Haptic Security PIN Entry System Using Magnetic Repulsive Force

Andrea Bianchi
KAIST
Daejeon, Korea
andrea@kaist.ac.kr

Ian Oakley
Madeira ITI
Funchal, Portugal
ina@uma.pt

Dong Soo Kwon
KAIST
Daejeon, Korea
kwonds@kaist.ac.kr

ABSTRACT
The security of authentication processes in public spaces is undermined by the risk of observation attack. One solution to this problem is the use of non-visual, haptics based authentication techniques. However, despite the recent development of numerous haptic authentication methods the technology underneath these systems is still based on mechanical movable parts, which emit sound. By recording the leaked sound and analyzing the patterns, an attacker can potentially recover the original password or PIN, reducing or minimizing the beneficial aspects of haptic-based authentication methods. This paper proposes a technical solution to this problem by introducing a simple haptic input device based on the electromagnetic repulsive force generated between magnets and digitally controlled solenoid coils. This interface does not leak auditory information and is suitable for use with authentication techniques and processes previously presented in the literature.

Author Keywords
Haptic, Security, PIN entry, Authentication, Magnetic.

ACM Classification Keywords
H.5.2 User Interfaces: Input devices and strategies.

INTRODUCTION
Authentication in public spaces through terminals or private devices is commonplace. This fact is illustrated by the widespread presence of passwords and PINs as authentication mechanisms that are employed daily by million of users. However, the ubiquity of these methods also leads to a high exposure to malicious attacks, especially for those cases where a password or PIN is the getaway to important information (such as an electronic bank account). As an example, the annual loss from ATM fraud in the USA is estimated to be 60 million USD [8].

Both public terminals and private devices used in public spaces are commonly subjected to attacks based on observation [6]. The risks associated with observation of a PIN (whether peeping over someone's shoulder, unintentionally looking or using recording equipment) while accessing secure data is so highly regarded in the security community that numerous authentication methods based on non-visual information have been proposed. In particular, a range of haptic based authentication systems that do not rely on the display of visual information, and are therefore are inherently unobservable, have been recently introduced [e.g., 1, 2, 3].

However, current haptic-based PIN entry methods are typically based on technology that relies on mechanical movable parts (vibration motors [e.g. 1, 7], PIN arrays [e.g. 9] and servo motors [e.g. 10]) to generate cues. This opens the door to a new type of observation attack based on recording and analyzing the auditory information emitted by the mechanical parts of the haptic actuators. A similar audio attack based on recording and analyzing the noise generated by typing on a standard keyboard has been shown to reliably yield correct passwords [11], suggesting these concerns are well-founded.

Addressing this issue, this paper introduces ongoing work on a new hardware haptic interface based on the electromagnetic repulsive force between magnets and digitally controlled solenoid coils. This actuation method is silent and the interface we propose can be easily applied to a recently developed authentication technique based on repeated presentations of a simple, single haptic cue [4].

RELATED WORK
Several researchers have explored techniques to make haptic-based authentication on terminals or mobile devices less susceptible to observation attacks. A first family of methods is based on recognizing and selecting a specific sequence of structured, temporally varying patterns of vibration (often called tactons [5]). Examples of this interaction technique are provided by Bianchi et al. [1, 2, 3]. A second related set of methods is based on spatially, rather than temporally, varying tactile cues. Examples of this technique include the pin array authentication system developed by Kuber et al. [9] and the servo motor based system proposed by Sasamoto et al. [10]. Finally, there is a class of interfaces that uses haptic information displayed as a single cue rather than encoded structured pattern. Examples include de Luca's Vibrapss [7], a system that relies on the presence of a simple haptic vibration to modulate entry of a standard password, and Bianchi et al.'s Spinlock [4] which encodes a password as a sequence of repeated pulses of vibration in response to continuous rotary input.

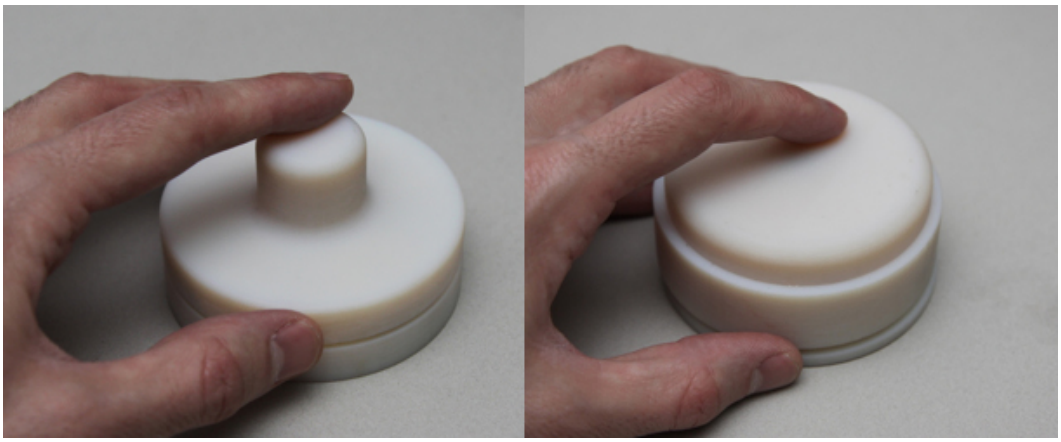

Figure 1. Two design variations of the hardware wheel that explores various size handles for creating different torques.

The Spinlock system is a key motivator for this work. It takes the form of a phone prototype based on the dial-lock of a safe, in which passwords are composed of a sequence of data items specified by direction of motion (clockwise or anti-clockwise) and number of pulses of haptic vibration that are displayed. By counting the number of cues in response to movement users are able to enter structured data in the form of direction-count pairs. In this paper we introduce the prototype of a physical interface that can satisfy the input/output requirements of this technique, but that substitutes the pulse of vibration (which generates noise) with a haptic cue generated by repulsive magnetic force. Production of such a cue should reduce or eliminate the noise emitted by the device.

HARDWARE DESIGN AND PROTOTYPE

The hardware prototype is an evolution of the Haptic Wheel [1], a custom made electronically controlled wheel interface for public terminals that features an internal pager motor to generate vibrotactile stimuli, an encoder to track the rotation, and a button to trigger a selection. This wheel was used to display a secret PIN as a sequence of vibration patterns. However, one of the limitations of such approach is that the internal pager motor causes noise, exposing the PIN to an attack with microphones - by capturing the sound of the motor during an authentication process, an attacker could recover the user's PIN. The hardware presented in this paper addresses this limitation and provides a method to generate tactile feedback that is inaudible, even with microphones.

This is achieved by using a combination of magnets and solenoid coils in order to create a bump-like haptic effect based on electromagnetic repulsive force. When electrical current passes through a solenoid coil, an electromagnetic field is generated. The wheel is designed in such a way that magnets are continually facing the solenoid coils and a micro-controller is able to regulate the flow of electricity through the coils in order to generate a repulsive magnetic field independent of the orientation of the wheel component. The hardware outer shield is made of an upper handle, which is rotated by the user and connected to a fixed base via a bearing. Permanent magnets are situated in the handle while solenoid are in the base. When solenoids are activated and the user is spinning the wheel, the user can perceive a haptic bump generated by the repulsive electromagnetic field.

A hardware prototype has been implemented and its component parts described below:

Outer shield. The outer shield of the wheel is formed from two parts connected with a bearing: the top part can rotate around its center, while the bottom is fixed. The shield is made of plastic using a polyjet rapid prototyping machine (Figure 1). The diameter of the wheel is of 8.2 cm, the height is 5 cm and the diameter of the handle is 2.8 cm.

Encoder. A step rotary encoder is used to sense rotation of the wheel. Due to the friction in the encoder, switching to an optical encoder or sensing directly from the solenoid coils may lead to clearer haptic cues.

Magnets and solenoids. Four permanent magnets are fixed in the top part of the wheel at 90 degrees from each other. Two solenoids (~1180 rounds), one at zero degrees and the other one at 225 degrees, are mounted in the base. This configuration essentially subdivides the rotational space into eight regions, each one spanning 45 degrees, that can be activated independently. In fact, for each 45 degree segment only one solenoid will be facing a magnet (see Figure 2), simplifying the generation of haptic cues. A rotational angle of 45 degrees for cue separation was determined through iterative subjective experimentation with the goal of maximizing the effect of the repulsive force felt given the size of the wheel, the magnets (dimeter 1.4 cm) and the solenoids (dimeter 1.7 cm).

Micro-controller. The solenoids are independently connected to a micro-controller through an H-bridge. The micro-controller can therefore regulate the flow of current through each of the solenoids in the wheel, independently controlling their magnetic fields.

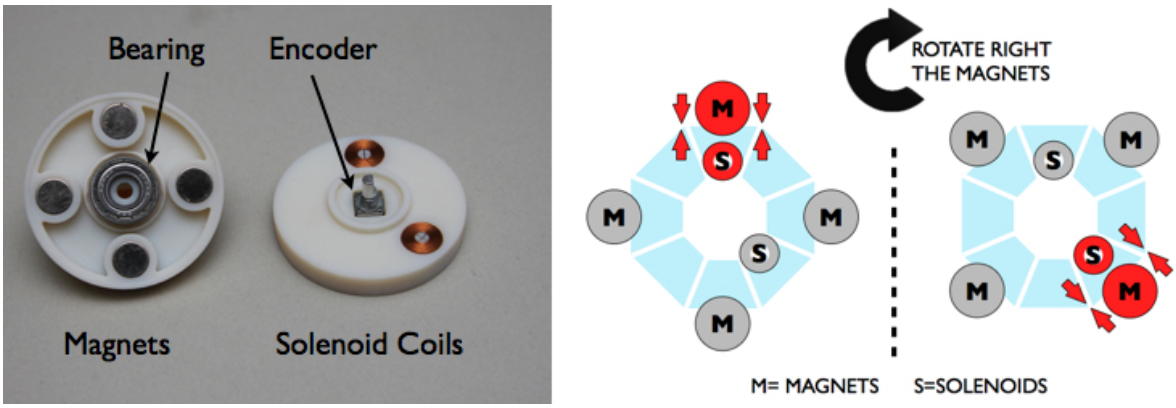

Figure 2. Components inside of the hardware wheel (left) and layout of magnets and solenoids (right): this layout is designed to minimize the number of internal components but still being able to render haptic cues for 8 different angular regions.

FUTURE WORK AND CONCLUSIONS

The hardware prototype proposed in this paper is still a work in progress and several improvements are being considered. For instance, with have experimented with different handle sizes, in order to explore the effects of different torques on the perception of the repulsive force experienced while rotating the wheel (Figure 1). Moreover, in one prototype, the solenoids and magnets were arranged vertically, while in another they were arranged horizontally, in order to explore the effects of magnetic noise on the circuit underneath the wheel. Finally, we are also working on the design of custom solenoid coils to amplify the magnetic field and the effect of repulsive force.

Future work includes the development of an authenticaton scheme based on the technique and prototype presented in this paper, and evaluations to test the feasibility and usability of this technique in real-world settings. Furthemore, we plan further explorations to gauge if the sound emitted by the device (from the rotary parts) is sufficient to make it susceptible to an auditory observation attack, and directly compare our technique against related work reported in the literature.

In conclusion, this paper introduces a novel haptic technique that is suitable for authentication interfaces in public terminals. It proposes a method that uses a haptic electromagnetic repulsive force - and is therefore silent and immune to audio observation attack - and that is easily applicable to the Spinlock [4], a recent interaction authentication technique which based on repeated presentation of a single haptic cue.

REFERENCES

1. Bianchi, A., Oakley, I., Lee, J., Kwon, D. The haptic wheel: design & evaluation of a tactile password system. In Proceedings of CHI 2010, ACM, New York, NY, pp. 3625-3630.
2. Bianchi, A., Oakley, I., Kostakos, V., Kwon, D., The Phone Lock: Audio and Haptic shoulder-surfing resistant PIN entry methods. To appear in Proc. of ACM TEI'11, ACM, New York, NY.
3. Bianchi, A., Oakley, I., Kwon, D.S., The Secure Haptic Keypad: Design and Evaluation of a Tactile Password System. In CHI 2010, ACM, New York, NY, pp. 1089-1092.
4. Bianchi, A., Oakley, I., Kwon, D.S., Spinlock: a Single-Cue Haptic and Audio PIN Input Technique for Authentication, In Proc. of HAID 2011.
5. Brewster, S. A. and Brown, L. M. Non-visual information display using tactons. In Ext. Abs. of CHI 2004, ACM, New York, NY, pp. 787-788.
6. De Luca, A., Langheinrich, M., Hussmann, H., Towards understanding ATM security: a field study of real world ATM use. In Proceedings SOUPS '10.
7. De Luca, A., von Zezschwitz, E., and Hußmann, H., Vibrapass: secure authentication based on shared lies. In Procs. of CHI '09. ACM, New York, NY, pp. 913-916.
8. Giesen, L. ATM fraud: Does it warrant the expense to fight it? Banking Strategies, 2006, vol. 82, issue 6.
9. Kuber, R., Yu, W., Feasibility study of tactile-based authentication, in International Journal of Human-Computer Studies, Vol. 68 (3), March 2010, 158-181.
10. 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.
11. Zhuang, L., F. Zhou, and J. D. Tygar. Keyboard Acoustic Emanations Revisited. In Proceedings of Computer and Communications Security 2005, pp. 373-82.