Pre-print: Kuber, R. & Yu, W. 2006: Authentication using Tactile Feedback. In proceedings of the 20th BCS Conference on Human Computer Interaction - HCI'06 Volume 2, London, UK, 141-145 (5 pages when in print).

Authentication Using Tactile Feedback

Ravi Kuber & Wai Yu
Queen's University Belfast, Belfast, BT7 1NN, UK
{r.kuber, w.yu}@qub.ac.uk

As current knowledge-based systems do not take into account human limitations when recalling authenticating strings, individuals often select short or guessable passwords. As a result, a compromise is created between memorability and security. To address these issues, a novel approach has been developed examining the use of recognition-based authentication, through the use of the haptic modality. The Tactile Authentication System (patent pending) allows the user to authenticate entry through the ability to recognize previously perceived tactile sensations. This method of authentication presents benefits over alternative visual-based systems. Stimuli are perceived underneath the fingertips, protecting the user from the threat of observers recreating the authentication sequence. As the sense of touch is personal to each individual, tactile sensations are difficult to describe in concrete terms, so cannot be easily shared with others. This paper reports the design of the Tactile Authentication System (TAS), and presents results from a one-month trial. Participants were able to recognise their pre-selected tactile stimuli from a wider range of sensations, and could form their personal sequences to authenticate entry to the system. TAS has been shown to present a memorable and usable alternative to conventional knowledge-based authentication systems.

Authentication, memorability, haptics, perception, tactile.

INTRODUCTION

The need for heightened security is intensifying as organisations begin to automate more business functions, which in turn, increases the amount of sensitive data stored in electronic format on shared networks. Renewed security threats and legislation such as the Data Protection Act (1998), have driven organisations to realise the importance of information security. Knowledge-based authentication (KBA) is the most common method of user authentication, where the trusted individual identifies himself/herself with a username, and authenticates entry using an alphanumeric password [4]. Identification establishes the user's right to access the system. The authentication mechanism verifies that the user is the legitimate owner of the ID [2]. KBA is favoured over alternatives such as biometric authentication, as it is a well tested form of technology, simple to administer, well understood by users and system administrators, and requires no additional hardware or software [11].

Whereas in the past, organisations have mainly concentrated on securing data from the threat of physical attacks, the focus has shifted to issues associated with the user (human factors). This is due in part to limitations of the human memory. With the proliferation of technology, individuals need to increasingly authenticate access to multiple systems on a daily basis [2]. Precise recall of information is known not to be a strong point of human cognition [3]. Natural decay of information from our memories and within-list interference effects from other similar chunks of information can occur, meaning that the user may find it difficult to authenticate entry into systems, particularly when recalling randomly generated passwords. As a result, individuals often tend to select 'weaker' passwords, which are often short and guessable. In an attempt to achieve memorability, security is compromised. The threat of third-party attacks with KBA mechanisms is also evident. Individuals have been found to write-down or share authentication information with others [1]. 'Shoulder-surfers' monitor the spatial position of keystrokes made by users on numerical-keypads and keyboards. In both cases, authentication sequences can be recreated and system entry can be achieved. A need has been identified for a system addressing issues of weaknesses arising from human factors and observer attacks.

GRAPHICAL AUTHENTICATION & THE TACTILE MODALITY

Studies have shown that pictures can be easily committed to memory [2,3,11]. In contrast to recall-based systems used for remembering alphanumeric passwords, systems employing graphical authentication make use of the benefits offered by recognition. Recognition involves a less resource-intensive process when compared to recall, so would benefit the end-user when interacting with authentication technology. The Déjà Vu system [3] has been designed to effectively recognize abstract art images in a sequence (portfolio), from a larger set of images presented by a server. The Passface system [2] works in a similar fashion, asking users to remember and cognize photographs, exploiting our exceptional abilities to recognize faces. Whereas a recognition-based approach can lead to a lower level of mental workload being expended, scanning through each item visually can prove to be a time consuming process. This possibly accounts for the limited market share of graphical-based authentication mechanisms, compared to alphanumeric-based ones.

Research has shown the human ability to remember haptic information [10], however relatively little is known about the sensory memory store responsible for retaining haptic data [5]. Estimates dictate that our tactile memory span is between two to three items [14]. Mahrer & Miles [8] found participants were able to recall between four to six tactile stimuli, presented through the form of taps to the fingers. The researchers have also discussed the benefits that vision can bring to the tactile recognition process [9]. Relatively little research has been conducted in the areas

of tactile recognition and the long term capacity of tactile memory. However, it is thought that the tactile channel could provide benefit for purposes of authentication.

SYSTEM REQUIREMENTS

The Tactile Authentication System (TAS) has been developed in order to provide an alternative to alphanumeric and graphical authentication systems. It makes use of our tactile memory capabilities to remember and recognize pre-selected tactile stimuli. The system has been designed according to the following criteria, discussed in greater detail by [1, 2, 3]:

- **Memorability**: The system should benefit from the strengths offered by recognition, compared with recall.
- **Security**: Users should not be able to select 'weak' authentication information. Design should focus on weaknesses arising from human factors. Threats from observer attacks should be minimised, and authentication information should be difficult to externalise.
- **Usability**: The system should be easy to learn, providing the user with a usable and stimulating experience.

SYSTEM DESIGN

The VT Player device (Figure 1) has been chosen for the purposes of the demonstration, as it works in a similar manner to a computer mouse, and has the benefit of providing customised tactile output through a pair of electronically-controlled matrix units (contactors) built into the surface just where the fingers rest. The matrices roughly resemble the display of Braille cells. Each 4x4 matrix holds 16 pins which rise and fall dynamically, gently delivering a tactile sense of the screen to the user's fingertips. Pins can be arranged to form static patterns (Figure 2), or alternatively can be designed to change state over time, providing animated-style sensations. The user places his/her index and middle finger over the contactor pads to perceive the tactile stimuli. As participants' fingers cover the entire contactor pads, patterns are visually-occluded when using the device.

The Tactile Authentication System [6] interface has been developed using the following Web technologies; HTML, Javascript, VB Script, and the VT Player SDK, enabling users to authenticate access to a system on a standalone PC. The Web application environment has been simulated using Microsoft Internet Information Server 5.0, allowing the standalone PC to act as a server. The tactile sensations used in TAS have been developed in view of the findings from an earlier perceptual study conducted by [7]. Distinctive static and animated pin patterns have been designed to enable users to quickly and accurately denote differences between each form of stimuli. Pin stimuli in the form of visual objects such as geometric shapes, lines, and symmetrical patterns have been included, as users were able to recognise these effectively in [7] (Figure 2). Pins were not positioned in close spatial or temporal proximity, in order to reduce effects of tactile occlusion.

FIGURE 1: VT Player device

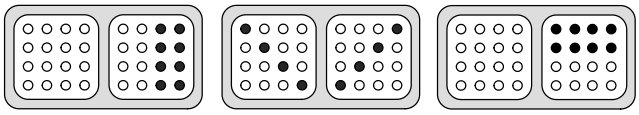


FIGURE 2: Examples of pin stimuli used in experiment

ENROLLMENT & MAIN TRAINING

All participants are provided with initial training on the VT Player device to expose them to a wide array of tactile stimuli and test basic recognition abilities. They are asked to select four tactile stimuli, from a selection of thirty-six distinctive sensations. Participants are then questioned on their reasons for selection, and given the opportunity to feel and memorise the tactile stimuli, in sequence format. They are then presented with a series of stimuli, including their own (main training phase), and are asked to identify their personal tactile sensations, in the sequence originally selected. Participants are then asked to repeat this procedure ten times, to commit the authentication sequence to memory.

AUTHENTICATION TO TAS

The authentication process employed by TAS is based on the method used by [2]. In order to successfully authenticate entry into the system, the participants select their name from a drop-down list, and then choose their personal tactile authentication sequence, comprising of four tactile stimuli, in the order originally selected in the enrollment stage.

Participants are presented with four grids, each of which contains nine visually-identical squares arranged in a 3x3 format (Figure 3). Each square contains a static or animated stimulus from the original thirty-six pin patterns designed for the study. As the users hover over each square, a different stimulus is perceived underneath the fingertips. Participants are asked to explore the sensations present in the first grid, and select one stimulus which corresponds to a sensation in their own personal authentication sequence. The process is repeated on the remaining three grids, until four stimuli have been selected (Figure 4). The order of grid presentation remains constant, as does the nine tactile stimuli contained within each grid. To minimise the chance of participants memorising the visual position of squares containing tactile stimuli, the order of sensations presented within a grid is randomized. Using four tactile stimuli selected from four grids provides 9^4 combinations, meaning that the chance of someone guessing a sequence at random would be 1 chance in 6561.

The user can try up to four times to enter the authentication sequence, before a sequence reminder containing four tactile stimuli, is sent to the participant. This is similar to the system employed by banks, where three PIN attempts can be made using the same card, in any one ATM machine. Upon receiving a reminder, the participant would be asked to go through the training procedure again, to commit the sequence to memory.

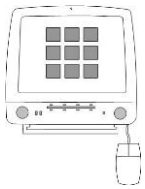


FIGURE 3: TAS system displaying grid of tactile stimuli

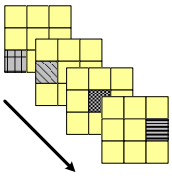


FIGURE 4: Example of authentication sequence to enter system

EXPERIMENT DESIGN, FIELD TRIAL RESULTS & DISCUSSION

A field trial was conducted with sixteen participants (12 male, 4 female, aged between 23 and 42), ten of whom had accessed the VT Player device one month prior to the trial. The trial aimed to assess the following:

- Recognition of tactile stimuli sequences over a short and long term period.
- Usability of the TAS interface and general system.

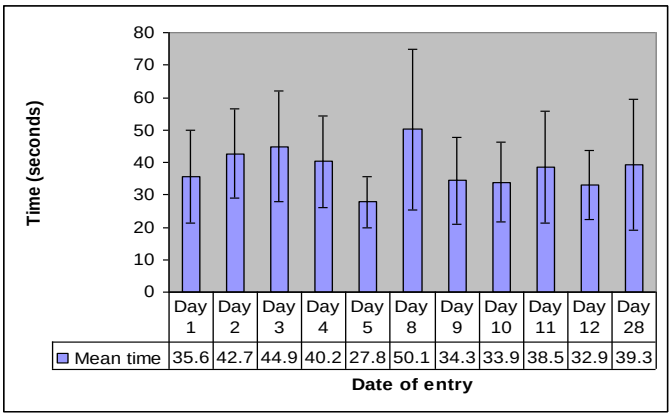
The participants were asked to log-in to the system every working day (Monday to Friday) for two weeks, and once at the end of the fourth week, following a procedure adapted from [13, 2]. Both the enrollment and authentication stages were completed in secure environments away from third-parties, as specified by [3].

Participants took up to four minutes carefully selecting tactile stimuli, in an attempt to build-up an authentication sequence. The reason behind the lengthy enrolment time was due to the fact that participants wanted to firstly perceive all tactile stimuli available, and make an informed choice as to which they thought the most distinctive sensations were to be. It was also evident that participants selected static, or a mixture of static and animated tactile stimuli, to form their authentication sequences. When questioned on their choice of stimuli, most replied that distinguishing between animated stimuli was a tougher process, compared with differentiating between static feedback. This could have been attributed to the participants' unfamiliarity with haptic devices and temporal limitations which made distinguishing between animated pin stimuli a tougher process for the users. Further analysis of authentication sensations used, revealed that participants were not selecting the same pin patterns as each other, opting for diverse 'static' or 'static and animated' choices.

TABLE 1: Successful attempts to authenticate entry

	% remembered (initial attempt)	% remembered (successive attempts)
Day 1	100% (1st attempt)	N/A
Day 2	93.8% (1st attempt)	100% (4th attempt)
Day 3	78.6% (1st attempt)	100% (2nd attempt)
Day 4	91.7% (1st attempt)	100% (2nd attempt)
Day 5	100% (1st attempt)	N/A
Day 8	87.5% (1st attempt)	100% (2nd attempt)
Day 9	92.3% (1st attempt)	100% (2nd attempt)
Day 10	100% (1st attempt)	N/A
Day 11	100% (1st attempt)	N/A
Day 12	92.9% (1st attempt)	100% (2nd attempt)
Day 28	84.6% (1st attempt)	100% (2nd attempt)

FIGURE 5: Time taken to authenticate access using tactile feedback



After selecting their stimuli, users were asked to enter their chosen tactile sensations, ten times in sequence order. The system would help the users to recover from any errors made during these practice sessions, by visually highlighting incorrect selections and directing the participants towards the square containing the original stimulus. By the fourth attempt, participants managed to authenticate their entry into the system free of errors, indicating a priming stage may have taken place. Human implicit memory, indicated by priming, refers to a change in performance of some task, due to prior exposure to the task materials [5]. The implicit memory has been shown to extend to the haptic memory [12], indicating that our tactile abilities may have played a part in the encoding of tactile authentication sequences in the TAS study.

After the training period, all sixteen participants were successful at authenticating entry to the system within the first attempt (100% - Day 1). This was performed in an average entry time of 35.6 seconds (Figure 5). For the rest of the week, participants continued to attempt to enter the system, with low levels of error (Table 1). Users could work their way through the nine stimuli contained within a grid, quickly enough to perceive the pattern presented within a short period of time and make a decision whether to select, or to move to the next stimulus. Interestingly, after gaps without rehearsal of authentication sequences, participants were still able to accurately authenticate entry to the system within the first few attempts, highlighting the long-term memory aspects of non-textual feedback, also found in studies by [13]. It was noted that participants would spend longer after a gap of the weekend (50.1 seconds – Day 8), carefully selecting stimuli from the choices available. However, the time taken to

authenticate entry would reduce on successive days. By the end of the month, with over two weeks without using the tactile stimuli, all participants were able to login within the second attempt. This shows that the tactile channel can be beneficial in both the short and long term for purposes of authentication.

Participants were generally found to be successful at authenticating entry on the first attempt (92.9%). Throughout the course of the one month trial, users were found to make 13 incorrect attempts to access the system from a total of 153 recorded entries (8.5%). 7 self-aborted attempts were also recorded. Further analysis revealed that a small number of participants were becoming confused between two similar stimuli, which they could not distinguish between. This was most likely due to the effects of occlusion. Brostoff and Sasse [2] have noted that failed login attempts are user costs, and so should be minimized where possible. As all participants were able to log-in within the four attempt limit, no reminders needed to be sent out.

Regarding the question of how were users able to remember their stimuli, many participants admitted that as they were able to explain their choice of stimuli verbally, and make a visualization of the patterns in their minds. This may have aided them to retain authentication information over the month-long trial period. Mahrer and Miles [9] have suggested that memory for a sequence of tactile stimuli involves the deployment of strategies using a combination of verbal rehearsal and visio-spatial recoding rather than relying solely on the retention of tactile sensations. A similar situation may have also applied to TAS users.

In terms of usability, TAS was rated quite favourably as a method for authenticating entry. The system was found to be understandable, learnable, and operable without the need for technical support. However, participants did point out that isolating each stimulus within each grid was a time-consuming process. An average of 38.2 seconds was taken to authenticate entry to TAS. Using a recall-based approach would be considerably faster. It is thought that by providing salient feedback which can be perceived instantly on a less visual-centric interface, may bridge the gap between time taken to enter both types of mechanism. Participants were generally pleased with the strengths that the randomized presentation of information on the Tactile Authentication System interface brought. It led them to feel more secure from the threat of observer attacks. Tactile feedback experienced underneath the fingertips was perceived as a secure method of presenting information away from shoulder-surfers. With the recent switch-over to Chip'n'Pin technology to the UK and the growth of ATM machines, users saw promise in using tactile feedback to occlude visual information from onlookers when making financial transactions. Tactile authentication technology was thought to provide an inclusive authentication solution, allowing the visually-impaired community to access private data more effectively. Whereas participants of the TAS study highlighted the benefits and feasibility that tactile authentication has to offer, the tactile authentication trial was not completely representative of the memory demands placed upon users. This was the first tactile authentication sequence that participants were asked to remember, so there were no issues from within-list interference. Future work will aim to assess how effectively multiple authentication strings can be recognised, and whether interference effects will occur in these situations.

CONCLUSIONS & FURTHER WORK

The paper has described the design and development of a novel authentication system that makes use of our ability to memorise and recognise tactile feedback. Results from a study have shown that sixteen participants were able to memorise and authenticate entry for a month long period, with low levels of error. The sense of touch is unique to each user, making tactile stimuli more difficult to write-down or disclose to others. Tactile stimuli are occluded from view when entering the system, so it will be tough for third parties to observe the sensations. The next logical step would be to evaluate TAS over a longer period of time, to obtain a greater representation of the capabilities of the human memory, when using tactile feedback. The findings can then be compared with those of alphanumeric and graphical authentication. It is thought that the human-computer interaction of TAS could be enhanced with a more suitable interface design, and by providing more recognizable forms of tactile feedback on larger areas of skin. In this way, the tactile stimuli could also be perceived within a shorter time frame.

REFERENCES

[1] Adams, A. & Sasse, M. A. (1999) Users Are Not the Enemy. Communications of the ACM 42, 12, pp. 40-46.
[2] Brostoff, S. & Sasse, M.A. (2000) Are passfaces more usable than passwords? In Proc. HCI'00, pp. 405-424.
[3] Dhamija, R. & Perrig, A. (2000) Deja Vu: A User Study Using Images for Authentication. In Proc. USENIX'00.
[4] Garfinkel, S. & Spafford, G. (1996) Practical Unix and Internet Security, O'Reilly & Associates, USA.
[5] Klatzky, R. L. & Lederman, S. J. (2002) Touch. In Experimental Psychology, Wiley, New York, USA, pp. 23-25.
[6] Kuber, R. & Yu, W. (2006) Tactile Authentication. Patent No 0603581.0 (Patent Applied For).
[7] Kuber, R. & Yu, W. (2006) Using Tactile Feedback for Authentication (In process of submission to IJHCS).
[8] Mahrer, P. & Miles, C. (1999) Memorial and Strategic Determinants of Tactile Recency. Exp Psy, 25, 3, 630-643
[9] Mahrer, P. & Miles, C. (2002) Recognition memory for tactile sequences. Psychology Press 10, 1, 7-20.
[10] Millar, S. (1999) Memory in touch. Psicothema, 11, 747-767.
[11] Renaud, K. & De Angeli, A. (2004) My password is here! Interacting With Computers, 16, 6, 1017-1041.
[12] Srinivas, K., Greene, A.J. & Easton, R.D. (1997) Implicit and explicit memory for haptically experienced two-dimensional patterns. Psychological Science 8, 243-246.
[13] Valentine, T. (1998) An Evaluation of the Passface Personal Authentication System (Tech Report). London.
[14] Watkins, M.J. & Watkins, O.C. (1974) A tactile suffix effect. Memory & Cognition 5, 529-534.