Pre-print: Kuber, R. & Yu, W. 2010: Tactile vs. Graphical Authentication. In proceedings of Eurohaptics (Lecture Notes in Computer Science 6191), Amsterdam, Netherlands, 314-319.

Tactile vs Graphical Authentication

Ravi Kuber [1] and Wai Yu [2]

[1] UMBC, 1000 Hilltop Circle, Baltimore, MD, 21250, USA
[2] Thales, Alanbrooke Road, Belfast, BT6 9HB, UK
rkuber@umbc.edu

Abstract. This paper describes a novel approach to authenticate entry to a system using tactile feedback. The user is required to remember a sequence of pre-selected pin patterns. A study has been undertaken to determine the feasibility of the tactile authentication mechanism, through a comparison with a graphical scheme. Findings from a within-subjects study have revealed that both tactile and graphical authentication sequences could be entered at specific points over the course of a five month period. While graphical sequences could be entered on average 28.5 seconds faster than tactile sequences, participants believed the tactile mechanism offered greater levels of security from observers. As pins are presented underneath the fingertips, they are concealed from the view of third parties. As tactile sensations are difficult to describe, it is less likely that they will be disclosed to others, thereby reducing the chances of unauthorized access.

Keywords: Authentication, haptics, human factors, photographs, tactile

1 Introduction

Haptic technologies can be used to enhance interaction with a wide variety of interfaces, ranging from virtual museum applications to medical training software [1]. More recently, touch has been applied to the design of authentication mechanisms, providing an alternative to traditional systems requiring both a username and alphanumeric password. The VibraPass system [2] presents vibrations via the user's own mobile telephone when entering a Personal Identification Number (PIN) into a public terminal. The vibrations indicate whether the user should 'lie' and enter a different digit from the numbers contained within his/her PIN. The aim is to confuse 'shoulder surfers' seeking to record their victim's PIN. Deyle and Roth [3] have developed an authentication system using eight solenoids, which are either raised or lowered. To enter the system, the user must accurately indicate the state of the solenoids corresponding to his/her personal authentication sequence. Orozco Trujillo et al. [4] have integrated biometric data as part of their authentication procedure. The software extracts key information including the force exerted using the stylus, the torque and the orientation. These features can be used to verify that the user's authenticity. In contrast with these solutions, the Tactile Authentication System [5]

enables the user to authenticate entry through the ability to remember a sequence of pre-selected patterns of raised pins. Pins are presented to users via cells (contactor pads) on top of the VT Player tactile mouse (Figure 1-left). Four different pin patterns are selected and memorized by users as their 'tactile password' to a system, similar to a four digit PIN for an ATM (Figure 1-right).

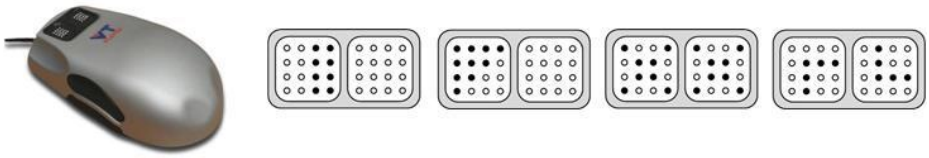

Fig. 1. VT Player (Virtouch Ltd) (left) with sequence of tactile stimuli forming 'tactile password' (right). The filled circles indicate which pins are raised.

Benefits of the Tactile Authentication System (TAS):

- TAS capitalizes on our abilities to remember arrangements of raised pins. This is evidenced by Braille readers, who are able to successfully associate tactile patterns with alphanumeric characters.
- Stimuli are perceived underneath the fingertips, occluding the feedback from view, thereby protecting the user from the threat of third parties observing and recreating the authentication sequence.
- Up to thirty-two pins can be raised to form a variety of patterns on the tactile mouse. Pins can be presented in a timed sequence forming 'animated' stimuli, in conjunction with 'static' raised arrangements.
- The interface has been designed enabling the user to recognize his/her pre-selected stimuli, rather than recalling information. The process of recognition is known to be less cognitively intensive compared with the process of recall.

Fig. 2. Sequence of facial photographs adapted from Passfaces™ [6]

A study has been designed to determine the feasibility of TAS, by comparing it with an alternative authentication mechanism. Graphical schemes have grown in popularity in recent years, capitalizing on our abilities to remember images. Passfaces™ has been designed to enable users to enter a system, by recognizing a series of pre-selected stimuli (facial photographs) in a prescribed order (Figure 2). Studies have shown Passfaces™ to be memorable and recognizable over a long-term period [7,8,9].

2 Tactile Authentication System

A web-based authentication interface has been designed using HTML, ASP, Javascript, VBScript and the VT Player SDK. It is hosted on a local server. In order to enter the system, the user firstly selects his/her full name from a drop-down box, and then selects his/her personal authentication sequence by choosing four tactile stimuli from a wider range presented. The TAS interface consists of four grids, each of which contains nine visually-identical squares arranged in a 3x3 format (Figure 3), similar to the layout used by Brostoff and Sasse [7] in their study. Each square is associated with a unique tactile stimulus [10], presented via the VT Player mouse. By actively exploring the interface, the user will be able to locate the first stimulus from his/her 'tactile password'. The process is repeated on the remaining three grids, until four stimuli have been selected (Figure 4). Tactile sensations are randomly arranged within each grid, so that an observer cannot distinguish the spatial position of the stimulus chosen. A more detailed explanation of the design of TAS is presented in [10].

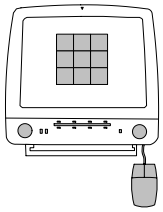

Fig. 3. TAS system displaying grid of tactile stimuli

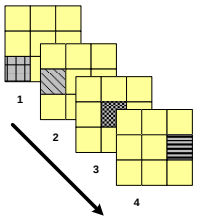

Fig. 4. Example of authentication sequence to enter system

For purposes of the comparison study, TAS was modified to either present tactile information or facial photographs. The photographs were selected both from the Passfaces™ demonstration software and other sites containing headshots. Photographs were selected to ensure that attention would not be unduly drawn to them (e.g. monochrome backgrounds, limited facial jewelry). Similar to entering a 'tactile password', in the graphical condition, the user locates and selects one photograph from each of the four grids presented (Figure 2). After four stimuli have been chosen, entry can be granted, providing the photographs match the user's pre-selected stimuli. The chance of a third party guessing either a tactile or graphical sequence at random would be 1 in 6561 (9^4 combinations [7]).

3 Experiment Design

An experiment was designed where sixteen participants were exposed to two conditions. Participants were first asked to select a tactile authentication sequence consisting of four static and/or animated stimuli. They were asked to log-in to the

system from Monday to Friday only for two weeks, and once at the end of the fourth week, following a procedure adapted from Valentine [8,9]. Participants were then asked to select a graphical authentication sequence, consisting of either male or female faces. These would be entered using the same schedule. Sixteen weeks after participating in each condition, participants were asked to enter their authentication sequences for one last time, to determine their ability to remember secure information over a long term period without rehearsal. In order to determine the feasibility of both the tactile and graphical approaches, measures such as task time taken, failed authentication attempts and resets made were recorded and analyzed.

4 Results and Discussion

Fourteen out of the original sixteen participants completed both conditions of the study. Findings revealed that fewer errors were made by the fourteen participants on their first attempt entering a system under the graphical condition (90.0% rate of success) compared with the tactile condition (86.4% rate of success). Results are presented in Table 1. Levels of accuracy entering the system on the first attempt appeared to reduce when sequence entry could not be rehearsed (e.g. Day 8 after a gap of two days, Day 28 after a gap of sixteen days, and Day 140 after a gap of four months).

Table 1. Accuracy of entry and time taken to enter system for both by condition

	Accuracy of first entry attempt (Tactile)	**Average time Taken (Tactile)**	**Accuracy of first entry attempt (Graphical)**	**Average time taken (Graphical)**
Day 1	100.0%	35.4 s	100.0%	8.6 s
Day 8	87.5%	50.1 s	100.0%	9.4 s
Day 12	92.3%	33.0 s	90.0%	11.0 s
Day 28	83.3%	39.9 s	100.0%	15.0 s
Day 140	58.3%	58.0 s	90.0%	20.0 s

Graphical sequences could be entered on average 28.5 seconds faster (SD 13.4 seconds) compared to entering tactile sequences. Results from a paired t-test revealed that this difference was significant ($p < 0.005$). Reasons were attributed to the presentation of tactile information. Participants were observed moving cautiously through each grid, perceiving each of the tactile stimuli presented, prior to choosing their pre-selected stimulus. A greater level of deviation was also experienced under the tactile condition (16.6 seconds) compared to the graphical condition (3.2 seconds).

There were more incorrect authentication attempts when entering a tactile sequence (20 out of 137 recorded attempts – 14.6 %) over the five month period, compared to when entering a graphical sequence (3 out of 112 recorded attempts – 2.7%). Fourteen of the twenty-three incorrect attempts were made on Day 140 (i.e. four months later). While this in part may have also been attributed to limitations of both tactile and graphical the memory, some participants suggested that they were able to remember their respective authentication sequences but had selected the mouse button twice in quick succession. As a result, two stimuli were entered instead of one (e.g. one stimulus from one grid, another from a second grid). Findings from the study have indicated that participants were able to recover from errors made, and authenticate entry by the fourth attempt. The levels of self-initiated resets were also judged as comparable, with a total of seven resets made for the tactile condition, and a total of five made for the graphical condition.

In terms of perceived security, seven out of fourteen participants stated that they felt more secure using tactile authentication compared to conventional alphanumeric passwords and PINs. When using an ATM, participants remarked that they often shielded the keypad using their hand or wallet when entering their PINs, to reduce the threat of observer attacks. However, as tactile stimuli are occluded from view in TAS, they suggested that they would not need to perform this task when using the tactile mechanism. Participants agreed that as the sense of touch is difficult to describe and is personal to each user, stimuli would be tougher to disclose to others. Even if the tactile sequence was disclosed, there would be no guarantee that a verbal explanation of a tactile pattern could be replicated easily by a third party, as descriptions would vary from person to person. While the graphical condition was not thought to offer the same level of perceived security, eight participants suggested that it was a less cognitively intensive process to visually-scan each grid and recognize graphical stimuli, compared with tactile identification. Participants suggested that concentration was needed for tactile perception, as it was a relatively unpracticed skill, in contrast with facial recognition. As a result, the graphical scheme was found to be more usable than the touch-based mechanism by half the group of participants.

When questioned upon their selections of graphical stimuli, nine participants selected facial photographs from a mixture of racial groups, which they described as being a key factor to help them distinguish between faces. Participants also remarked that accessories within photographs such as glasses and shirt collars offered them a cue to remember and recognize their selected photograph. Analysis of tactile stimuli selected revealed that popular choices included patterns containing a small number of raised pins, or pins arranged in geometric patterns (e.g. formed into lines or shapes). Animated patterns were less widely chosen by participants compared with static patterns. Reasons for this were most likely due to our limited spatial and temporal resolution abilities, making distinguishing between animations a more time-consuming and cognitive intensive process.

5 Conclusion

This paper has described the results of a study to determine the feasibility of a pin-based authentication approach through a comparison with a graphical scheme. Both sets of authentication sequences could be committed to memory, and entered over at points over a five month period. However, results showed that the process of identifying and selecting tactile stimuli was slower compared to graphical stimuli. The tactile channel offers the benefits of presenting information underneath the fingertips, away from prying eyes. As the sense of touch is personal to each user, it is harder to externalize or to share with others [10]. Future work will focus upon investigating challenges facing TAS, which also pertain to mechanisms requiring alphanumeric passwords/PINs. Research will focus upon the impact of infrequent tactile authentication sequence usage, and the problems associated with remembering multiple 'tactile passwords'.

6 Acknowledgements

The authors would like to thank Passfaces Corporation for the use of the Passfaces™ demonstration software [6].

7 References

1. Brewster, S.A. 2005. Chapter 30: The impact of haptic 'touching' technology on cultural applications. Digital Applications for Cultural Heritage Institutions. Ashgate Press, UK, 273-284
2. De Luca, A., von Zezchwitz, E. and Hußman, H. 2009. VibraPass-Secure Authentication Based on Lies. In Proceedings of ACM SIGCHI'09, 913-916.
3. Deyle, T. and Roth, V. 2006. Accessible Authentication via Tactile PIN Entry. Computer Graphics Topics, 2, 24-26.
4. Orozco Trujillo, M., Shakra, I. and El Saddik, 2005. Haptic: The New Biometric-Embedded Media to Recognizing and Quantifying Human Patterns. Proceedings of the 13th Annual ACM International Conference on Multimedia.
5. Kuber, R. & Yu, W. 2006. Tactile Authentication. Patent No 0603581.0 (Patent Applied For).
6. Passfaces™ Demonstration Software. 2009. Passfaces Corporation. www.passfaces.com
7. Brostoff, S. and Sasse, M.A. 2000. Are Passfaces™ more usable than passwords? A field trial investigation. Proceedings of HCI'00, 405-424.
8. Valentine, T. 1998. An Evaluation of the Passface Personal Authentication System (Technical Report). London, UK.
9. Valentine, T. 1999. Memory for Passfaces™ after a Long Delay (Technical Report). London, UK.
10. Kuber, R. & Yu, W. 2010. Feasibility Study of Tactile-based Authentication. International Journal of Human Computer Studies, 68, 158-181.