Obfuscating Authentication Through Haptics, Sound and Light

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

Ian Oakley
Madeira Interactive Technologies
Institute
University of Madeira
Funchal, Portugal
ian@uma.pt

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

CHI 2011, May 7–12, 2011, Vancouver, BC, Canada.
ACM 978-1-4503-0268-5/11/05.

Abstract
Sensitive digital content associated with or owned by individuals now pervades everyday life. Mediating accessing to it in ways that are usable and secure is an ongoing challenge. This paper briefly discusses a series of five PIN entry and transmission systems that address *observation* attacks in public spaces via shoulder surfing or camera recording. They do this through the use of novel modalities including audio cues, haptic cues and modulated visible light. Each prototype is introduced and motivated, and its strengths and weaknesses are considered. The paper closes with a general discussion of the relevance of this work and the upcoming issues it faces.

Keywords
PIN, authentication, security, usability, observation

ACM Classification Keywords
H5.2. User Interfaces: Input devices and strategies

General Terms
Security, Human Factors

Introduction
The Internet has ushered in a connected world in which organizations as commonplace as banks, stores and

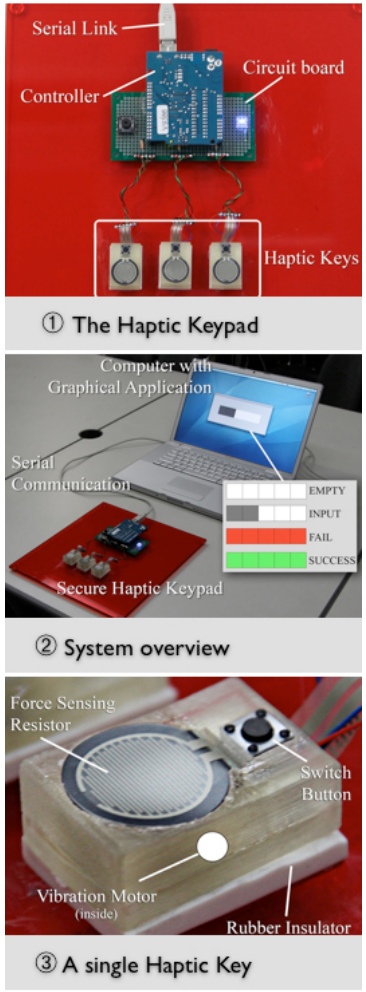


Figure 1. The *Haptic Keypad* system, an overview of how it is interfaced to a computer and a close-up of a key.

supermarkets offer always-on access to a wide range of services. This has led to a dramatic increase in the amount of sensitive digital content associated with individuals. The mechanisms by which access to this material can be secured usably and effectively are a rapidly growing research area within the field of Human Computer Interaction (HCI) [e.g. 6]. The work in this paper is situated in this emerging application domain.

In the broadest sense, ownership of and access to digital content is mediated by the presentation of public *identity* information such as usernames, physical tokens (such as bank cards) or biometric data (such as fingerprints). Before access is granted, this identity information is verified by the provision of private *authentication* data, usually in form of alphanumeric passwords [e.g. 5]. While successfully deployed in interfaces as diverse as public terminals (e.g. ATMs), personal computers and web services, this paradigm is susceptible to a number of attacks. One of the most prominent is the observation attack, in which a malicious third party observes the password entry process in person (termed should-surfing) or via appropriate recording equipment [6]. Although crude, this method has been proved to be highly effective and responsible for the loss of million of dollars annually [8].

Researchers have reacted to this issue by proposing a range of methods that obfuscate the password entry process. These include methods based on complex visual information [e.g., 7], passwords with non-visual components [e.g., 2] and methods relying on complex authentication procedures [e.g., 5]. Typical disadvantages of such systems are the slow authentication times or the high levels of cognitive load they engender in their users.

The goal of this paper is to introduce a simultaneous, lightweight presentation of five prototype systems tackling different aspects of this problem space in order to highlight overarching issues and to spur and encourage a full discussion of the possibilities afforded by this topic. Each of the prototypes described was designed and built in order to explore how authentication in public spaces can be rendered more secure and usable without incurring costs in terms of performance or workload. The paper concludes with a discussion highlighting the lessons learnt and key upcoming research issues. Where possible, reference to prior publication of the prototypes is made.

The Secure Haptic Keypad

The *Secure Haptic Keypad* [2] tackled the problem of a visual observation attack by proposing a non-visual password composed of a sequence of tactile cues, or tactons [4], rather than alphanumeric characters. This concept was instantiated in an interface composed of a set of three pressure sensitive keys (Figure 1), each containing a tactile actuator capable of rendering three different tactons. Password entry in this system took the following form. First, the tactons were randomized on the three keys. Second, users explored the keys with their fingers to locate the first tacton in their password. The tactons were played only when a user touched each key; a click on the key (i.e., pressing with greater force) resulted in the selection of the tacton. Thirdly, the tactons were randomized on the keys and entry of the next password item commenced. The randomization of tactons to keys ensured that a visual observer was left with no overt clues as to password contents. The simplicity of this system is its key strength – password items are found via haptic

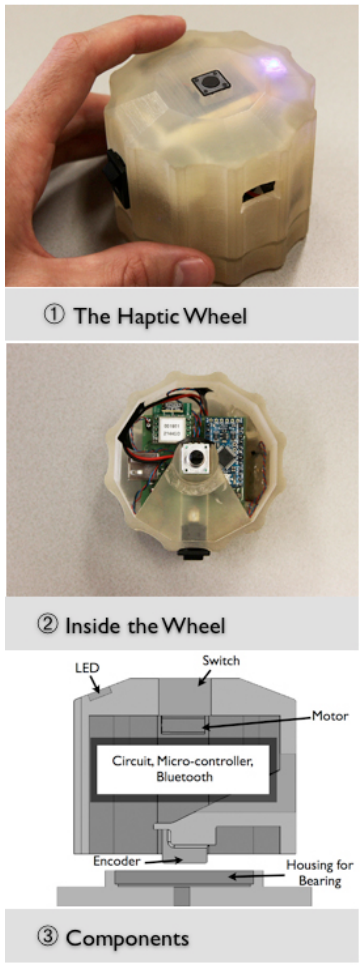


Figure 2. The *Haptic Wheel* hardware system, with special attention to its internal components.

exploration and, after being indentified, simply pressed to indicate selection.

A study showed that users could successfully enter passwords using this system with a high level of accuracy and reasonable task performance time (approx 25s) [2], validating the basic concept. However, subjective measures revealed that it caused an increased level of mental workload when compared to standard numerical entry systems. This is in part due to the search style it engendered: serial searches for tactons across the set of three keys. This search style led to the key limitation of the *Haptic Keypad* - its lack of scalability. It is based on the idea that each tacton in the system is always present on a key. Consequently, in order to present a richer input space based on a larger tacton set (therefore requiring shorter passwords), additional keys are necessary. However, the serial tacton search strategy employed by users suggests that any such additions will exert a highly negative effect on task performance.

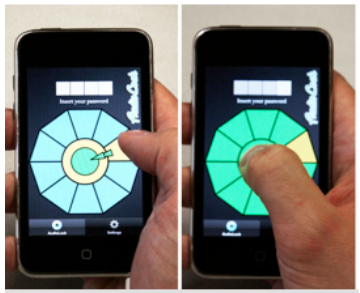
The Haptic Wheel

The *Haptic Wheel* (Figure 2) extended the paradigm introduced in the *Haptic Keypad* in order to tackle its limitations of scale [3]. It took the form of a freestanding electromechanical dial (resembling the rotary control of a safe) capable of making continuous revolutions in both directions, of producing vibro-tactile cues and of accepting explicit input from a button mounted on its top surface. The rotational input space was partitioned into equally sized angular targets, each of which could be associated with a tacton. The Haptic Wheel was designed to use a subjectively sequential set of tactons spanning pulses from low to high frequency. Password entry on the *Haptic Wheel* resembled that of the *Haptic Keypad*. First, the tactons were randomly assigned to the angular input segments, ensuring the sequential order was retained. The user then rotated the wheel to the appropriate tacton and selected it (via the device's button). The tactons were randomized prior to the entry of the next password item.

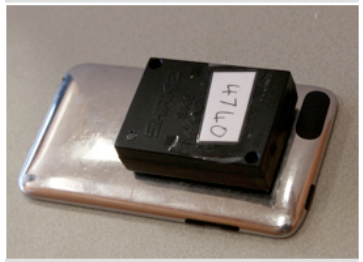
The system maintained the resistance to observation of the *Haptic Keypad* and increased the scalability, as users could take advantage of the sequential nature of the tactons to infer target locations. In fact, by recognizing one tacton, users could ascertain the location of any other, providing a shortcut to avoid the serial search strategy. User evaluations [3] validated this assertion and showed the *Haptic Wheel* could be used with larger tacton sets (in our studies, composed of up to five tactons). It also outperformed the *Haptic Keypad* in terms of security, accuracy and authentication speed, though at the cost of a more complex and expensive hardware unit.

PhoneLock

While the password entry paradigm identified in the *Haptic Keypad* and *Haptic Wheel* prototypes is promising, the reliance on custom hardware solutions limits its applicability. The *PhoneLock* prototype addresses (Figure 3) this issue by porting the interaction model to a smart-phone [1].



① PhoneLock interaction



② PhoneLock SHAKE unit

③ PhoneLock user study

Figure 3. The *PhoneLock* system, the SHAKE unit attached to the back of the mobile device and a user test.

The *PhoneLock* is a password entry system for mobile phones based on locating and identifying auditory or tactile cues rather than visual ones. As with the previous systems it is resistant to visual observation and can be used eyes-free. It is based on interaction with a dial drawn on the display of a touch-screen phone. As with the Haptic Wheel, different segments of this dial can be associated with different cues, each of which is played in response to a user's touch. The *PhoneLock* system maintains the constraint that the cues must be organized around its rim sequentially. Finally, as the *PhoneLock* wheel is a software system, it is simple to configure with differently sized cue sets and segment sizes.

The *PhoneLock* can be used with either audio or tactile cues and has been implemented on an Apple iPhone. Audio cues are delivered via headphones to ensure they remain private, while tactile cues are rendered using an external pager motor (in a SHAKE device [10]) physically mounted to the phone and controlled via Bluetooth. Interaction is once again based on a paradigm of randomization of cue location prior to user search and selection for a password item. However, rather than being restricted to moving to adjacent wheel items, users can also 'jump' between non-sequential items by making rapid, repeated screen taps, potentially provided improved performance.

PhoneLock prototypes have been constructed using iconic audio cue sets (spoken numbers from zero to four and zero to nine) and tactons sets (again five and ten items in size). A user study [1] suggested that with the use of appropriate cues sets, the system maintains or improves upon the performance levels reported in studies of the Haptic Wheel. Although full and formal evaluations of this system are currently required, these explorations suggest the *PhoneLock* system succeeds in porting the *Haptic Wheel* model to a standard mobile platform.

SpinLock

One limitation of the *PhoneLock* and *Haptic Wheel* systems are their reliance on sets of iconic cues – learnt material such as audio icons, spoken words or tactons – which must be perceived by users to be sequentially ordered. Although this is relatively simple for audio cue-sets (e.g., numbers), it is more challenging in the haptic domain, particularly when tacton sets of 5 or more items are used. However, such large sets are desirable as they can reduce required password length by increasing the strength of each item. For example with a set of ten cues, a four-item password can take one of 10000 (10^4) unique forms, making it hard to break via brute force, or random guesses. With a set of 5 cues, a four-item password leads to only 625 (5^4) possibilities. In such cases additional password items must be used in order to provide sufficient resistance to brute force attacks.

Spinlock attempts to solve this problem by using repeated presentation of a single cue, rather than a set of different ones. It is implemented for a smart-phone and based on the same metaphor of a dial. However, instead on moving to particular segments in order to experience tactons, a user touches the dial and then moves around its rim in either a clockwise or anti-clockwise direction. As they move, brief cues in the form of haptic clicks or audio ticks are delivered at randomly determined intervals. In this system, as with a traditional safe, a password is composed of a combination of a direction and number of clicks (e.g. 2-

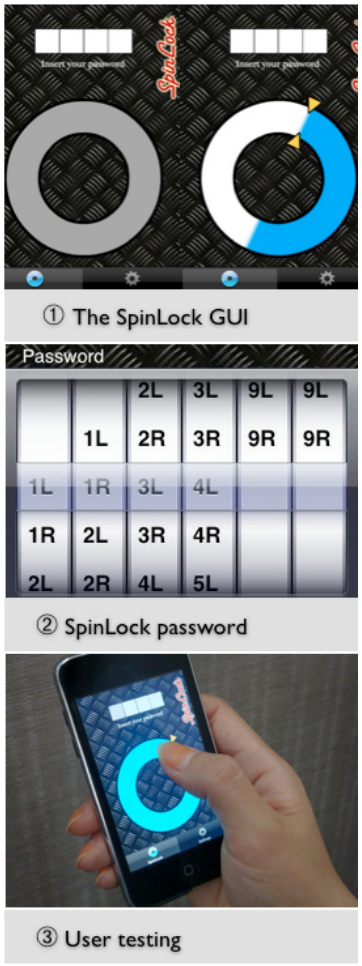


Figure 4. The *SpinLock* GUI prototype and its usage.

left, 3-right). Differently from many real safes, users are not forced to alternate the direction in which they spin the wheel and can select any combination of direction and number of clicks per input.

The *SpinLock* interface remains resistant to observation, as the on-screen distance between each cue is randomly determined. This technique is currently in the prototype stage (Figure 4). Upcoming issues include determining optimal cue distances (with a target of 10 rapidly recognizable cues) and the development of appropriate weighting for the random function in order to prevent attackers correlating observed distance travelled with PIN item entered. Although formal user studies on this technique need be conducted, current informal tests suggest it is a viable technique particular suited to use with haptic cues. Users also express appeal toward this technique.

LuxPass

The *Haptic Keypad* and the *Haptic Wheel* share a common problem: because they are interfaces intended to operate as part of fixed public terminals, like regular keyboards found at the ATMs, they are inherently exposed to observation attacks, where observation could be visual, auditory or even rely on vibration sensors. Hence, we developed a system that takes advantage of the intrinsic security of a user-owned device, such as a mobile phone, and of a communication technique based on light impulses to communicate with a public terminal without requiring any specific pairing mechanism.

This system is LuxPass (Figure 5). It allows users to shift (in time and space) an authentication procedure: PIN entry takes place on a mobile phone away from a potentially observed public terminal and this information is transmitted to the terminal when in close physical proximity. Prior attempts to use mobile phones as a getaway to interaction with public terminals have taken two broad directions. They either ensure an encrypted connection between a mobile device and a remote third party by means of a pre-agreement (i.e., a public key infrastructure), or use out-of-band (OOB) [9] side channels to establish a paired connection between the phone and the terminal (i.e., shake to establish a connection with a listener).

In contrast, *LuxPass*, presents a novel method that allows users to authenticate to a public terminal using a mobile phone without requiring explicit pairing. *LuxPass* works by displaying messages through modulated patterns of light on a mobile phone screen, which are sensed by a dedicated sensor on the terminal and decoded to identify the password. *LuxPass* relies on close physical contact with a sensor terminal to ensure this channel is private. A key advantage of this approach is that it is based on standard component of a mobile device (the screen) making it economical and easy to deploy.

Discussion and Conclusions

The goal of this paper is twofold. The first is to provide an overview of our work in non-visual PIN entry; five interfaces have been briefly presented. The second is the following discussion of the general challenges they raise in the area of security and usability. A substantial body of recent research [e.g., 2, 3, 5, 7] has been devoted to methods to counteract the observation attack (camera recording or shoulder-surfing) during authenticating to public terminals. Although these methods are clearly effective, it is evident that they

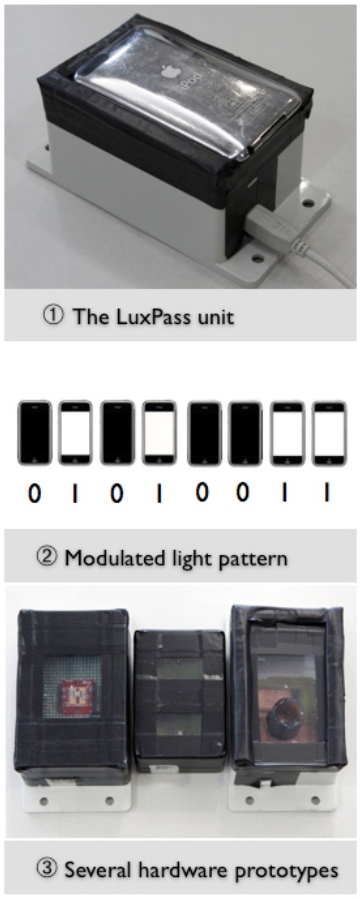


Figure 5. The *LuxPass* system in use, an example of modulated light pattern, and several hardware prototypes variations.

also introduce higher level of complexity for users, which is often mitigated by compromising security for improved usability.

It is furthermore clear that methods proposing to counter observation attacks based exclusively on modifications to interaction at the public terminals are bound to fail because of their intrinsic vulnerability: they remain situated in public spaces. On the other hand, those methods that merely rely on private devices such as phones (i.e., phone based internet banking) are not helpful in those cases in which users have no choice but to access a service on a public terminal.

In this paper we argue that only a combination of the two approaches will suffice to provide a secure and ubiquitous authentication mechanism. For instance, simply shifting the authentication process from a public terminal to a safer user-owned private device (e.g., [1]), such as a mobile phone, improved security can be achieved without compromising usability. On the other hand, by using the physical contact and light as media (e.g., *LuxPass*) we can also assure a secure transaction between the private device and the public terminal without relying on pre-agreements, third party infrastructures or pairing.

In sums, by decoupling the authentication process into two modular and independent sub-tasks (the *input-interaction* and the *PIN-transmission*) this paper argues it is possible achieve a highly usable front-end PIN entry interface backed up by a secure system for transmitting it to terminals. Further research is currently required to develop and optimize both components of the system and improve their integration. Regardless, we anticipate that decoupling authentication into these two key sub-tasks will become a common practice in future authentication systems for public terminals.

Reference

[1] Bianchi, A., Oakley, I., Kostakos, V., Kwon, D., The Phone Lock: Audio and Haptic shoulder-surfing resistant PIN entry methods. To appear In Proc. TEI'11.

[2] Bianchi, A., Oakley, I., Kwon, D.S., The Secure Haptic Keypad: Design and Evaluation of a Tactile Password System. In Proc. CHI 2010, pp. 1089-1092.

[3] Bianchi, A., Oakley, I., Lee, J., Kwon, D. The haptic wheel: design & evaluation of a tactile password system. In Ext. Abs. of CHI 2010, pp. 3625-3630.

[4] Brewster, S. A. and Brown, L. M. Non-visual information display using tactons. In Ext. Abs. of CHI 2004, pp. 787-788.

[5] De Luca, A., Hertzschuch, K., Hussmann, H., ColorPIN: securing PIN entry through indirect input. In Proc. of CHI 2010, pp.1103-1106.

[6] De Luca, A., Langheinrich, M., and Hussmann, H., Towards understanding ATM security: a field study of real world ATM use. In Proc. of SOUPS 2010, pp. 1-10.

[7] Forget, A., Chiasson, S., Biddle, R., Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In Proc. CHI 2010, pp.1107-1110.

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

[9] Kobsa, A., Sonawalla, R., Tsudik, G., Uzun, E., Wang, Y., Serial hook-ups: a comparative usability study of secure device pairing methods. In Proc. of SOUPS '09.

[10] SHAKE SK6:http://code.google.com/p/shake-drivers.