Pre-print: Kuber, R. & Sharma, S. 2010. Toward Tactile Authentication for Blind Users. In proceedings of the 12th International ACM Conference on Computers and Accessibility – ASSETS'10, Pittsburgh, USA, 289-290.

Toward Tactile Authentication for Blind Users

Ravi Kuber and Shiva Sharma
UMBC
1000 Hilltop Circle
Baltimore, MD 21250, USA
rkuber@umbc.edu

ABSTRACT
This paper describes the design of an accessible authentication mechanism. The Tactile Authentication System has been adapted to enable individuals who are blind to access electronic data using their sense of touch. To enter the system, users must identify a set of pre-selected pin-based icons from a wider range presented via a tactile mouse. As information is presented underneath the user's fingertips, 'tactile passwords' are shielded from observers, thereby enhancing security from third-party attacks. Results from a pilot study showed that five participants were able to authenticate entry to the non-visual interface over the course of a two week period. However, findings have revealed that the time needed to perform this process should be reduced to improve the quality of the user experience.

Categories and Subject Descriptors
H5.2 [Information Interfaces and Presentation]: User Interfaces - Haptic I/O.

General Terms: Human Factors.

Keywords
Authentication, multimodal interfaces, tactile feedback.

1. INTRODUCTION
As user authentication is commonly required to access personal data held within electronic systems (e.g. online banking and shopping), a number of passwords need to be recalled on a daily basis. The process of authentication can be stressful for many users. This can be attributed to the challenges faced when memorizing 'stronger' passwords which are difficult for others to guess or 'crack', combined with fears of observers viewing password entry (shoulder surfing) thereby breaching security. Individuals who are blind may experience additional difficulties with the process of authentication. While screen readers provide valuable support to access graphical user interfaces (e.g. web pages), issues have been found when filling-out online forms, such as log-in screens [4]. As content from the interface is presented through speech, blind users are required to wear headphones to access the system securely. However, environmental sounds may be attenuated or occluded whilst performing the task. As a result, blind users may not be aware of 'shoulder-surfers' behind them, observing password entry.

ASSETS'10, October 25–27, 2010, Orlando, Florida, USA.
ACM 978-1-60558-881-0/10/10.

2. PREVIOUS WORK
In order to address some of the difficulties which individuals experience when recalling alphanumeric passwords, alternatives such as PassFaces™ [5] have been developed. The system has exploited the brain's iconic memory for faces, and our superior facial recognition abilities. Users choose pre-selected photographs of male or female faces from a series of grids. As the photographs are positioned randomly within each grid, observers are less able to monitor the sequence of entry, compared with entering a traditional alphanumeric password or a personal identification number (PIN). However, the system is not accessible to individuals with visual disabilities. Sauer et al. [6] have developed accessible picture verification boxes (CAPTCHAs), by presenting information through auditory means. Results from their studies revealed that participants were able to authenticate successfully into the system in an average of 65.64 seconds. However, the researchers suggest that further work would need to be completed to enhance the usability of the solution. Deyle and Roth [2] have developed a prototype where users are required to position four fingers from each hand over a set of solenoids which are connected to pins. To authenticate entry, users must accurately identify the status of the pins (e.g. whether raised or lowered). Bianchi et al. [1] have developed a haptic wheel, which is rotated in a specific way to facilitate authentication to the system. While the haptic information provided by the wheel was found to be identifiable, the position of the device can be monitored by shoulder surfers. From the review conducted, a need has been identified to develop a system which addresses issues of security, memorability and accessibility.

3. TACTILE AUTHENTICATION SYSTEM
A web-based Tactile Authentication System (TAS) [3] has been developed to enable users to authenticate entry using their sense of touch. Similar to PassFaces™ [5], the user is presented with four grids of nine squares (Figure 1). Each square contains a unique pattern of raised pins presented via cells (contactor pads) on top of the VT Player tactile mouse (Figure 2). Participants in an earlier study [3] were asked to select and memorize four different pin patterns from a range of thirty-six stimuli. This formed their 'tactile password' to the system. Four stimuli were chosen to provide a comparative amount to a four digit PIN for an ATM (Figure 3).

Findings showed that participants were able to use their tactile passwords over a month-long period, and achieved a 92.9% rate of success accessing the system on their first attempt. As tactile information was presented underneath the fingertips and therefore shielded from view, levels of security were perceived to be higher compared with ATMs (3.25/5). While TAS was found to be

usable by the majority of participants in the earlier study, the interface was originally designed taking for granted the user's ability to move the mouse around each grid, to perceive the tactile stimuli contained within each square. Many blind individuals are not familiar with using a mouse, as keystrokes are often favored to interact with a screen reader.

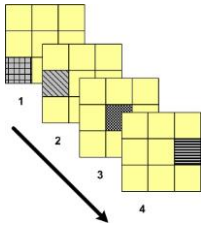

Figure 1. Grid squares containing tactile stimuli

Figure 2. VT Player (Virtouch Ltd)

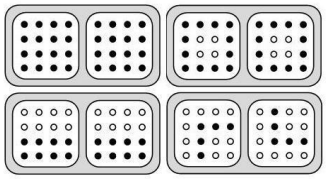

Figure 3. Examples of pin patterns which form an authentication sequence

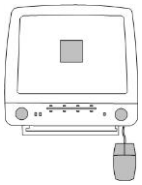

Figure 4. Different tactile stimuli are temporally presented within one square

In response to the situation, TAS has been adapted to widen access to blind users. Instead of presenting tactile information within four different grids, information is presented inside one grid square positioned at the center of the screen (Figure 4). Nine tactile stimuli are presented in a randomized order via the mouse when positioned over the square. Each pin pattern is presented for eight seconds. The user must identify one stimulus which corresponds to one pattern within his/her pre-selected 'tactile password', and then press the mouse button to confirm his/her choice. He/she should not need to move the mouse during this time. Three more sets of nine tactile icons are then played. Once the user has selected four icons, one from each set, he/she presses the 'Enter' key on the keyboard to submit his/her authentication sequence. If an inaccurate attempt has been made, the user has two more chances to enter his/her authentication sequence. Other instructions for usage of the interface are presented through speech-based cues.

4. PILOT STUDY

Five sighted volunteers were recruited to participate in a pilot study to determine the feasibility of the enhanced version of TAS. The participants were blindfolded. Each was introduced to the system, and asked to select a tactile authentication sequence, comprising of four pin patterns. He/she was required to practice these ten times to commit these to memory. Participants were required to login to the system using their tactile sequences at points over a two-week period. To do this, the participants would select their name from a drop-down box using arrow keys on the keyboard, and then be prompted to actively move their fingers around the contactor pads on the mouse, to identify their pre-selected stimuli.

Findings have shown that all five participants were able to enter their authentication sequences over the two-week period, in the absence of graphical cues. The rate of accurate identification of tactile sequences on the first attempt using the system was 86.7%. This was performed within a time of 121.7 seconds (SD: 33.7 seconds). All participants managed to authenticate entry by their third attempt. Even though the time taken using the adapted version of TAS was higher than the previous version of the system [3], the current version was described by participants as having the potential to offer blind users an accessible authentication experience. However, the usability of the interface would need to be improved. Suggestions included presenting tactile icons for a shorter period of time (e.g. five seconds instead of eight), as pin patterns could be adequately perceived within this period. All five agreed with the statement that using TAS would offer a more secure experience from onlookers, compared to an ATM, as stimuli are not visible to observers. In contrast with alphanumeric passwords, tactile sequences were described as being difficult to write down or share with others, thereby enhancing security from third party attacks.

5. CONCLUSIONS AND FUTURE WORK

The Tactile Authentication System has been adapted to provide blind individuals with an accessible method of entering a knowledge-based mechanism. Participants were able to explore the non-visual interface and log-in to the system over a two-week period. The interface was perceived to be more secure than other alternatives, as information is presented underneath the fingertips. The next logical step in the research is to refine the prototype to improve time taken to select and enter a tactile authentication sequence, and to test the system's feasibility with blind users.

6. REFERENCES

[1] Bianchi, A., Oakley, I., Lee, J.K. and Kwon, D.S. 2010. The haptic wheel, Design and Evaluation of a Tactile Password System. In *Extended Abstracts of CHI'10*, 3625-3630.

[2] Deyle, T. and Roth, V. 2006. Accessible authentication via tactile PIN entry. *Computer Graphics Topics* 2, 24–26.

[3] Kuber, R. and Yu, W. 2010. Feasibility Study of Tactile-based Authentication. *International Journal of Human-Computer Studies*, 68, 158-181.

[4] Murphy, E., Kuber, R., McAllister, G., Strain, P., Yu, W. 2008. An empirical investigation into the difficulties experienced by visually impaired Internet users. *Universal Access in the Information Society*. 7(1), 79-91

[5] PassFaces™. Real User Corporation. Available from: http://www.passfaces.com

[6] Sauer, G., Hochheiser, H., Feng, J. and Lazar, J. 2008. Towards a Universally Usable CAPTCHA. In *Proceedings of Symposium on Accessible Privacy and Security (SOAPS)*.