The Haptic Wheel: Design & Evaluation of a Tactile Password System

Andrea Bianchi
Korea Advanced Institute of Science and Technology
373-1 Guseong-dong
Yuseong-gu, Daejeon
305-701 Korea
andrea@kaist.ac.kr

Jong Keun Lee
Korea Advanced Institute of Science and Technology
373-1 Guseong-dong
Yuseong-gu, Daejeon
305-701 Korea
mango@kaist.ac.kr

Ian Oakley
Madeira Interactive Technologies Institute
University of Madeira
Campus Universitario da Penteada
Funchal, 9000-390, Portugal
ian@uma.pt

Dong Soo Kwon
Korea Advanced Institute of Science and Technology
373-1 Guseong-dong
Yuseong-gu, Daejeon
305-701 Korea
kwonds @kaist.ac.kr

CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.
ACM 978-1-60558-930-5/10/04., USA.

Abstract
Authentication through passwords in public spaces (such as in ATMs) is susceptible to simple observation attacks, such as shoulder surfing, which can result in the password being compromised and ultimately the exposure of users to fraud and theft. Haptic technology, which can present information non-visually to users, offers a potential solution to this problem through the creation of tactile passwords. Situated in this space, this paper presents the design and initial evaluation of a novel haptic device, the haptic wheel, which displays tactons, or structured tactile messages, to enable password entry. It describes this device and the tactile passwords it supports in detail before presenting two short user studies. The results of these reveal that the chosen tactons are easily identifiable and that password entry times are significantly improved compared to previous systems based on haptic authentication.

Keywords
Tactile UI, non-visual interaction, security, PIN entry.

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

General Terms
Security, Experimentation, Human Factors.

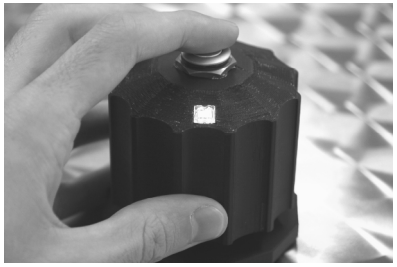

Figure 1. The Haptic Wheel hardware

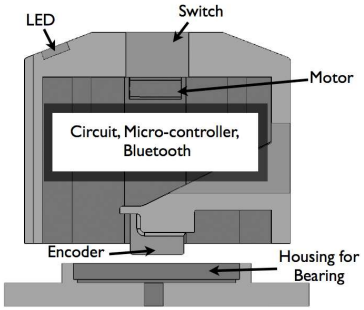

Figure 2. Cross section of the Haptic Wheel hardware

Introduction

Authentication through entering numerical codes and passwords in public spaces is common; bank ATMs are the most prominent example and are used on a daily basis by millions. However, it is a paradigm inherently exposed to a very simple attack: PIN theft via surveillance from a nearby observer (e.g. shoulder surfing) or concealed recording equipment. This is a serious issue, resulting in an estimated loss of 60 million dollars annually in the USA [4].

Addressing this attack vector, a number of recent research prototypes have explored authentication mechanisms which rely on haptic (or touch) cues to visually conceal or encode PIN entry. These attempts can be divided into two main groups. In the first, a tactile signal is used to obfuscate or complement regular password entry. Such multimodal systems typically combine a hidden haptic challenge with the input of a visually observable password. Examples include the use of pressure as an input modality during otherwise observable authentication [5] and the use of tactile cues delivered to one hand to modulate the input of password items entered by the other [6]. In the second group, password entry is uni-modal, relying solely on haptic cues. Examples of such systems include the Secure Haptic Keypad [2] (which uses passwords composed solely of a series of discrete vibration patterns) and Alsulaiman et al.'s [1] haptic signature authentication system (which relies solely on the physical cues produced while the signature is being written rather than the final visual artifact).

Although a promising paradigm, these systems typically feature long authentication times and high error rates – multimodal PIN entry systems feature PIN entry times in the order of 25-45 seconds and with error rates of 26-52% [6]. Recent research suggests that simpler uni-modal systems may support better performance, with entry times in the range of 30 seconds and with errors rates of 10-15% [2]. However, these figures still compare poorly to standard numerical or graphical PIN entry and further research is clearly required before such systems offer a level of usability and performance, which can match user expectations and requirements.

This paper attempts to address this challenge. It introduces a novel uni-modal haptic password entry system based on tactile cues delivered through the haptic wheel, a bespoke dial control (Figure 1). The ultimate aim of this work is to create a secure tactile password system which meets real world requirements in terms of PIN entry time, error rate and cognitive load. The remainder of the paper is structured as follows: the hardware and system implementation details are introduced; two short user studies are discussed; avenues for future work are explored.

System Description

The haptic wheel hardware (figure 2) is a dial which can make continuous (unbounded) revolutions. It features two internal vibration motors capable of rendering a range of tactile cues, a selection button mounted on its top center and a diode which indicates device status. Physically, it is a standalone 3D printed handle (resembling the rotary control of a safe) which turns on a slim base and integrates all required electronic components: rotary encoders, selection button, a bearing, pager motors, Arduino microcontoller, Bluetooth communications, battery and charging circuits. It is controlled by software written in the Arduino framework and Java (on a host PC).

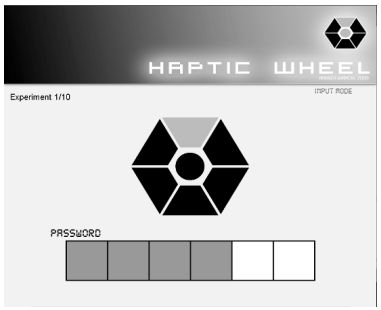

Figure 3. Screenshot of the Haptic Wheel software GUI

Interaction with the haptic wheel takes place through rotational movements in both clockwise and anti-clockwise directions. In software its angular input space is segmented into a continuous loop of non-overlapping targets. Each is 56° in size, a figure selected to minimize error rates and selection times through informal and subjective experimentation by one of the authors. In this system, a password item is entered through rotating the device to a particular target and making a selection operation using the top-mounted button. A password is composed of a sequence of such item selections.

However, the haptic wheel provides no visual feedback as to the current target. Instead, this information is provided through structured tactile cues, or tactons [3], which can be felt through the casing when the device is held during normal operation. A simple range of tactons was designed for this device based on activating its vibrating motors to the maximum strength at an ascending range of frequencies from fully off (no-activation) through regular oscillations at 2Hz, 4Hz, 16Hz to continuous activation. These tactons are always assigned to the wheel's targets in an ordered manner such that clockwise rotation corresponds to an increase in frequency and anti-clockwise motion to a decrease. The sequence of cues also wraps around, so that a clock-wise rotation from the final (highest frequency tacton) will transition to the first (lowest frequency) tacton and vice-versa.

However, although it involves no explicit visual information, this tactile channel is not by itself secure against observation attacks. For example, through recording a user's motions during PIN entry, much of the structure and content of a password could be inferred. To tackle this problem, the haptic wheel system randomizes the position of the sequence of tactons, but maintains their ascending order, after every item entry. Through such a manipulation, the movements made to select a given set of tactons are rendered uninformative about the identity of individual tactons it is composed of. Each time a tacton needs to be entered, a user must actively search for it afresh and its position bares no relationship to its position during the previous item entry. Maintaining the ascending order of the tactons through this randomization simplifies the resulting search task. At the start of each item entry, users need only identify the tacton currently being displayed in order to make a decision as to the location of the next tacton in their password and the movement they need execute in order to reach it.

The haptic wheel system also features a simple PC based screen user interface. This is used to present state information about the password entry, including the number of PIN items already input and the point at which rotational movements cause a transition between adjacent targets. This interface presents no information about the tactile content of each target and features six 60° segments (approximately the same size as the control targets). Choosing a number of visual targets greater than the number of tactons was an explicit choice aimed at reducing user's tendency to relate particular tactons to particular on screen targets. The goal of this screen UI is to minimize the cognitive load of users by providing feedback which helps structure their tacton search and password entry tasks without compromising the resilience of the system to observation attacks. A screen shot of this system can be seen in Figure 3.

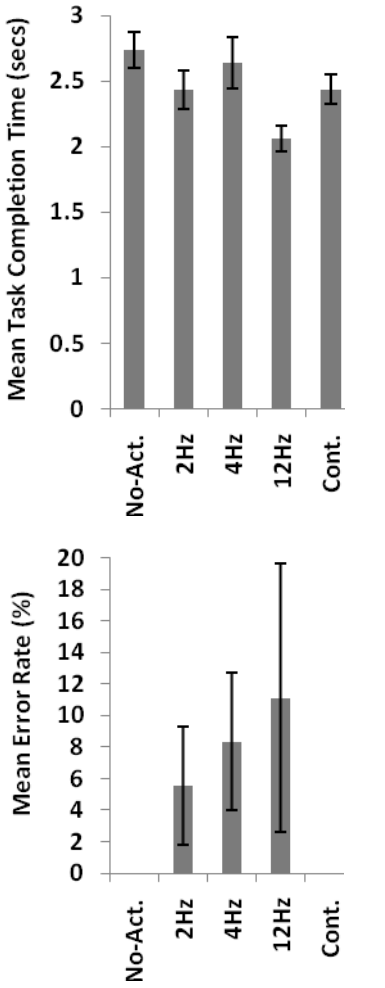

Figure 4. Mean task completion time (top) and percentage error rate (bottom) during pilot study on tacton recognition. Bars show standard error.

Haptic Wheel Password Design and Security Analysis
The goal of this work is to build an interface resilient to both observation and brute-force attacks. In line with other researchers [2, 6], an adequate level of security is defined as a password which can be guessed, via either of these attacks, with a probability of no more than 1 in 10,000. This figure also has real world validity: it is the strength of common 4 digit ATM PINs against brute force attacks.

The design of haptic wheel password system aims to provide no visual clues as to the PIN items entered. It does this by randomizing the tactons assigned to each target zone for every item entry. Consequently, both brute-force and visual observation attacks (both shoulder surfing and recording) occur with the same probability. An observer is presented with no clues as to the tacton a user is currently feeling and is not able to infer (from subsequent rotations or selections) what tacton has been selected, reducing visual observation attacks to same level of sophistication as brute force attacks.

The probability with which passwords can be broken in the haptic wheel system is therefore $1/t^k$, where t is the number of tactons available in a password and k is the length of that password. Based on this formula, two password variants were designed: a password based on the full set of five tactons (no-activation, 2Hz, 4Hz, 12Hz, continuous activation) with a length of six items and a password based on a reduced set of three tactons (no activation, 2Hz, 4Hz) with a length of nine items. Respectively, these have strengths of $1/5^6$ (1 in 15625) and $1/3^9$ (1 in 19683), exceeding the minimum requirements identified at the start of this section.

Evaluation

The evaluation was composed of two separate studies, each completed by the same set of participants. The first experiment was a pilot intended to ascertain recognition rates and times for the tactile cues. The second test evaluated user performance during PIN entry. It took participants approximately 40 minutes to complete.

Participants
12 participants were recruited for this study. They had a mean age of 25.6 (SD 3.44), two were female and ten male. They were a mix of researchers, students and administrative staff, all of whom worked at one of our institutions. 11 reported themselves to be familiar with haptics and 8 to be advanced computer users.

Pilot
The pilot study used a reduced version of the hardware consisting of a single vibrotactile actuator capable of rendering the set of tactons designed for the haptic wheel. It was based around a simple experimental structure. In each trial, participants were exposed to one of the five tactons at random, which they were then required to identify using a simple mouse-based GUI which showed graphical representations of cue frequency. In total, every user was presented with a total of 20 trials split into four blocks composed of one presentation of each of the five tactons. The first block served as practice. Task completion time and errors (in the form of incorrect identification of tactons) were measured. During the study participants wore headphones and listened to pink noise to block any possible vibration sound from the actuator.

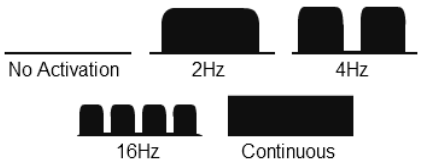

Figure 5. Graphical notation used to visually represent the tactons in both user studies.

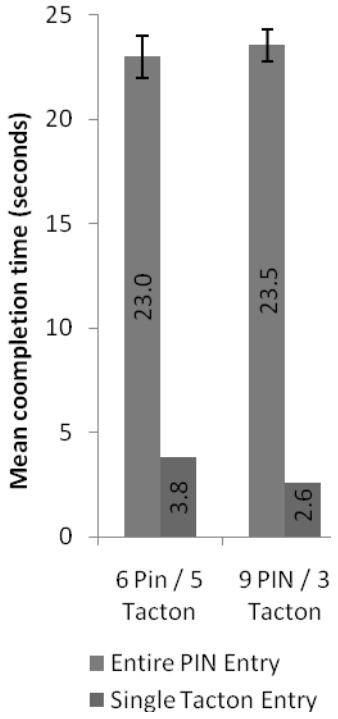

Figure 6. Mean task completion times from haptic wheel experiment. Shows both PIN entry time & (derived) tacton entry time). Bars show standard error.

The results of this experiment are shown in Figure 4. A one way ANOVA revealed significant differences in the task completion time for the tactons ($F(4, 11) = 3.39$, $p=0.01$). Post-hoc t-tests confirmed that the 12Hz tacton was identified more rapidly than both the no-activation and 4Hz tactons and the continuous tacton more rapidly than the no-activation tacton. A one-way ANOVA on the mean error rate showed no significant differences ($F(4, 11) = 1.16$, $p=0.33$). The overall mean task completion time and error rate for all tactons was 2.46 seconds and 5%, respectively.

In summary, these results indicate tacton identification was both rapid and accurate. They are also broadly comparable with the previous literature [2], suggesting the tactons are easy for users to recognize. This is an encouraging result. Although the data is insufficient to draw firm conclusions, there is evidence suggesting a trade-off between the task completion times and error rate with the 12Hz tacton, highlighting the importance of carefully selecting and evaluating such tactons.

Haptic Wheel Experiment

Encouraged by the results of the pilot, an initial PIN entry study was conducted. This examined a pair of conditions, involving the two password formats introduced previously (5-tacton/6-item and 3-tacton/9-item). The goals were to capture basic user performance with the system (to compare against the state of the art) and to explore the tradeoff between password length (i.e. the number of PIN items) and password complexity (i.e. the size of the set of tactons).

The study used a fully balanced repeated measures design splitting the 12 participants into two equally sized order conditions. Each trial took the form of a complete PIN entry and each condition was composed of a 7 trial practice session followed by a 10 trial test session. The empirical data is therefore based on 10 PIN entries by 2 conditions by 12 subjects for a total of 240 complete PIN entries composed of 1800 individual tacton selection events. Objective measures included individual tacton entry time (and by inference PIN entry time) and error rate (in the form of selection of an incorrect tacton). At the end of each condition, participants completed a NASA TLX questionnaire, an established instrument which measures workload.

Random passwords were assigned to participants at the beginning of experiment. These were shown using a simple illustrative graphical notation (shown in Figure 5) based on the ascending frequency of cues and replicated from the GUI in the pilot study. Participants were also exposed to a short informal explanation of the working principles of the system prior to starting the experiment. Finally, participants wore headphones and listened to pink noise to mask any sounds from the actuators for the duration of the experiment.

Results

Mean task completion time for PIN entry sessions (and individual tactons) is shown in figure 6 The error rate (in terms of entire authenication sessions) was 16.4% for the 6 PIN/5 tacton condition and 18.1% for the 9 PIN/3 tacton condition. Paired t-tests did not yield significant results for either time or errors ($p=0.46$ and $p=0.86$ respectively). Analysing the different control inputs made using the wheel enabled the breakdown of task completion time into two distinct activities: Action Time, or the time spent rotating the device and Tacton Recognition Time, or the time spent dwelling on the

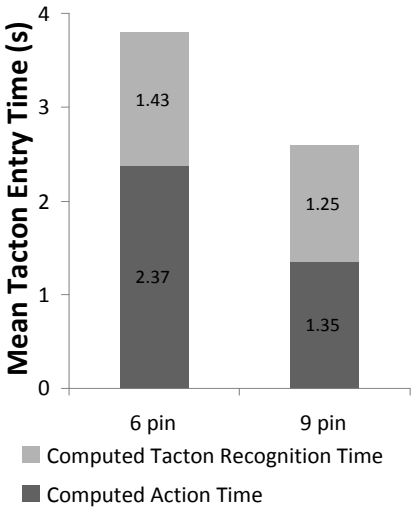

Figure 7. Single Tacton Entry times split in Tacton Recognition and Action Time.

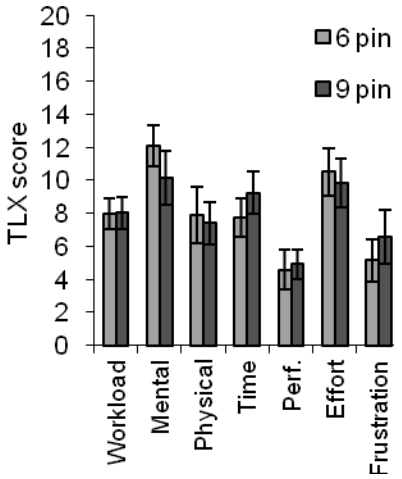

Figure 8. NASA TLX results.

final tacton prior to selection. These data are shown in Figure 7. The mean number of rotation actions performed was 1.95 in the 6 PIN/5 Tacton condition and 0.93 in the 9 PIN/3 tacton condition. Finally, the TLX data are shown in Figure 8. A paired t-test on overall workload was not significant ($p=0.97$).

Discussion

No significant difference in PIN entry performance, including time, errors and workload, was detected between the two conditions. However, at the level of the recognition of individual tactons, there is clear evidence of a temporal tradeoff: a larger set of tactons results in an increased completion time per tacton. While unsurprising, it is interesting to note that this increase is largely due to the additional cost of navigating between tactons and that actual dwell times on the final target are considerably below the tacton recognition times reported in the pilot study. Furthermore, tacton recognition times are also relatively similar between the two conditions. Taken together these facts suggest that participants were able to use the structured order of the tactons to simplify their search task and attain a good level of temporal performance. The mean authentication time of 23 seconds also represents an improvement over previous systems using both multi-modal [6] and uni-modal [2] approaches of between 10% and 50%. Error rates in the system are comparable to much of the previous research, but still require reduction before viable real world systems can be produced. Although the current study cannot provide an explanation of this behavior, it is worth noting that key problems occur in the first and last PIN digits where, respectively, 42% of errors occurred in the 6 PIN/5 tacton condition and 52% of errors in the 9 PIN/3 tacton condition.

Future work on this topic needs explore this issue. Other avenues for investigation include further combinations of PIN length and tacton set size (e.g. 7 PIN/4 tacton) and the production and validation of a GOMS style formula for predicting user performance. Issues of memory and long term system use are also important; a subsequent session with two of the current experimental participants resulted in no errors, but a more serious treatment of this issue is urgently required. In summary, the work presented in this paper makes steps towards the production of a rapid, robust, reliable and secure non-visual authentication system; further work is required to fully realize this vision.

References

[1] Alsulaiman, F. A., Cha, J., and Saddik, A. User Identification Based on Handwritten Signatures with Haptic Information. Lecture Notes In Computer Science, Springer, vol. 5024, pp,114-121, 2008.

[2] Bianchi, A., Oakley, I., Kwon, D.S., The Secure Haptic Keypad: Design and Evaluation of a Tactile Password System. In Proceedings of CHI '10, 2010.

[3] Brewster, S. A. and Brown, L. M. Non-visual information display using tactons. In Ext. Abs. of CHI '04, ACM, New York, NY, 2004, pp. 787-788.

[4] Giesen, L. ATM fraud: Does it warrant the expense to fight it? *Banking Strategies*, 2006, vol. 82, issue 6.

[5] Malek, B., Orozco, M., Saddik, A., Novel shoulder-surfing resistant haptic-based graphical password. In Proceedings of EuroHaptics, 2006.

[6] Sasamoto, H., Christin, N., and Hayashi, E. Undercover: authentication usable in front of prying eyes. In Proceedings of CHI '08. ACM, New York, NY, 2008, pp. 183-192.