Is FacePIN Secure and Usable?

Paul Dunphy
School of Computing Science
Newcastle University , UK
(+44)191 2464621
P.M.Dunphy@ncl.ac.uk

Jeff Yan
School of Computing Science
Newcastle University , UK
(+44) 191 222 8010
Jeff.Yan@ncl.ac.uk

ABSTRACT

Personal identification numbers (PINs) and hardware tokens are often used together for authentication purposes, e.g., in financial transactions with ATM machines. However, many people cannot remember their PINs. This has caused insecure practice, extra management cost, or both. In this paper, we evaluate FacePIN, a solution proposed to improve the security and memorability of the PIN scheme.

1. INTRODUCTION

PINs are widely used together with hardware tokens particularly bank cards for authentication. Unfortunately, many people forget their PINs. This causes inconvenience to card holders and extra management cost to card issuers. Moreover, the struggle to remember assigned PINs often leads to insecure practices such as writing them down or sharing them with others as a form of backup. In response to this, some banks then allowed cardholders to choose their own PINs. However, many people select guessable numbers such as the birthdays of loved ones, using the same PIN for each card they have.

To address the above problems, Davies proposed a FacePIN scheme [1] that supplements the current PIN system using the concept that underlies the Passfaces [2] graphical password system, i.e., our innate ability to recognize faces. This system can be applied to any system that requires management of cards and PINs.

For a PIN of *n* digits, FacePIN cards have *n* grids of faces printed on the reverse. The layout of the faces within each grid ideally mirrors the keypad layout of the PIN entry device. Cardholders are then assigned one face in each grid instead of a numeric PIN. To reconstruct a PIN the user must for each grid: recognize their assigned face and select the digit in the corresponding location on the PIN entry keypad. An example of FacePIN where the PIN is comprised of the digits 1-9 can be seen in figure 1.

In this paper, we present our initial work of evaluating security and memorability of the FacePIN scheme. To our best knowledge, this is the first such study independently carried out for this scheme.

Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.

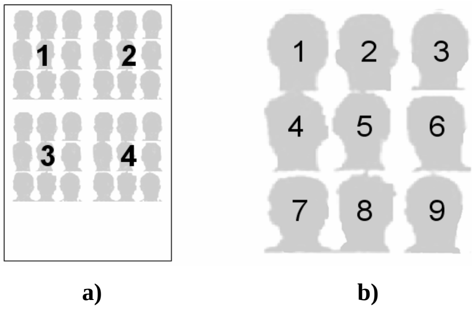

Figure 1. a) The position within the PIN each grid represents b) The mapping between faces and PIN digits

2. RELATED WORK

De Angeli et al [3] proposed three variants of Visual Identification Protocol (VIP) and compared its performance to PIN. VIP is an image selection scheme that replaces the management of numbers with recognition of images. Instead of learning a PIN, users must learn their assigned images and have to recognize them amongst a set of decoys in the correct order. The user study examined 3 flavors of VIP: VIP1 simply replaced the traditional 10 digit numeric keypad with images. VIP2 extended this by randomizing the locations of the keypad images at each login. VIP3 increased the number of decoy images on-screen from 6 to 12. Also the user was assigned a portfolio of 8 images, having to recognize a random subset of 4 at each login.

The memorability performance of all variants exceeded that of PIN; however VIP1 and VIP2 suffer from the same, if not a greater risk of shoulder surfing than PIN. This is mainly due to our increased memory ability for images, and the few number of decoys presented at any one time. VIP3 was the most secure solution; the greater number of decoys increased confusion for the attacker. The cost of a shoulder-surfer viewing an entire login was also reduced in comparison to VIP1 and VIP2.

3. USER STUDY

We conducted a user study to compare the usability of FacePIN to PIN.

The first issue in our experiment design was to choose a layout for the face-grids that would be suitable to represent a PIN comprised of digits 0-9. We decided to keep the 3×3 configuration (as seen in figure 1), maintaining an ATM keypad look and feel, whilst being space-efficient. If a particular PIN digit was zero, no face would be assigned to the user in the corresponding grid.

We created 30 mock credit cards, 15 containing the FacePIN enhancement and 15 without. The faces used were taken from

Passfaces [2] with permission and were the same on each FacePIN card. Then we generated 15 4-digit PINs at random using the digits 0-9. These PINs were used in both groups. We created credit card-sized paper *masks* to reveal the assigned PIN to each participant using the FacePIN scheme.

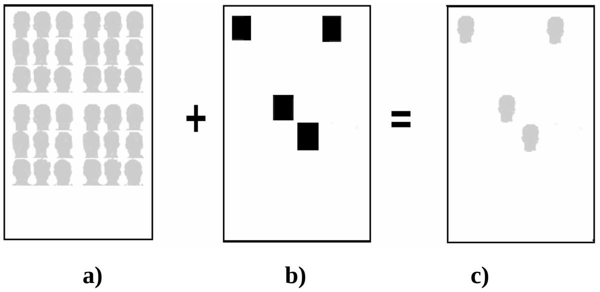

Figure 2. a) The reverse of the credit card, b) the mask and c) Overlaying the card with the mask

We recruited 29 participants (27 male, 2 female), and assigned them randomly into two groups, FacePIN and PIN. To the FacePIN group we distributed the enhanced cards along with a mask representing their assigned PIN (figure 2), and to the PIN group mock cards without the faces. For this group each PIN was distributed on paper. After 10 minutes we collected in both PINs and masks, to give added assurance participants were using their memory alone to reconstruct PINs. We asked the participants to recall their PIN 45 minutes later (a lecture was used as the distraction), 1 week later, and 5 weeks later.

3.1 Results

The results we obtained are displayed in Table 1.

Table 1. FacePIN recall results

		Subjects	Correct	Bad Guesses
45 mins	FacePIN	14	14	0
	PIN	15	15	0
1 week	FacePIN	7	7	0
	PIN	13	13	1
5 weeks	FacePIN	7	7	1
	PIN	15	11	21

In the first recall test all participants in both groups were able to successfully repeat their PIN.

After 1 week we lost exactly half of the FacePIN participants and only 2 from the PIN group. Again all participants were able to repeat their PINs with only one participant in the PIN group requiring more than one attempt.

After 5 weeks FacePIN participants were much more effective at repeating their PINs (only one incorrect guess), and every participant being able to recall their PIN. PIN participants produced 21 incorrect guesses with 4 people unable to provide their PIN at all and being ‘locked out’ of the system. The average number of guesses required by the FacePIN group was 1.17 with a standard deviation of 0.4. The average number of guesses required by the PIN group was 2.13 with a standard deviation of 1.46.

FacePIN and PIN performed in similar ways over the period of one week. However over a longer period, the cued-recall of FacePIN enabled users to considerably out-perform their PIN counterparts. One limitation of the study was that participant turnout in the FacePIN group was half that in the PIN group in the second and third recall tests.

3.2 Security issues

Unlike VIP [3], FacePIN is not a replacement of PINs, but a supplement to increase their memorability and security. As such, any vulnerabilities of PIN still apply. FacePIN does not impact security as the faces do not communicate the cardholder’s PIN to anyone but the legitimate cardholder who has been through the enrolment phase using the mask. Vulnerability would arise if users distinguished their assigned faces on the card using a pen, effectively writing their PIN down.

As FacePIN can function in a customizable PIN mode, cardholders could select their PIN based on a special number they have in mind, or be influenced by the faces on their card. In the case of the latter, FacePIN could be subjected the “Race effect” discussed by Davis and Monrose [4]. In the former case, FacePIN could suffer from the same poor user choice as suffered by PIN. The best solution would be to assign the user a random PIN and use FacePIN to make this memorable.

4. SUMMARY & FUTURE WORK

Our user study suggests that FacePIN is indeed more effective than the PIN scheme. More studies are planned for understanding whether FacePIN will eventually provide a usable and secure PIN solution.

For example, interesting issues arise when considering the *interference* from managing more then one FacePIN card, with a distinct PIN for each. We suspect that a distinct set of faces must be used on every card, from usability rather than a security perspective. Confusion would be inevitable if cardholders had to remember a certain face on one card, but remember to ignore it on another for a distinct PIN. Our future work will involve studying how well people can manage multiple FacePIN cards, and user choice when being allowed to choose their own PIN.

Our representation of zero digits might not be optimal. For example, this might be prone to error, as if a cardholder has completely forgotten their PIN, the benefit of cued-recall is lost as they must recall which grid does not contain a key face (if any). Other space saving measures will be investigated. Ideally FacePIN would minimize impact on card design, whilst maximizing the size of the faces for accessibility purposes.

5. REFERENCES

[1] J. Davies, “Visual Code Recordal and Communication Thereof”, International Patent PCT/GB1999/001688, 1999.

[2] Passfaces – http://www.passfaces.com Last accessed 20/05/07

[3] De Angeli, A., Coventry, L, Johnson, G.I and Coutts, M. (2003). Usability and user authentication: Pictorial passwords vs. PIN. In P.T.McCabe, (Ed.). *Contemporary Ergonomics 2003* (pp. 253-258) London: Taylor & Francis.

[4] D. Davis, F. Monrose and M.K. Reiter. On User Choice in Graphical Password Schemes. In *13th USENIX Security Symposium*, 2004.