SAN JOSÉ STATE UNIVERSITY

# Swipe Authentication: Exploring Over-the-Shoulder-Attack Performance

Auriana Shokrpour, Ashley Palma, Michelle Gomez, Felicia Santiago, & Jeremiah Still

Department of Psychology

## Introduction

Much of our valuable, and sensitive, data are accessible digitally. For example, we no longer have to go to a physical bank to transfer money, we simply download an application on our cellular phone. However, this level of convenience comes at a cost. Thieves are now more easily able to access our accounts. Therefore, it is critically important that systems housing valuable data are able to correctly verify users' identity. This is accomplished through authentication interfaces (i.e., virtual locks). Traditionally, authentication was achieved by simply asking for a username and a secret password. Users are instructed to use a "strong password", because they are more difficult for hackers to determine. Therefore, some basic guidelines for creating strong character-based passwords exist to facilitate security. Interestingly, the more secure a character-based password becomes, the less memorable it is for the user (Vu et al., 2007). This trade-off between usability and security has driven the development of other methods of authentication. One of the most popular alternatives to typical passwords is the swipe based passcode.

Swipe passwords are usually completed by drawing a line to connect dots within a nine point grid. When users input a swipe password they often receive feedback – that is, they can see the drawn line - which creates a graphical representation of the passcode. Studies have shown that graphical passwords are more memorable (Li, Sun, Lian, & Giusto, 2005), easier to execute (De Luca, Hang, Brudy, Lindner, & Hussmann, 2012), and are more liked by users (Zezschwitz, Dunphy, & De Luca, 2013) than character-based.

The rising popularity of swipe passwords demands empirically based recommendations. Our study explored basic factors that ought to increase the security of gesture passwords against over-the-shoulder attacks. We examined the effect of turning off and on visual feedback and the effects of using symmetrical and asymmetrical gestures.

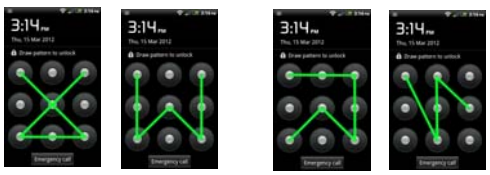
## Method

Eight undergraduate volunteers participated for course credit. Stimuli were created using a web camera and touch screen cellular phone with the standard swipe authentication process. The videos were played in pseudo-random order within Paradigm experimental presentation software.

The experiment employed a within-subject factorial design with 2 Feedback (yes or no) x 2 Symmetrical (yes or no). This design produced four conditions each containing 32 trials. Thus, each participant viewed 128 videos of a person entering a gesture-based password on a phone (e.g., see Figure 1).

Participants watched the videos and attempted to reproduce the viewed gestures. They were asked to draw the swipe pattern onto a nine point grid using a pencil. The dependent measure was the accuracy of the reproductions.

### Figure 1: Examples of Trials with Visual Feedback



Symmetrical

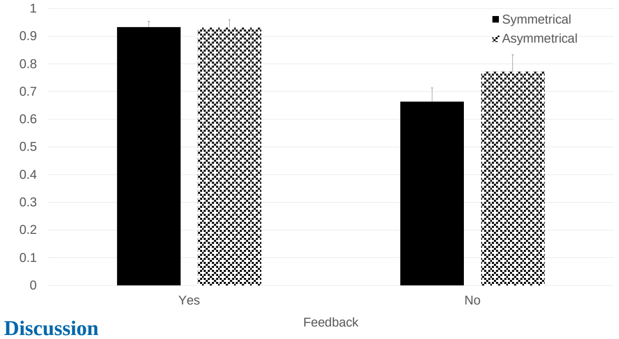
Asymmetrical

## Results

A repeated measures ANOVA was conducted to explore the impact of 2 Feedback (yes, no) x 2 Symmetry (yes, no). We found a main effect of Feedback, *F*(1,7) = 34.07, *MSE* = .01, *p* = .001. However, this finding was qualified by a significant Feedback x Symmetry interaction, *F*(1,7) = 5.82, *MSE* = .004, *p* = .047 (see Figure 2).

A paired samples t-test revealed a significant difference between no Feedback: Asymmetrical (*M* = .77, *SE* = .06) and Symmetrical (*M* = .66, *SE* = .05) videos, *t*(7) = 2.62, *p* = .034.

### Figure 2: Accuracy of Over-the-Shoulder Attacks



## Discussion

Based on the findings of this study, we recommend that users turn off the swipe authentication visual feedback. It is too easy for a thief to employ the over-the-shoulder-attack method to gain access to your valuable data.

Interestingly, symmetrical gestures were more difficult to capture than asymmetrical gestures without feedback. This was an unexpected finding! Our future work will examine the impact these recommendations have on usability (i.e., login error rates and memorability).

## References

De Luca, A., Hang, A., Brudy, F., Lindner, C., & Hussmann, H. (2012). Touch me once and I know it's you!: implicit authentication based on touch screen patterns. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12). ACM, New York, NY, 987-996.

Li, Z., Sun, Q., Lian, Y., & Giusto, D. (2005). A secure image-based authentication scheme for mobile devices. In *Proceedings of the 2005 international conference on Advances in Intelligent Computing - Volume Part II* (ICIC'05), 751-760.

Vu, K., Proctor, R., Bhargav-Spantzel, A., Tai, B., Cook, J., & Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65, 744-757.

Zezschwitz, E., Dunphy, P., & De Luca, A. (2013). Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (MobileHCI '13). ACM, New York, NY, 261-270.

Psychology of DESIGN

Contact Information: jeremiah.still @sjsu.edu