Pictures at the ATM: Exploring the usability of multiple graphical passwords

Wendy Moncur
Department of Computing Science
University of Aberdeen
Aberdeen
wmoncur@csd.abdn.ac.uk

Grégory Leplâtre
School of Computing
Napier University
Edinburgh
g.leplatre@napier.ac.uk

ABSTRACT
Users gain access to cash, confidential information and services at Automated Teller Machines (ATMs) via an authentication process involving a Personal Identification Number (PIN). These users frequently have many different PINs, and fail to remember them without recourse to insecure behaviours. This is not a failing of users. It is a usability failing in the ATM authentication mechanism.

This paper describes research executed to evaluate whether users find multiple graphical passwords more memorable than multiple PINs. The research also investigates the success of two memory augmentation strategies in increasing memorability of graphical passwords. The results demonstrate that multiple graphical passwords are substantially more effective than multiple PIN numbers. Memorability is further improved by the use of mnemonics to aid their recall.

This study will be of interest to HCI practitioners and information security researchers exploring approaches to usable security.

Author Keywords
Usable security, user authentication, graphical passwords, ATMs, authentication mechanisms.

ACM Classification Keywords
H5.2. Information interfaces and presentation (e.g., HCI): Graphical User Interfaces, Interaction styles, Screen design, User-centred design.

K6.5. Computing milieux: Security and protection – Authentication.

INTRODUCTION

Secure user authentication at ATMs is delivered through a combination of a token and a knowledge-based password unique to an individual and an account. The 'token' is a bank card, the 'knowledge-based password' is a four-digit password commonly known as a PIN (Personal Identification Number). Yet the latter part of this authentication mechanism is unsatisfactory: PINs are easily forgotten [12]. Users circumvent this forgetfulness through insecure behaviors. Subverting security, they write down their PINs, make them all the same, or disclose them to friends and family [1]. Security administrators may blame the user, yet in reality authentication at the ATM is paying the price of disregarding usability needs [14].

Awareness is emerging of the need to design authentication with usability in mind [11]. Usable security is a growing field of research, with interest developing in both replacing and augmenting knowledge-based passwords. Options include biometrics, personalisation and behaviour, and graphical passwords. This paper focuses on graphical passwords. Findings from earlier research have indicated that graphical passwords offer greater usability, and potentially greater security, than knowledge-based passwords [5]. However, as previous studies have pointed out [2, 5, 12], a critical issue regarding the use of passwords remains to be addressed: bank customers typically need to remember several PIN numbers. Although the merits of graphical passwords have been established, there is no indication that these merits scale up as the number of passwords increase. Retention of PINs and graphical passwords involve distinct strategies, and the effect of their multiplication is unknown. This paper addresses this issue, and provides answers to the following questions: can people remember multiple graphical passwords successfully, and what can improve that memorability? Existing usability flaws in Western knowledge-based authentication systems are described, and current graphical authentication alternatives reviewed. There follows a description of the research undertaken and a discussion of the results. Conclusions are drawn and further work that could appropriately be carried out is identified.

BACKGROUND

Password usability: What's the problem?

Usable security is a field in its infancy [4, 11]. Although nascent considerations for usability appear to conflict with security requirements, it is argued that it is the very lack of consideration for usability which undermines current mechanisms [14, 15].

CHI 2007, April 28–May 3, 2007, San Jose, California, USA.

For an authentication mechanism to be secure, it must be undisclosed, abundant and predictable [13]. The security of a password can be rated for the ability of a potentially malign user to observe the code (observability), guess the code (guessability) and record the code (recordability) [5].

Legitimate users can find the knowledge-based passwords that are foisted on them unusable [1, 6]. They have difficulty remembering strong syntactic passwords, succeeding only 35% of the time [21]. To cope, they undermine security by adopting insecure, apparently careless, behaviors [20]. In addition, users allow their passwords to be observed [11]. Up to 50% of them create weak, guessable passwords and record them in obvious places [1]. Contrastingly, part of the success of malign users can be attributed to the attention that they pay to legitimate users and their behavior [1].

By incorporating usability considerations in security requirements from system inception, it is suggested that users are more likely to adopt desirable secure behaviors.

Exploiting memory through graphical authentication

One option in the search for increased usability is the employment of graphical passwords for authentication. The approach exploits the understanding that people remember images far better than words – an ability sometimes referred to as the "Picture Superiority Effect" [5, 10]. Individuals can remember more images, more accurately, and with less adverse effects from ageing in comparison to semantic or syntactic items.

An added attraction of graphical passwords is that they offer less recordability, as they are harder to disclose than knowledge-based passwords such as PINs, semantic and syntactic passwords [5]. A disadvantage is that user-driven graphical password selection is more protracted than choosing a knowledge-based password, thus potentially increasing observability [6, 12]. This disadvantage can be circumvented by assigning the password automatically, consequently also avoiding predictability problems [5].

Although graphical authentication is a markedly immature area, three dominant techniques have emerged that seek to replace knowledge-based passwords [16]. These techniques can be defined as "locimetric", "drawmetric" and "cognometric" [5]. In addition, techniques have been developed to augment knowledge-based passwords [13].

Locimetric systems

The locimetric approach exploits mnemonic systems of memorisation and cued recall. Originating in Blonder's work, the approach involves users touching a series of pre-defined points on an image, in a pre-defined order [16]. The approach has some weaknesses when considered against criteria of observability, guessability and recordability. According to a study by Wiedenbeck and colleagues', if users create their own locimetric password, there is a tendency for the password to be predictable, and thus insecure. 'Obvious' points in the picture with high visual salience are chosen [19]. Password entry is slow compared to PINs, and a high degree of accuracy is required in selecting the correct points to click on [19]. In the aforementioned study, training and practice were needed to assist users in successful password entry.

Drawmetric systems

This approach involves users initially drawing a simple outline on a grid. Authentication consists of redrawing this picture. Position, sequence and visual appearance are analyzed for a match with the original [5, 8]. However, the approach has not met with success. While users could remember what their 'doodle' looked like, they could not recreate it accurately, or with the correct stroke sequence.

Cognometric systems

Cognometric systems display images to the user, who must identify which are the 'target' images amongst a set of redundant 'distractor' images [5]. The use of artist-drawn images, computer-generated abstract images and photographs has been explored within this approach. The strength of the cognometric approach lies in the exploitation of recognition rather than recall, through the Picture Superiority Effect [5]. Its weakness lies in its poor usability for those with impaired vision.

Artist-drawn images are used by the commercial product "PicturePIN" by Pointsec. Users are invited to create a short story around target images and their order, thus deploying mnemonics as a memory strategy to augment recall. Research into the memorability of the artist-drawn images is currently limited and unsatisfactory [18].

Computer-generated abstract images were evaluated in the 'Déjà Vu' study (see Figure 1). Memorability for abstract images was found to be only half as good as that for photographic images with a clear central subject [6,18]. Personal photos had the highest levels of memorability, but they were also predictable, and therefore not good candidates for secure password systems [17].

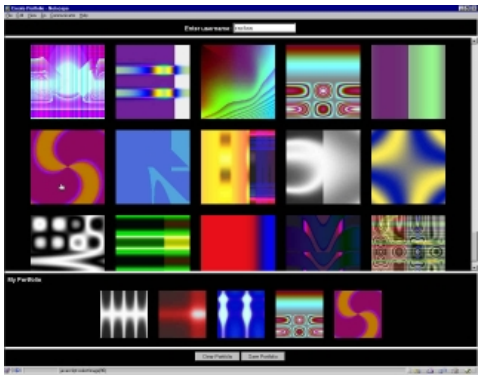

Figure 1. Screenshot of the Déjà Vu interface

The usefulness of photographic images was further explored in the VIP project, which applied the cognometric approach to ATM authentication [5]. Graphical passwords consisting of detailed, colorful, meaningful photographic images were assigned to users. Showing semantically similar images caused confusion, known as memory interference [5]. Problems with memory interference were subsequently avoided by defining semantic categories, and only ever assigning and displaying one image from any one category. The greatest success for VIP was achieved with the approach that demanded pure recognition from users. The position of the component images in a graphical password were not static, thus preventing recourse to kinaesthetic cues (remembering a pattern of physical actions involved in selecting a password) or spatial coding (recognizing the physical position of an image, rather than the image itself). The error rate for authentication was 11%, compared to 27% for standard PIN authentication, and 24% for a cognometric approach that used a mixture of recognition and recall [5]. It appears that the Picture Superiority Effect may have advantages for authentication if exploited in isolation.

The research described within this paper seeks to extend the work of the VIP project, by exploring the effect of *multiple* graphical passwords on memorability.

STUDY

Can VIP's cognometric approach be equally successful when users are required to recall multiple passwords? How many distinct passwords can be successfully recalled using graphical passwords?

It was decided to allocate five passwords to each participant, and test retention over a four week period. The number of passwords was based on the average number of bank cards for a sample set of users canvassed, as the existing literature does not suggest how many passwords it takes to challenge users' retention abilities. Less than five could have have proved a trivial task for users. Allocating a very large number of passwords would not have been realistic: passwords are seldom provided in bulk, and do not usually have to be assimilated all at the same time

In addition to comparing the retention of multiple PINs to that of multiple graphical passwords, two factors were added to the experiment, in an attempt to learn more about the graphical password retention process.

Previous studies by De Angeli *et al.,* [5] and Yan *et al.,* [21] have demonstrated that the use of a mnemonic can aid recall. For example, a graphical password containing pictures of a cat, a house, a sunflower and a bread roll could be remembered as:

> *"The cat left its house, smelt the sunflower, and then ate a bread roll".*

The effectiveness of color as an additional recall cue was also investigated in this experiment. It was decided that some graphical passwords would be displayed against a specific background color. Such a feature may be of value for banks who could allocate their own color to their passwords (e.g. - blue background for Bank 1, purple for Bank 2). Although it seems reasonable to presume that this cue would represent a valuable memory aid, the background color may conversely not constitute a salient enough feature to augment the password images.

As a result, a comparative longitudinal user study was conducted online using an experimental, fixed, post-test factorial design to test the following hypotheses:

- H1: Multiple graphical passwords are more memorable than multiple PIN numbers.
- H2: Memorability of multiple graphical passwords can be improved by using a mnemonic to aid recall
- H3: Memorability of multiple graphical passwords can be improved by showing password and distractor images against a signature colored background.

Methodology

A total of 172 participants volunteered to take part in the study by responding to an email sent to university staff and student distribution lists.

Group	Password mechanism
0	Control group using a 4 digit PIN number to reflect the existing PIN mechanism employed at ATMs.
1	Graphical passwords
2	Graphical passwords with signature color background to graphical images to augment memorability
3	Graphical passwords with mnemonic strategy to augment memorability
4	Graphical passwords with mnemonic strategy and colour background to augment memorability

Table 1. Password mechanism by group

Participants were assigned to one of five experimental groups as presented in Table 1. The allocation was made randomly by the system. Each participant was subsequently allocated five passwords by the system according to their group. As in the VIP study cited earlier [5], for all groups except the control group, each password was made up of four detailed, colorful, meaningful photographic images from separate semantic categories, allocated at random. Members of the control group were allocated five passwords each comprising four randomly selected digits.

The retention tests used in the study involved challenge sets containing ten components – images for Groups 1, 2, 3 and 4, and digits for Group 0. The four components forming a password were displayed along with six distractor components. The distractor images were also selected at random, one from each of the unused semantic image categories for each iteration of the test. In the case of Group 0, the six unused digits were used as the distractor

components. The position of the password components amongst the distractor components was randomly generated for each iteration of the password test. A sample challenge set for a graphical password is presented on Figure 2.

Figure 2. Example graphical password selection screen representing a challenge set

The PIN selection interface looked the same, and had the same mechanism for choosing password components, as the graphical password selection interface, thus delivering internal physical and graphical consistency [9]. The PIN selection screen is illustrated by Figure 3.

Procedure

a) Three retention tests (RT1, RT2 and RT3) were carried out with a gap of two weeks between each of them, producing a total duration of four weeks for the longitudinal test.

b) All participants undertook a training session, entering each of their assigned passwords correctly twice. This was a smaller amount of rehearsal than that carried out in other studies, which used up to ten rehearsals per password [5]. Although rehearsal has been proven to increase retention of passwords [14], there was believed to be a risk of participant attrition from the study if the total training involved 50 rehearsals in a session (5 passwords * 10 rehearsals), due to the voluntary nature of participation. Unlike the VIP study, participants were not paid to take part.

c) The number of permitted retries for any password was limited to three, to replicate existing PIN mechanisms [2]. After a third failed login, the participant was automatically reminded of their password. During the training phase, they were then able to practice correct submission of their password again.

d) During the retention phases, participants progressed to the next password after three failed attempts.

Figure 3. Example numerical password selection screen

In Week 0, participants completed a questionnaire to extract quantitative demographic data, and establish their existing experiences, behaviors and views with respect to using passwords at the ATM. Finally, after RT3, participants completed a second questionnaire, to ascertain the strategies they had used to recall their passwords.

Measures of effectiveness.

Effectiveness of password memorability was measured as the proportion of participants who remembered their passwords correctly. Details of both successful and unsuccessful password selections made by participants during training and retention sessions were also captured. Individual password component choices were recorded. Subjective data was collected through questionnaires issued at the beginning and end of the study.

Results

Demographics

Of the participants who completed the study (see Dropout rate section, below), 27 were male and 33 were female. They were predominantly educated to university degree level or above (81.67%). The age distribution is illustrated by Figure 4.

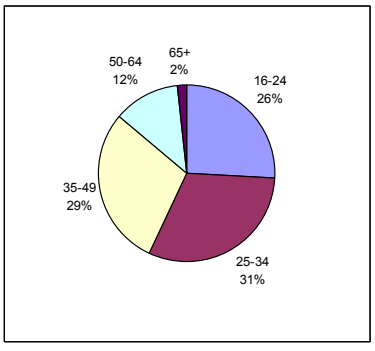

Figure 4. Age Range of Participants

Dropout rate

The first indicator of the memorability of the various password types is provided by the dropout rate in each group (Table 2).

The overall dropout rate for the experiment was high at 64.91%. This can be explained by three main factors.

- The time-consuming nature of the task put off a lot of participants. To complete the study, participants had to enter five different passwords on five occasions (two rehearsals plus three tests), as well as completing two detailed questionnaires and five distractor tasks.
- Participants were not paid to take part in the study. Participation was voluntary, with little incentive to complete the study. This in contrast to the longitudinal VIP study, where participants were paid (De Angeli et al, 2005).
- Many of the participants were students. The study ran over the university exam period, when the study would not have been their top priority.

The second main finding is the higher dropout rate for Group 0, who had been allocated PINs (76%), which provides a first indication that H1 may be verified. However the dropout rate differences were found not to be significant ($\chi^2 = 1.34$, df = 4. p >0.05). Nonetheless, Group 0 was the only group for which unsolicited feedback indicated that some participants found the task impossible, even during the training phase.

It must also be noted that one participant who completed the study was excluded from analysis of results because of their non-compliance. They admitted to writing down the story which they had invented, to aid recall of their graphical password. The results presented in the following sections involve the data collected from participants who completed the study.

Group Code	Participants enrolled	Participants completed	Dropout rate %
0	29	7	75.86
1	37	16	56.76
2	30	10	66.67
3	38	14	63.16
4	38	14	63.16
total	**172**	**61**	**64.91**

Table 2. Dropout rates

Analysis methodology

Given the chosen experimental protocol, one may have expected to carry out a two way ANOVA analysis with replication. However, the difference in participant numbers between groups and the very high dropout rates made this type of analysis problematic; consequently, the statistic of choice in this analysis was the password retention rate. Chi-squared tests were used to establish whether the differences observed were significant or not.

Retention rates – differences between groups

As Figure 5 illustrates, differences between groups can be observed to various degrees. An overall test on the five groups showed a very acute overall difference between the average retention rates of each group ($\chi^2 = 51.13$, df = 4. p < 0.001). Further tests revealed a significant difference between Group 0 and Group 1 ($\chi^2 = 25.6$, df = 1. p < 0.01). This demonstrates that graphical passwords were remembered more effectively than PINs and validates H1.

The difference of retention between Group 1 and Group 3 was significant ($\chi^2 = 8.66$, df = 1. p < 0.01). This proves that using mnemonic strategies improved the retention of the five passwords and validates H2.

Other differences between groups did not all appear to be substantial on Figure 5. The overall difference of retention between Group 1 and Group 2 approached but did not reach a significant level ($\chi^2 = 2.80$, df = 1. p > 0.05). Therefore, the addition of a background color to the graphical passwords did not improve retention, which disproves H3.

Interestingly, Figure 5 seems to indicate that retention in Group 3 was superior to retention in Group 4, suggesting that the addition of a colored background could be detrimental to password retention. However, this difference was not significant either ($\chi^2 = 1.42$, df = 1. p > 0.05).

Retention rates – evolution over time

Figure 5 clearly shows a large difference between the retention tests conducted in Week 0 (immediately after the passwords were supplied to participants) and subsequent tests, conducted in Weeks 2 and 4. A Chi square test confirmed that there was an overall effect of time on retention performance ($\chi^2 = 440$, df = 2. p < 0.001). As suggested by Figure 5, the difference of performance between RT1 and RT2 was extremely significant ($\chi^2 = 338$, df = 1. p < 0.001).

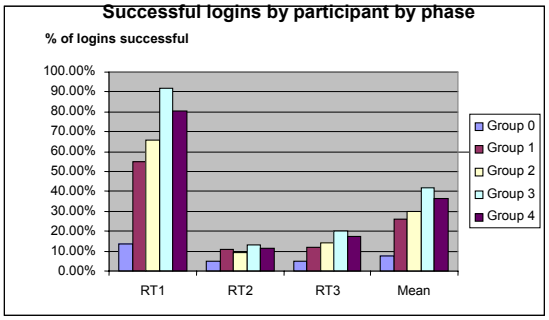

Figure 5. Password retention rates

Interestingly, the performance seemed to have improved from RT2 (Week 2) to RT3 (Week 4) for all groups. This trend also proved significant ($\chi^2 = 5.24$, df = 1. $p < 0.01$).

The considerable difference of performance between RT1 and RT2 can be explained by the fact that RT1 involved short-term memory while RT2 did not. The improvement in retention between RT2 and RT3 cannot be explained so easily. One can only suggest that, once the short-term memory effect disappeared, RT2 acted as a training stage which helped reinforcing the long term memorability of the passwords.

Errors

To understand the factors that caused the password retention failures, the data for each erroneous password entry for each group was further analyzed. An erroneous password could involve either of the three following error:

- *Order confusion*: correct components selected, but wrong order.
- Component selected twice (will be referred to as *double click*).
- *Wrong component*(s) selected (but no double click).

Figure 6 illustrates the different types of error triggered by the different types of password. Errors made in graphical password selections were predominantly due to order confusion. In Group 3 (graphical password with mnemonic), order confusion represented over 70% of all errors made. Conversely, PINs were more prone to selection of the wrong component. This illustrates that participants were far more likely to remember the components of their numerous passwords if they were graphical rather than numeric. Feedback received from participants reflects this.

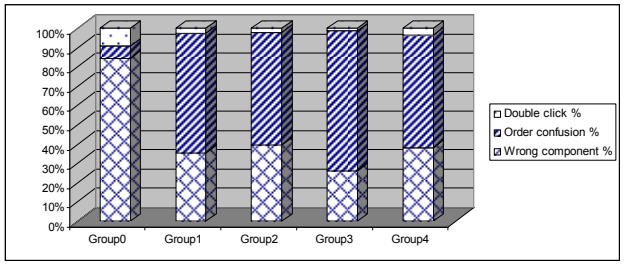

Figure 6. Types of errors committed by each group

This result implies that the retention of multiple graphical passwords could be increased *substantially* by allowing users to choose the components of their password in any order. This usability would however come at a cost: reduced security of the system.

Retention strategies

During the design of the experiment, the potential was noted for participants to deliberately or inadvertently adopt an alternate memory strategy to the one that they were instructed to use. The debriefing questionnaire revealed that adoption of alternate strategies remained limited. Overall, 57% of participants gave details of the strategy they used to remember their passwords. The three generic strategies deployed are illustrated in Figure 7. Strategies for graphical passwords were different to those for PINs. Strategies for PINs involved visualization and speaking the numbers aloud, categorized as *rehearsal*.

> *"I tried to picture the numbers on the grid on an ATM. I use the picture of the layout and the physical movement involved in pressing the PIN to remember the numbers."*
>
> Feedback from Group 0 participant

For graphical passwords, participants who were instructed to use stories (*mnemonic*) as a memory strategy obeyed (Group 3 and 4, see Figure 7). In Group 1 and 2, participants were not given a memory strategy. Where used, the strategies deployed were diverse: making up a story (*mnemonic*), word and event association (*elaborative rehearsal*), naming the images aloud (*rehearsal*). Those who used a mnemonic strategy consistently reported order confusion:

> *"I tried to make up stories that helped for remembering the images, but made it perhaps even more tricky to get the order right."*
>
> Feedback from Group 3 participant

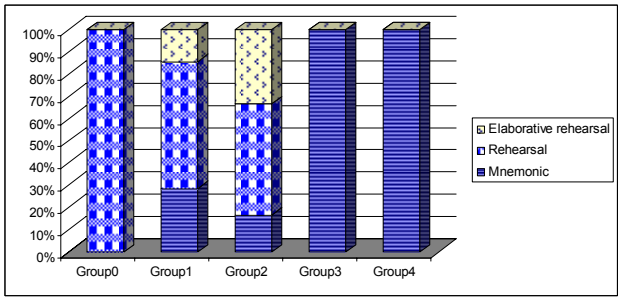

Figure 7. Retention Strategies

Additional results

Attitudinal and behavioral data was captured via questionnaires. Users reported having between 0 and 11 bank and store cards. Consistent with the more extreme findings from earlier studies [1], insecure memory strategies were adopted by 48.33% of participants, to circumvent difficulty in recalling their PINs. Strategies included sharing their PINs with someone else (1.66%), writing down PINs (10%) and, most commonly, having the same PIN for more than one bank card (31.67%). The insecure strategies adopted may explain why the mean number of PINs that people forgot in the past 12 months was so low, at 0.783.

The figure of 1.66% for sharing PINs is dubiously low. Adams and Sasse cited a conservative estimate of 36% of

users disclosing their password [1]. It is possible that participants in this study felt more inclined to admitting insecure behaviors which were less serious, such as writing down their password, rather than the 'heinous crime' of sharing their PINs, as they were taking part in a password study.

Discussion

This study explored three hypotheses relating to the potential for the use of multiple visual codes in authentication mechanisms.

The first hypothesis (H1), that "Multiple graphical passwords are more memorable than multiple PIN numbers", was confirmed. This is in keeping with findings by Suo *et al.*, on single graphical passwords [16]. People remember images far better than words or numbers, through the exploitation of recognition rather than recall that is attributable to the Picture Superiority Effect [5, 10].

The second hypothesis (H2), that "Memorability of multiple graphical passwords can be improved by using a mnemonic to aid recall", was also confirmed. Group 3 tested this hypothesis. This memorability improvement is consistent with findings that recall is easier when distinct items are associated with each other in a special scheme – as they were by using the mnemonic technique [13, 14, 21]. It is suggested that use of a mnemonic strategy complements the Picture Superiority Effect, rather than interfering with it, thus enhancing memorability of graphical passwords further.

The third hypothesis (H3), "Memorability of multiple graphical passwords can be improved by showing password and distractor images against a signature colored background", was not confirmed. It is possible that the strategy did not have the intended effect as participants were not told to take notice of the background colors. In contrast, instructions to use a mnemonic for Groups 3 and 4 were specific. Another possibility is that the soft tones used were inappropriate, and that a deeper intensity of color may give better results. This would be worth exploring. The combination of mnemonic and color did not have any positive effect over the use of mnemonic alone.

All users made mistakes to various degrees. Yet the degree of error for those with graphical passwords was less pronounced. They tended to recognize the right password components, but got them in the wrong order. This reflected findings that pure recognition based systems deliver greater memorability than those requiring recognition and spatial coding [5]. In contrast, those allocated to PINs failed to even recognize their allocated numbers when making an error. This suggests that if password component order were unnecessary, the superior memorability of graphical passwords over PINs would become even more pronounced [6]. The trade-off would be an increase in guessability, one of the measures of (in)security.

It is possible that some password errors can be explained by the lack of kinaesthetic cues offered. It is common for users to remember their password via these cues, as static positioning is the 'norm' for password entry at the ATM [13]. Not only was there no static position for password images, but participants were not warned of this, and some entered passwords erroneously as a result. Although static positioning is undesirable from a security perspective because it increases password guessability, it would have been worthwhile to alert participants to the dynamic nature of the password displays.

It is arguable that the decision to make the authentication for Group 0 (PINs) internally consistent with graphical authentication, rather than externally consistent with current ATM authentication, may have been detrimental to Group 0. The participants were regular users of ATMs, with pre-existing habits relating to entry of their PINs [13]. Faced with a PIN-style entry screen in the study, asked to recall PINs, Group 0 users in particular may have expected external consistency. When digits were not displayed in sequence in static positions as they are at the ATM, confounded expectations may have lead to confusion, raising the level of difficulty of the task for Group 0 [7, 9]. This was illustrated by the use of visualisation as a memory strategy by Group 0 participants, as discussed earlier.

Conclusion

This study has demonstrated that the merits of graphical passwords over PINs identified in previous studies also stand when multiple passwords (five) have to be remembered. A longitudinal study which proved almost impossible to complete using four digit PINs was completed with significantly more success using graphical passwords. Moreover, performance improved when participants used mnemonics to recall their graphical passwords.

This suggests that graphical passwords represent a valuable solution to the usable security problem caused by the multiplication of passwords.

Suggestions for future work

It would be of interest to repeat the study with larger sample sizes. Graphical password studies so far have consistently used small sample sizes, a failing identified by Suo et al [16]. With larger sample sizes, exploratory data analysis could be carried out to look for unexpected patterns. For example, the effects of age and gender on the memorability of graphical passwords could be explored. These two aspects are currently unexplored, although psychology studies suggest that visual memory appears less affected by ageing than knowledge-based recall [3].

Finally, further studies will be required to further assess the merits and drawbacks of this system over substantially longer periods of time. This will require the implementation of a long-term longitudinal study. It is

suggested that most benefit could be drawn from this if the control group using PINs exhibited external, rather than internal, consistency.

ACKNOWLEDGMENTS

We thank Lynne Coventry of NCR for her valuable advice on the current state of graphical authentication research, and Karen Renaud of Glasgow University for supplying some of the images used in the study.

REFERENCES

1. Adams, A., & Sasse, M. (1999). Users are not the enemy. Communications of the ACM, 42(12), 41-46.
2. Brostoff, S., & Sasse, M. A. (2000). Are passfaces more usable than passwords? A field trial investigation. In *Proc. HCI 2000.*
3. Brown, SC. & Park, D.C. (2003) Theoretical models of cognitive aging and implications for translational research in medicine. Gerontologist, 43(1), 57-67.
4. Coventry, L., De Angeli, A., & Johnson, G. (2003). Usability and biometric verification at the ATM interface. In *Proc. CHI 2003.*
5. DeAngeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63(2005), 128-152.
6. Dhamija, R., & Perrig, A. (2000). Deja Vu: a user study using images for authentication. In *Proc.9th USENIX Security Symposium.*
7. Frøkjær, E. & Hornbæk, K. (2002). Metaphors of Human Thinking in HCI: Habit, Stream of Thought, Awareness, Utterance, and Knowing. In *Proc. HF2002/OzCHI 2002*.
8. Goldberg, J., Hagman, J., & Sazawal, V. (2002). Doodling our way to better authentication. In *Proc. CHI 2002.*
9. Grudin, J. (1989). The case against user interface consistency. Communications of the ACM, 32(10), 1164-1173.
10. Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A. (1999). The design and analysis of graphical passwords. *In Proc. 8th USENIX Security Symposium.*
11. Patrick, A. S., Long, A. C., & Flinn, S. (2003). HCI and security systems. In *Proc. CHI '03.*
12. Renaud, K., & De Angeli, A. (2004). My password is here! An investigation into visuo-spatial authentication mechanisms. Interacting with computers, 16(2004), 1017-1041.
13. Renaud, K., & Smith, E. (2001). Jiminy: helping users to remember their passwords. In *Proc. SAICSIT Annual Conference.*
14. Sasse, M., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122-131.
15. Smetters, D. K., & Grinter, R. E. (2002). Moving from the design of usable security technologies to the design of useful secure applications. In *Proc. New Security Paradigms Workshop 2002, 82-89.*
16. Suo, X., Zhu, Y., & Owen, G. (2005). Graphical Passwords: A Survey. In *Proc. ACSAC'05.*
17. Tullis, T. S., & Tedesco, D. P. (2005). Using personal photos as pictorial passwords. In *Proc. CHI 2005.*
18. Weinshall, D., & Kirkpatrick, A. S. (2004). Passwords you'll never forget, but can't recall. In *Proc. CHI 2004.*
19. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005a). Authentication using graphical passwords: effects of tolerance and image choice. In *Proc. SOUPS 2005*.
20. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005b). PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human - Computer Studies.
21. Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2001). The memorability and security of passwords - Some empirical results. (Technical report No. 500). Cambridge: Cambridge University Computer Laboratory.