Leveraging Motor Learning for a Tangible Password System

Martez E. Mott
Computer Science Department
Bowling Green State University
Bowling Green, OH 43402 USA
memott@bgsu.edu

Thomas J. Donahue
Computer Science Department
Bowling Green State University
Bowling Green, OH 43402 USA
donahut@bgsu.edu

G. Michael Poor
Computer Science Department
Bowling Green State University
Bowling Green, OH 43402 USA
gmp@bgsu.edu

Laura Leventhal
Computer Science Department
Bowling Green State University
Bowling Green, OH 43402 USA
leventha@bgsu.edu

CHI'12, May 5–10, 2012, Austin, Texas, USA.
ACM 978-1-4503-1016-1/12/05.

Abstract
Tangible user interfaces (TUIs) may allow users to have more direct interaction with systems when compared to traditional graphical user interfaces (GUIs). However, the full range of applications where TUIs can be utilized in practice is unclear. To resolve this problem, the benefits of TUIs must be analyzed and matched to an application domain where they hold advantages over more traditional systems. Since TUIs require users to use their hands in order to interact with the system, there is the possibility for these systems to leverage motor learning to help users perform specific tasks. In this paper we will describe an early attempt to understand how motor learning can be used to create a tangible password system. A novel tangible password system was created and a small study conducted in order to identify future research objectives.

Author Keywords
Tangible Interaction; motor learning; passwords

ACM Classification Keywords
H.5.2 [Information Interfaces and Presentation]: User Interfaces – Interaction styles

General Terms
Experimentation, Human Factors

Introduction

The popularity of tangible user interfaces (TUIs) has grown rapidly, becoming an important component of many devices (smartphones, tablets, etc). As their popularity grows, so does the need to develop and test new TUIs to discover their benefits over more traditional systems. Attempts have been made by the research community to develop tools and frameworks to aid in the development, implementation and evaluation of TUIs [8, 12]. While these efforts have helped to identify common methodologies to design and test systems, the nature of the advantages of TUIs remain unclear [5, 13].

Many researchers [6, 7] agree that TUIs may offer numerous advantages over GUIs. One advantage is the capability to retain knowledge through physical interaction with the TUI, allowing the system to potentially capitalize on users' motor learning capabilities. Motor learning is essential in the development of motor skills, from everyday tasks, such as walking, to advanced tasks like playing a piano [11]. TUIs can leverage motor learning for applications where recall is an essential process. One possible application domain is usable security, where researchers strive to create systems where passwords are easier to remember. If motor learning is leveraged properly, tangible password systems may be a possible alternative to alphanumeric password systems. Through repeated physical manipulation of the TUI, a user can store a password in their procedural memory [14]. This type of system can reduce the cognitive load placed on users who are often required to remember long and obscure passwords.

This paper presents an exploration of motor learning for tangible interaction by describing a novel tangible password system and a small study conducted to evaluate user performance while interacting with the system. As our research is still in its early stages, this system will help us identify issues which may arise while attempting to create a tangible password system which hopes to leverage motor learning.

Related Work

Although there is no clear definition of what constitutes a tangible password system, closely related works include systems where haptic technology is used as the primary password identification mechanism and gesture based systems where the gestures are performed with the input device, not on a screen.

Haptic Password Systems

Two systems that include the use of haptic technology are the Haptic Wheel [1] and the Secure Haptic Keypad [2], both of which are aimed at secure authentication in public spaces. In these systems passwords are given in the form of a series of vibrotactile cues called tactons. To interact with the system, users place their fingers on three keys (Haptic Keypad) or their hand around a rotary dial (Haptic Wheel). After each individual entry, the vibrations emitted from the keys, or the dial, are randomly changed. The randomization of the vibration patterns is vital as it protects the system from outside observation, but it does not give the user the ability to recall their password from constant physical interaction with the device. Instead, users must remember a haptic password the way they remember an alphanumeric password.

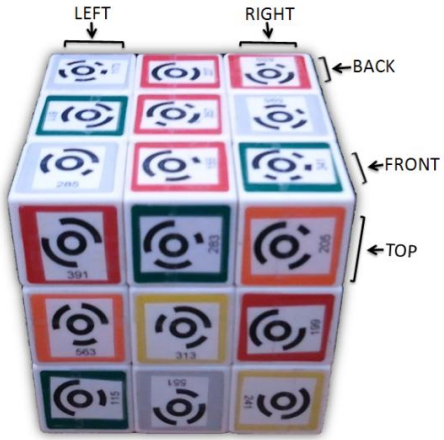

Figure 1. TangibleRubik, in orientation held by participants, identifying the faces as in the passwords

Gesture Based Authentication Systems
Gesture based authentication systems, which require the user to perform gestures by physically manipulating a device, are often suitable for small mobile devices with accelerometers (e.g. smartphones and media players) [9]. GesturePIN [3] is a mobile authentication system that gives users the ability to generate passkeys by performing gestures on their mobile device. Gestures consist of a series of three-dimensional (3D) directional movements (e.g. tilt device left). A benefit of the system is the direct physical control of the gestures, making them easy for users to recall when they choose to generate a PIN. However, this system does not require the user to recall any specific series of gestures, allowing users to generate passkeys on the fly and requiring users to only recall a small subset of possible gestures.

Summary
Haptic and gesture based passwords offer some of the same advantages of TUIs, primarily the ability for the user to use his or her hands in a nonconventional keyboard/mouse interaction. However, these applications do not take full advantage of the user's motor learning capabilities.

TangibleRubik

TangibleRubik is a novel attempt to create a tangible password system which takes advantage of a user's motor learning capabilities. This system was created to further understand the advantages of such a system and to identify areas for improvement.

Description
TangibleRubik allows users to physically manipulate a Rubik's Cube for authentication to a system. The various combinations of moves act as the users' password. By having users physically manipulate the cube, the system takes advantage of humans' innate ability to recall motor actions through repetition.

Implementation
TangibleRubik is implemented using a Rubik's cube (4 x 4 x 4 inch) augmented with barcode like symbols called TopCodes [4]. These codes are detectable using a standard webcam and allow the system to determine the code's location and orientation. A code is placed on each block of the cube for a total of 54 distinct codes. Before each password entry attempt, the system must know the current location of the codes on each face. This is accomplished by a scanning process where the webcam takes a snapshot of each side of the cube. This allows the system to create an internal representation of the cube's current state. The system carries out the user's password on the internal representation of the cube to determine the correct final cube state.

A user's password consists of a series of moves which can be performed on the cube. Passwords are given in the form a sequence of letter pairs. The first letter represents which face of the cube to alter and the second represents the direction of rotation in relation to the user. Each face is given an orientation description (see Figure 1) and each move is given a rotation description (Right, Left, Front and Back). For example, the password, LB, BR and TL, would instruct the user to first rotate the left face towards the back, then rotate the back face towards the right, and finally rotate the top face towards the left (or counter-clockwise). Users are limited to moves that alter the codes or the location of the codes on the top face (10 moves in total). The user must perform the moves in the order in which

they are given, failure to do so will result in a failed authentication attempt. After performing their password, the user scans the top face of the cube. If the codes present on the top face of the user's cube matches with the internal cube, then the authentication was successful.

Method

To test our system we performed a preliminary study, the goal of which was to determine if users could use the system to accurately and quickly enter their password. A second goal was to determine what effect differing password lengths would have on a user's ability to recall their password after being removed from the system for a brief period of time.

Predictions

We predicted users given passwords of longer length would have a higher error rate during both training and experimental trials, as well as a higher fail rate on final authentication attempts.

Participants

Eleven college student participants (7 men, 4 women) with a mean age of 22, volunteered for this study. All participants reported they had some experience with tangible interfaces (e.g. tablets, smartphones, Nintendo Wii remote, etc.).

Experimental Design

The study tested 2 conditions using a between subjects design. 6 participants in the first condition were given a 7 move password and 5 participants in the second were given a 10 move password.

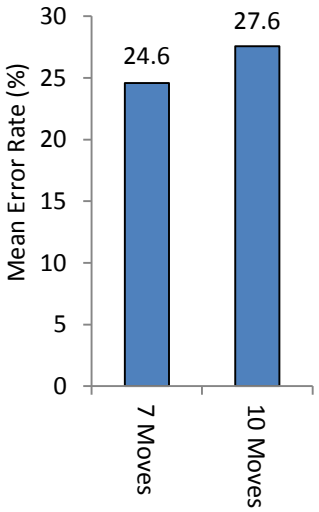

Figure 2. Mean error rate

Each participant completed a training session requiring him or her to successfully enter their password three consecutive times before moving on to the experimental trials. Textual representations of the passwords were visible to the user at all times during the training trials. This was done to aid in the learning of the password. All participants were given an introduction to the system and an explanation of their password.

Experimental trials directly followed training and required participants to correctly enter their password five consecutive times. This objective criterion was chosen to ensure that all participants had achieved the same level of competency, by the end of the experimental trials, in storing their password to memory. After the experimental trials, participants were given a distractor task, which consisted of a word search, to mentally remove them from the experimental task for a duration of 10 minutes. After the distractor task, participants were asked to enter their password a final time as a test of password mastery.

Performance measures collected during the study include the number of failed and successful authentication attempts in the training and experimental trials, and time to enter a password. The NASA Task Load Index (TLX) [10] questionnaire, measured the workload placed on the participant during the experiment.

Results

Comparing between the two password length conditions, no significant differences were found between the error rates in either the training and

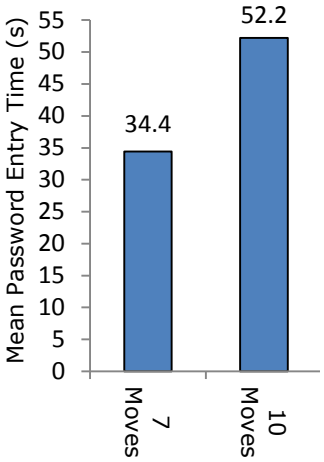

Figure 3. Mean password entry times

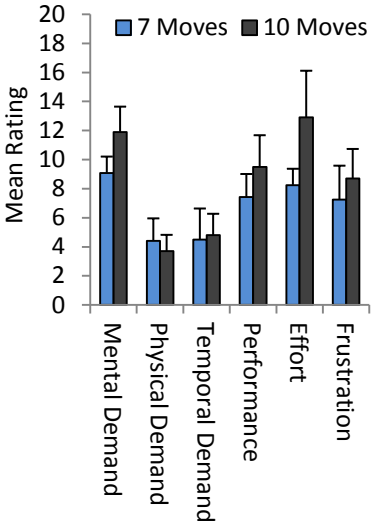

Figure 4. Summary of results from the NASA TLX

experimental trials, as shown in Figure 2. Similarly, performance on normalized (by password length) time-per-move on the final authentication attempt was not significant by condition. It should be noted that on the final authentication attempt, all participants were able to successfully enter their password after the distractor task. Mean password entry times for the two experimental conditions are shown in Figure 3, though there was no significant difference found by condition. No significant differences were found between groups in the TLX questionnaire data. However, correlation data revealed a significant positive correlation between both physical demand ($R(9) = 0.74$, $p < .05$) and frustration ratings ($R(9) = 0.74$, $p < .05$) with the normalized time-per-move on the final authentication attempt.

Analysis

Error rates during the experimental trials were surprising due to our prediction that participants in the 10 move condition would experience significantly higher error rates than those in the 7 move condition. This indicates that participants were able to utilize longer passwords just as effectively as users with shorter passwords. Although error rates are higher than we hoped, this may be an artifact of participants adjusting to a new system. Given that all participants were able to recall their password after performing the distractor task; this suggests participants were successful in storing their password in memory (at least for the short term). This result is promising as it shows users have the capability to learn and recall passwords of considerable length. The correlation between frustration, physical demand and the normalized time-per-move suggest TUIs which require users to perform task they find to be physically demanding can have a cascading effect, leading to higher frustration levels and longer password entry times.

Discussion

Our exploratory study provided useful information which identified items which must be addressed and will determine future research objectives. The first is password entry time. Mean entry times of 34 and 52 seconds are too long and must be shortened in order to be used in practice. The second is password memorability. Participants were able to recall their password after being removed from the system for ten minutes, but participants should be able to remember their passwords for weeks and months. The third is the ease in which someone can observe a person entering their password. This jeopardizes the security of the mechanism and may pose a critical security problem the same way shoulder-surfing has impacted authentication in public places.

To address these issues more research needs to be completed which evaluates a user's ability to recall their password over a longer duration. This study must also compare the memorability of the tangible password to other types of passwords. The type of manipulated object used to enter the password may also be altered. This may lead to significantly reduced password entry times and increased resistance to password observation.

Conclusion

In this paper we have presented an early examination of an exploratory tangible password system. The goal of this research is to understand how a tangible password system can leverage motor learning in order to reduce cognitive load placed on users and allow

them to utilize longer passwords. Our study shows that users can recall 7 and 10 length passwords after being removed from the system for a short time. These results indicate that tangible passwords which leverage motor learning may have the capability to become a suitable alternative to alphanumeric systems. More research is needed by the HCI and Security communities to determine how this type of tangible password system can be better utilized in practice.

Acknowledgements

Guy W. Zimmerman, Brianna J. Tomlinson and Samuel D. Jaffee

References

[1] Bianchi, A., Lee, J.K., Oakley, I., Kwon, D.S. The Haptic Wheel: Design & Evaluation of a Tactile Password System. *Ext. Abstracts CHI 2010*, ACM Press (2010), 3625-3630.

[2] Bianchi, A., Oakley, I., Kwon, D.S. The Secure Haptic Keypad: Design and Evaluation of a Tactile Password System. *Proc CHI 2010*, ACM Press (2010), 1089 – 1092.

[3] Chong, M.K, Marsden, G. and Gellerson, H. GesturePIN: using discrete gestures for associating mobile devices. *Proc MobileHCI 2010*, ACM Press (2010), 261 – 264.

[4] Horn, M. TopCode: Tangible Object Placement Codes. http://users.eecs.northwestern.edu/~mhorn/topcodes/

[5] Hornecker, E., Jacob, R., Hummels, C., Ullmer, B., Schmidt, A., van den Hoven, E. and Mazalek, A. TEI goes on: Tangible and embedded interaction. *IEEE Pervasive Computing Magazine/Journal*, 7(2). 91-95.

[6] Fitzmaurice, G.W., Ishii, H. and Buxton, W. Bricks: Laying the Foundation for Graspable User Interfaces. *Proc CHI 1995*, ACM Press (1995), 442-449

[7] Ishii, H. and Ullmer, B. Tangible Bits: Towards Seamless Interfaces between People, Bits and Atoms. *Proc CHI 1997*, ACM Press (1997), 234 – 241.

[8] Israel, J.H., Belaifa, O., Gispen, A. and Stark, R. An Object-centric Interaction Framework for Tangible Interfaces in Virtual Environments. *Proc. TEI 2011*, ACM Press (2011), 325-332.

[9] Patel, S.N., Pierce, J.S, Abowd, G.D. A gesture-based authentication scheme for untrusted public terminals. *Proc UIST 2004*, ACM Press (2004), 157 – 160.

[10] NASA TLX: Task Load Index. http://human-factors.arc.nasa.gov/groups/TLX/

[11] Schmidt, R.A. A Schema Theory of Discrete Motor Skill Learning. *Psychological Review*, (1975). 82(4), 225-260.

[12] Shaer, O. and Jacob, R. A specification paradigm for the design and implementation of tangible user interfaces. *Transactions on Computer-Human Interaction*, ACM Press (2009), 16(4).

[13] Shaer, O. and Hornecker, E. Tangible User Interfaces: Past, Present, and Future Directions. *Foundations and Trends in Human-Computer Interaction*, Now Publishing (2010), 3(1-2).

[14] Willingham, D.B., Nissen, M.J., and Bullemer, P. On the Development of Procedural Knowledge. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, American Psychological Association (1989), 15(6), 1047-106