salient areas that an attacker might guess. Finally, there is currently no efficient way of creating dictionary attacks against the system. These observations point to further study of the security and usability of PassPoints. From the viewpoint of security, we plan to study the potential for new kinds of dictionary attacks against graphical passwords. For example, edge detection techniques might be used to find out whether graphical passwords can be attacked by exploiting orderly ways in which users choose passwords on an image. From the viewpoint of usability, we are interested in determining the effect of the particular image used on success with graphical passwords, studying users' speed in skilled performance, and discovering what kinds of insecure password practices users invent for graphical passwords.

8 Acknowledgments

This work was supported in part by NSF grants CCR-0310490, CCR-0310793, and CCR-0310159.

9 References

Adams, A. and Sasse, M.A. (1999). Users are not the enemy. *Communications of the ACM* 42, 12, 41-46.

Birget, J.C., Hong, D., and Memon, N. (2003). Robust discretization, with an application to graphical passwords. Cryptology ePrint Archive. http://eprint.iacr.org/2003/168 accessed January 17, 2005.

Blonder, G.E. (1996). Graphical Passwords. United States Patent 5559961.

Boroditsky, M. Passlogix password schemes. http://www.passlogix.com, accessed December 2, 2002.

Brostoff, S. and Sasse, M.A. (2000). Are Passfaces more usable than passwords: A field trial investigation. In McDonald S., et al. (Eds.), *People and Computers XIV - Usability or Else, Proceedings of HCI 2000*, Springer, pp. 405-424.

Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology*, 18, 641-651.

Dhamija, R. and Perrig, A. (2000). Déjà Vu: User study using images for authentication. In *Ninth Usenix Security Symposium*.

Fitts, P.M. (1954). The information capacity of the human motor system in controlling amplitude of movement. *Journal of Experimental Psychology*, 47, 381-391.

Mandler, J.M. and Ritchey, G.H. (1977). Long-term memory for pictures. *Journal of Experimental Psychology: Human Learning and Memory*, 3, 386-396.

Morris, R. and Thompson, K. (1979). Password security: A case study. *Communications of the ACM*, 22, 594-597.

Norman, D.A. (1988). The Design of Everyday Things. Basic Books, New York.

Paivio, A., Rogers, T.B., and Smythe, P.C. (1976) Why are pictures easier to recall then words? *Psychonomic Science*, 11(4), 137-138.

Patrick, A. S., Long, A. C., and Flinn, S. (2003). HCI and security systems. In *Proc. CHI 2004*, ACM Press, 1056-1057.

Real User Corporation. (2001). The science behind Passfaces. http://www.realusers.com. Accessed: Dec. 2. 2002.

Rundus, D. J. (1971). Analysis of rehearsal processes in free recall.. *Journal of Experimental Psychology*, 89, 63-77.

Sasse, M. A., Brostoff, S. and Weirich, D. (2001). Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. *BT Technical Journal*, 19, 122-131.

Shepard, R.N. (1967). Recognition memory for words, sentences, and pictures. *Journal of Verbal Learning and Verbal Behavior*, 6, 156-163.

Standing, L.P (1973). Learning 10,000 pictures. *Quarterly Journal of Experimental Psychology*, 25, 207-222.

Wiedenbeck, S., Waters, J., Birget, J.C., Broditskiy, A., & Memon, N. (2005). PassPoints: Design and evaluation of a graphical password system. Submitted.

Wixted, J. T. (2004). The psychology and neuroscience of forgetting. *Annual Review of Psychology*, 55, 235-269.