The Secure Haptic Keypad: A Tactile Password System

Andrea Bianchi
Korea Advanced Institute of Science and Technology
Daejeon, Korea
andrea@kaist.ac.kr

Ian Oakley
Madeira Interactive Technologies Institute
Universidade da Madeira, Campus da Penteada, Funchal, Portugal
ian@uma.pt

Dong Soo Kwon
Korea Advanced Institute of Science and Technology
Daejeon, Korea
kwonds@kaist.ac.kr

ABSTRACT
Authentication in public spaces poses significant security risks. Most significantly, passwords can be stolen, potentially leading to fraud. A common method to steal a PIN is through an observation attack, either using a camera or through direct observation (e.g. shoulder-surfing). This paper addresses this problem by presenting the design and implementation of a novel input keypad which uses tactile cues as means to compose a password. In this system, passwords are encoded as a sequence of randomized vibration patterns, making it visually impossible for an observer to detect which items are selected. An evaluation of this system shows it outperforms previous interfaces which have used tactile feedback to obfuscate passwords.

Author Keywords
Tactile UI, security, PIN entry, user study

ACM Classification Keywords
H5.2. User Interfaces: Haptic I/O

General Terms
Security, Experimentation, Human Factors

INTRODUCTION

Interacting in public spaces to gain access to sensitive private services is commonplace. Everyday examples include bank ATMs, keypad entry door systems, quick flight check-in kiosks and many services available on computers and mobile devices. A typical mechanism with which to access such services is via authentication by entering numerical codes into keypads: PIN entry systems.

However, stolen PINs pose a significant risk to many systems. For example, banking terminal fraud in the United States is estimated to cost $60 million annually [4]. One of the simplest and most common ways to steal a PIN is through an observational attack in which the numerical keypad is monitored either using cameras or through "shoulder-surfing", essentially surreptitious human observation of the password entry process [3].

CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.

This paper addresses this problem by proposing a novel design for shoulder-surfing resistant password input based on tactile cues. This system, the Secure Haptic Keypad (SHK), was designed as an alternative to current alpha-numeric keyboards and was therefore intended to be economical, robust and capable of supporting rapid, reliable human input of authentication passwords. The system is based around the idea of encoding passwords as a sequence of vibration patterns rather than characters, numerals or images [1]**.** This makes it impossible for an observer (using visual means) to detect a user's selections.

The remainder of this paper is organized as follows: the subsequent section describes related work; the system is then introduced; a user study exploring human performance is described; and the paper closes with a discussion of the results and avenues for future work.

RELATED WORK

Considerable efforts have been dedicated to creating password systems that are resistant to shoulder-surfing. Broadly, these can be grouped into four key categories, described below.

The first category of interfaces combines textual or graphical passwords with the presence of additional steps (overhead) to obfuscate a user's selection. Mechanisms to achieve this include keypad layout randomization [10] and the inclusion of puzzles or cognitive trapdoor games [8]. Although shoulder-surfing resistant these approaches are vulnerable to camera based visual recording attacks. The second category consists of gaze-based password entry systems. In such systems, users select the input from an on-screen keyboard using eye motions [6]. Although relatively reliable and immune to observational attack, this method requires expensive specialized hardware devices. The third group features systems which rely on hardware interfaces owned and carried by users, such as mobile devices. As such systems are not a part of the public infrastructure attackers are unable to manipulate them. Examples include authentication to public terminals via mobile phones equipped with acceleration sensors [7] or through establishing a complimentary tactile channel to obfuscate a standard numerical PIN entry [3]. However, such methods suffer from a weakness to man-in-the-middle attacks on the (typically wireless) connections between the personal and public devices. They are also vulnerable to the theft of the personal device [7].

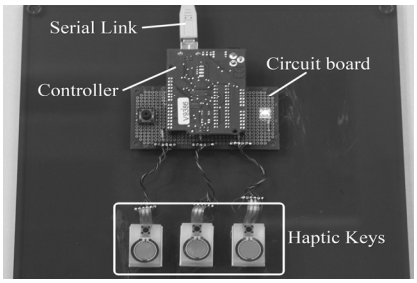

Figure 1. Plan view of the SHK hardware.

The last group of interfaces consists of special purpose devices which use haptic input or output to obfuscate a password entry process. A recent example is Undercover [9], a system which combines a hidden tactile challenge with the selection of a graphical password. The method described in the paper fits firmly in this final category, but is intended to address the weaknesses of prior work through reduced error rates, entry times and the (implied) levels of cognitive load which contributes to these. The key mechanism with which this is achieved is through the use of a uni-modal *haptic password*, rather than one which requires more complex multi-modal information.

SYSTEM DESCRIPTION

The SHK uses a special keypad constructed of three physically independent buttons each capable of sensing finger input and rendering vibrotactile cues in the form of tactons [2], or structured vibration patterns. Although tactons can involve multiple dimensions (such as amplitude and duration), those used in the SHK vary solely in the frequency with which vibration pulses are delivered. Three tactons are used, corresponding to the number of buttons, with frequencies of 1Hz, 2Hz and continuous activation.

Passwords in the system take the form of a sequence of these tactons. When entering a password the three keys each display one of the tactons and the user must physically search the keypad to identify which key should be pressed to correctly enter the next password item. Upon entering an item, the tactons are randomized among the keys and the next item can be sought and entered. No visual feedback is provided, meaning this entry mechanism is not susceptible to visual observation attack. The choice of three keys and tactons is intended to minimize cognitive load and was motivated by the fact that people perform better in absolute judgment tasks featuring a small number of options [11].

IMPLEMENTATION

The SHK is implemented with three identical bespoke hardware keys integrating physical switches and pressure sensors on their topmost surface and linear coil vibrotactile actuators within their casing. They are connected to an Arduino microcontroller interfaced to a personal computer and are shown in Figure 1. The switches allow users to make selections events while the FSR is used to detect contact and also to adjust the strength of the vibrotactile output: the harder the pressure, the greater the magnitude of the tactile cue presented. All software was written in Java and the Arduino framework.

Password Design

Two forms of interaction mode were designed for this hardware platform: *normal* and *hybrid*. In the normal mode, passwords consist of sequences of tactons which a user must seek out and select. Tactons are randomized on keys after each entry and each key always displays a unique tacton. The hybrid mode is more complex. Prior to entering each tacton in the password, the system asks the user to either insert the correct tacton (as in the normal mode) or to insert its complement – to simultaneously press the keys which do not show the current PIN tacton. In this mode, the one-to-one correspondence of keys to tactons is broken, meaning that users may be required to select one, two or three keys. The system ensures that at least one tacton is different from the others, resulting in seven possible input choices for every password item.

Security Analysis

This work aims to build an interface which is resilient to observation and brute-force attacks; more sophisticated attacks, including social engineering, are not considered. An adequate level of security is defined as a password which can be guessed with a probability of 1/10,000, a figure equivalent to a 4-digit numerical password and commonly adopted as a target by other researchers [9]. According to this definition the security of the normal and hybrid modes differs. The susceptibility of the normal mode to both brute force and (given the randomization of tactons to keys) observation attacks can be calculated simply by 3^i where i the number of password items. The hybrid mode is a more complex case. Password items in complement mode are more resistant to purely brute force (in which keys are pressed at random) and visual observation attacks due to the higher number of possible input combinations. A password in purely complement mode would offer a level of security of 7^i. However, this mode is susceptible to a more time consuming brute force attack involving exhaustive tactile exploration of the keys to determine the currently valid set of inputs prior to each tacton entry. This attack reduces the performance to that of the normal mode: 3^i. A password composed of a mix of normal and complementary items will have a level of security to pure brute force and observation attacks proportional to the mix of items.

EVALUATION

Two evaluations of the system were performed. The first was a simple pilot study with four participants intended to ascertain basic recognition rates and times for the tactile cues. It used a simplified version of the display hardware consisting of a single vibrotactile actuator in a single button and involved participants experiencing one of the tactons and then identifying it using a simple GUI. After a 15 trial practice session, a total of 60 trials (20 of each cue) were presented in two blocks of 30. Participants wore headphones and listened to white noise throughout to mask any noises

from the actuator. The results were encouraging: no errors were recorded, indicating that subjects found the task straightforward. Mean task completion times were also acceptable and varied for the 3 cues as follows: 1Hz (2.4s, SD 0.08s); 2Hz (2.44s, SD 0.15s); and continuous (2.7s, SD 1.5s). Although no formal analysis was performed on these data, these results suggest that identifying the continuous cue required that both the others first be eliminated.

Building on these positive results, an exploratory study to investigate optimal design of a tactile password was conducted. The goal of this study was to gather performance data to contrast the SHK against prior work such as Undercover [9]. A secondary goal was to explore performance differences between the normal and hybrid modes in order to compare simple direct input and input which requires more complex cognitive mappings. The results of this assessment will provide directions for further development of tactile password concept.

Participants

12 participants volunteered for this study. They had a mean age of 29 and were a mix of students, researchers and members of the general public. 4 reported themselves familiar with haptic technology and 10 to be advanced computer users. Several of them had casually experienced the SHK hardware while it was under development.

Experimental Design and Procedure

The study tested 3 conditions. Two used the normal mode and featured 6 and 9 item passwords. Respectively, these have a resilience to brute force and observation attacks of 3^6 (1/729) and 3^9 (19,863). The third condition used the hybrid mode and a 6 item password, weighted such that 55% of requests over the study asked for complementary responses. Correctly determining a password using purely brute force or visual attacks was therefore at a level of $1/(7^{(0.55*6)} * 3^{(0.45*6)})$ or 1/11941. The susceptibility to a brute force attack based on fully exploring the PIN items presented in compliment mode was 3^6 (1/729). Selecting these three conditions allowed the exploration of the tradeoff between using additional PIN items and more complex input mappings to increase security.

The study used a fully balanced repeated measures design with each participant completing each of the 3 experimental conditions in one of the six possible order conditions. Each experimental condition was composed of 10 trials, each taking the form of a complete PIN entry, and was preceded by a 6 trial practice condition. The experimental data is therefore based on a total of 10 PIN entries by 3 conditions by 12 subjects, or a total of 360 complete PIN entries composed of 2520 individual selection events.

Passwords were preset and presented to users at the start of the experiment using an iconic visual notation system illustrated in Figure 2. During the practice sessions, these visual representations were shown to reinforce learning, but were hidden during experimental sessions.

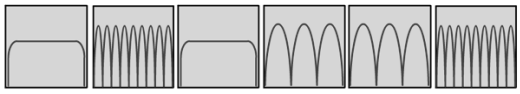

Figure 2. The iconic tacton PIN notation. Shows a 6 item PIN with the following tactons: Cont., 2Hz, Cont., 1Hz, 1Hz, 2Hz.

Participants were also exposed to a short informal introduction to the system and its cues prior to the start of the experiment. Earmuffs were worn throughout to minimize the impact of noise from the hardware and the entire experiment took approximately 30 minutes to complete.

The experimental measures included the time and correctness of explicit button selections and also the number and duration of contacts with the button surfaces (captured from the force sensors). Total trial time was measured from the first time a user touched a key after a trial commenced. Workload was measured using a NASA TLX questionnaire [5] administered after each condition.

Results

Median task completion times for the three experimental conditions are shown in Figure 3 (left). Medians were used to minimize the effect of outliers. An ANOVA revealed a significant trend in these data ($F(2, 11) = 39.6$, $p<0.001$) which was fully borne out by subsequent post-hoc pair-wise t-tests (all significant at $p<0.01$). Figure 3 (right) shows the errors in the form of mean percentage failed authentications. Although considerable differences are visible in the data, an ANOVA did not reveal a significant effect ($F(2, 11) = 0.9$, $p=0.37$), probably due to the high variance. Finally, the TLX data appear in Figure 4. A one-way ANOVA on overall workload showed a significant effect ($F(2, 11) = 4.67$, $p=0.016$).

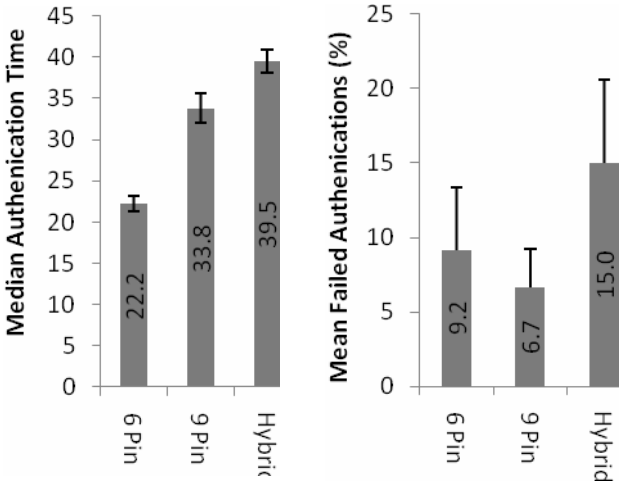

Figure 3. Task times & error rates from authentication study

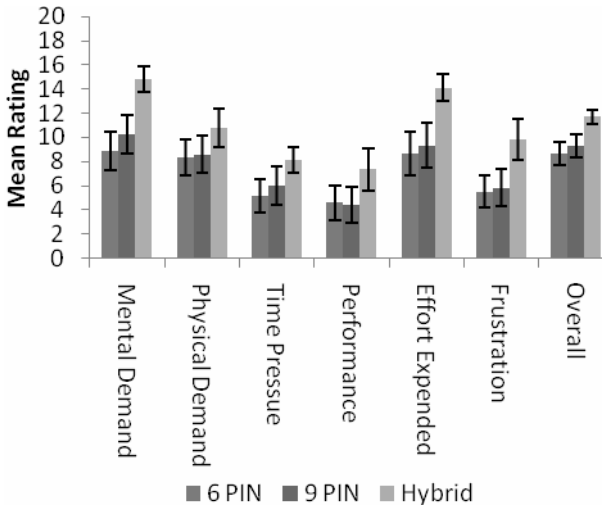

Figure 4. TLX data from authentication study.

DISCUSSION AND CONCLUSIONS

Performance was best using the normal mode with a 6 item PIN; this is unsurprising. However, contrasting these results to those in the 9 PIN condition is interesting. The 1.5 ratio between both the task completion times and number of PIN items suggests that users did not find entering additional PIN items to be more challenging. This notion is confirmed by the similarity in the error rate between these two conditions. This indicates that users found it relatively easy to remember the tactile PIN, recognize the tactons and physically use the system. This is an encouraging result supporting the concepts underlying the SHK. On the other hand, the hybrid condition performed worse than the other two conditions in both time and (non-significantly) in errors. The additional cognitive effort, visible in the TLX data, required to use this condition is likely to blame. As one participant remarked, "In the hybrid mode you need to remember what you have to do before choosing the right key". Sacrificing the normal mode's direct interaction (of finding a tacton and simply selecting its key) clearly added complexity to the task.

However, a caveat to this conclusion comes from comparing the results of this study with previous work. In particular, Undercover [9] is designed with highly similar goals to the SHK and also relies on tactile cues to obfuscate password entry. However, Undercover's median task completion times are reported to be 25-45 seconds, with a substantial number of users taking in excess of one minute to authenticate. Error rates for entire password entries are 26%-52%. In light of this data, performance using the uni-modal SHK looks highly promising. In particular the simple act of exploring tactons and immediately performing selection actions to enter PIN items in the same physical space appears rapid, easy to grasp and effective.

Future work on this system should tackle a number of pressing issues. For example, although designed to address visual observation, research on the SHK needs also consider its susceptibility to audio observation attacks which listen for the noise the vibration actuators produce. Tackling this may require exploration of a range of tactile technologies (such as piezoelectric pins) or the production of interference using conventional speakers. In a similar vein, more ecologically valid experimentation needs also take place. This will involve staging observation and recording attacks on SHK PIN entries in order to determine whether there is physical (or behavioral) evidence which allows an attacker to deduce a PIN. Exploring the memorability and learnability of tactile passwords is also a key area for future research. For example, determining retention rates for structured tactile passwords over time is a clear next step for this work. Finally, although user performance with the SHK represents an improvement over prior work, further development to optimize the system to maximize security while minimizing task completion times, errors rates and cognitive load is still required.

REFERENCES

1. Blonder, G. E. Graphical passwords. United States Patent 5559961, 1996
2. Brewster, S. A. and Brown, L. M. Non-visual information display using tactons. In *Ext Abs of CHI '04*. ACM, NY, 2004, pp. 787-788.
3. De Luca, A., von Zezschwitz, E., and Hußmann, H. 2009. Vibrapass: secure authentication based on shared lies. In *Procs. of CHI '09*. ACM, NY, pp. 913-916.
4. Giesen, L. ATM fraud: Does it warrant the expense to fight it? *Banking Strategies*, 2006, vol. 82, issue 6.
5. Hart, S. G., & Staveland, L. E. Development of a multi-dimensional workload rating scale. In *Human mental workload*, 1988, 139-183. Elsevier.
6. Kumar, M., Garfinkel, T., Boneh, D., and Winograd, T. Reducing shoulder-surfing by using gaze-based password entry. In *Procs of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*, vol. 229. ACM, NY, 2007, pp. 13-19.
7. Patel, S. N., Pierce, J. S., and Abowd, G. D. 2004. A gesture-based authentication scheme for untrusted public terminals. In *Procs of UIST '04*. ACM, NY.
8. Roth, V., Richter, K., and Freidinger, R. A PIN-entry method resilient against shoulder surfing. In *Procs of the 11th ACM Conference on Computer and Communications Security*, *(CCS '04)*. ACM, NY, 2004.
9. Sasamoto, H., Christin, N., and Hayashi, E. Undercover: authentication usable in front of prying eyes. In *Procs of CHI '08*. ACM, New York, NY, 2008, pp. 183-192.
10. Tan, D. S., Keyani, P., and Czerwinski, M. Spy-resistant keyboard: more secure password entry on public touch screen displays. In *Procs of the 17th Australia Conference on Computer-Human interaction* , pp. 1-10.
11. Wickens, C. D. & Hollands, J. G. Engineering Psychology & Human Performance, 2000, Prentice Hall.