Open Sesame: Design Guidelines for Invisible Passwords

Andrea Bianchi, *KAIST, South Korea*
Ian Oakley, *University of Madeira, Portugal*
Dong-Soo Kwon, *KAIST, South Korea*

Invisible input and output modalities, such as haptics and audio, are a potentially effective defense against observation-based attacks on PIN entry systems. However, the successful implementation of such systems calls for some general design guidelines.

In the tale of *Ali Baba and the Forty Thieves*, the words "open sesame" unlock the entrance to the thieves' treasure cave. This is an early, fictional case in which access to a coveted resource is restricted not by some physical token or key, but with a password—secret information known only to a privileged few.

In many ways, open sesame remains a model password: it is simple, quick, and easy to use. But the story has a darker side—Ali Baba steals the password by overhearing the thieves in conversation, and Cassim, Ali's brother, is killed after entering the cave, forgetting the password, and becoming entrapped. In fact, this ancient story highlights the key usability problems and tradeoffs associated with passwords today: they must be quick to input and easy to remember and share while remaining hard to guess and difficult to surreptitiously observe.

This tradeoff, essentially a tension between simplicity and security, has attracted much attention. For example, in 1967 Sir Shepherd-Barron introduced a six-digit personal identification number (PIN) for early automated teller machines (ATMs), but shortened it when his wife complained that she could effectively recall no more than four items.[1] A more recent example is the "pattern" screen unlock on Google's Android mobile phones, in which a gesture connects grid points shown on the touchscreen. For most users, the secret information is simple to remember and authentication takes place in a matter of seconds,[2] but even a casual glance can allow an observer to capture the password. Simply being in the right place at the right time, as Ali Baba was, is enough to discover the secret.

Such narratives aside, observation has emerged as a subtle and dangerous attack that undermines the safety of authentication on public terminals such as bank ATMs. Indeed, yearly losses from such attacks are reported to be approximately $60 million in the US alone,[3] and equipment to support attackers is rapidly growing in complexity. Arguably, this problem is largely due to the standardization of ATMs, PINs, and the numerical keypads used to enter them.[3] Efforts to maximize usability and memorability have created a homogeneous ecosystem of devices. This makes it simple for attackers to design, manufacture, and test exploits; observation is but the simplest and most effective of these exploits.[4]

To address this issue, researchers have proposed numerous observation-resistant input methods, including puzzles, cognitive mappings, keyboard randomizations, and eye trackers. A recent approach has been to rely on audio and haptics,[2,5,6] input and display modalities that are theoretically invisible—unobservable by visual means and therefore immune to standard observation attacks. However, nonvisual modalities for PIN entry raise new issues in terms of usability, performance, and memorability. Authentication

 Published by the IEEE Computer Society

is a frequent, demanding task that users are accustomed to performing rapidly and easily, and it is not clear how nonvisual interaction techniques can be best designed to meet these standards. See the "Usable Security and Tangible Interaction" sidebar for related work in this area.

Here, we focus on how researchers can design such systems to optimize usability in terms of speed, accuracy, and ease of authentication while remaining resistant to visual observation.

NONVISUAL AND HAPTIC PIN ENTRY TECHNIQUES

One recent approach to protecting PIN entry from observation was to create multimodal interfaces in which hidden haptic information obfuscated the entry of graphical or numerical codes. For example, Behzad Malek and his colleagues combined an observable graphical password with invisible input on an interactive, pressure-sensitive screen.[7] Users drew a graphical password by selecting a series of adjacent points displayed in a grid and simultaneously entered haptic information by systematically varying the pressure applied during the individual selection actions.

Similarly, in Vibrapass users enter numerical PINs on a standard keypad but modulate their input based on simple tactile cues that the system delivers via a securely prepaired mobile device carried in a pocket.[2] The operation is simple: when tactile cues are displayed, users enter incorrect PIN items on the keypad; when no cues are displayed, users enter correct information. In this way, the data entered on the keypad is hidden from observers via the addition of erroneous PIN items.

These approaches combine easy-to-remember PIN content with relatively simple unobservable information. Security studies have shown that these systems are more resistant to observation attack than standard PINs. However, both are susceptible to repeated observation either by inferring applied pressure from visual cues or by logically calculating PINs from recurring patterns.

To address this limitation, Hirokazu Sasamoto and his colleagues introduced Undercover, a graphical password system augmented by haptic information and designed to be resistant over multiple observations.[6] In this system, users place their nondominant hand on a force-feedback trackball and then use their dominant hand and a special keypad to enter an image-based authentication token by selecting items from a sequence of pictures displayed on a screen. The mapping between the displayed images and keypad buttons changes after each selection and is communicated to users via directional haptic cues rendered on the trackball. Although this system is highly resistant to observation, authentication times range from 35 to 45 seconds and error rates from 26 to 52 percent. Thus, this multimodal approach trades usability for security.

USABLE SECURITY AND TANGIBLE INTERACTION

Although security has traditionally been associated with cryptography and computer science, it is now widely acknowledged that human factors play a critical role. Indeed, systems are said to be only as secure as their users, and security researchers often refer to humans as the "weakest link"—that is, the most vulnerable to attack. Consequently, some new system designs borrow from the field of human-computer interaction. The resulting research in the emerging area of usable security considers both human and technical issues, with emphasis on the inherent tradeoff and tension between them.

Tangible interaction **connects bits with atoms. These systems require users to interact with digital content by directly manipulating physical objects—for example, changing their orientation or position, or the arrangement and configuration of items in a group. Prominent research in this field includes Hiroshi Ishii's work on tangible bits at MIT's Media Lab[1] and Durrell Bishop's Marble Answering Machine (http://design.cca.edu/graduate/uploads/pdf/marbleanswers.pdf), a prototype introduced in 1992 that lets users interact with stored voice messages by manipulating physical tokens in the form of colored marble balls.**

Researchers have recently augmented tangible systems with haptic technology, a key step toward developing tangible systems that have not only embedded computational power but also rich interactional expressiveness.

Reference

1. H. Ishii and B. Ullmer, "Tangible Bits: Towards Seamless Interfaces between People, Bits and Atoms," *Proc. Conf. Human Factors in Computing Systems* (CHI 97), ACM, 1997, pp. 234-241.

Unimodal nonvisual PIN entry systems—that is, systems based solely on touch or sound—could improve user performance. According to recent reports[8] in the cognitive science literature, users can achieve higher performance levels in attention-demanding tasks when central cognitive resources are dedicated to a single sensory channel. For example, the Tactile Authentication System (TAS), which is intended for visually impaired users, presents PIN items in the form of a range of shapes or different spatial patterns of Braille dots.[9] To enter a PIN, users search for and select the shapes that correspond to their PIN. Evaluations of this system revealed that participants could reliably authenticate over a one-month period with low error rates, but that authentication remained time-consuming, with a mean authentication speed of 38 seconds.

Encouraged by such findings, we sought to develop unimodal nonvisual PINs with the objective of improving performance and usability while maintaining accessibility and security against observation.

INVISIBLE PASSWORD SYSTEMS

We classify invisible password systems as those that rely on the recognition of structured nonvisual cues to support PIN entry processes, and those based on counting

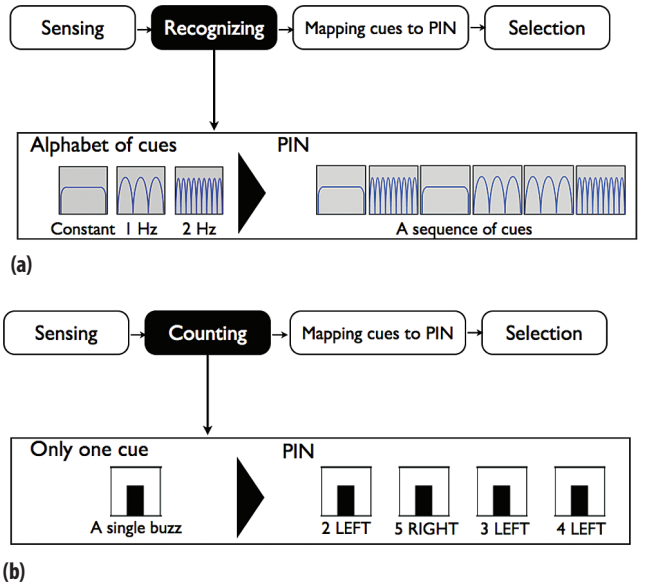


Figure 1. Invisible password systems rely on either (a) the recognition of different cues or (b) counting the occurrences of a simple single cue.

occurrences of simple, rapidly presented, identical cues. The conceptual diagram in Figure 1 illustrates the differences between the two approaches.

Recognition techniques

Recognition approaches to nonvisual PIN entry rely on sets of structured tactile or auditory cues or patterns, known respectively as tactons[10] and auditory icons. Tactons are abstract haptic cues with a set of distinctive properties (such as vibration roughness, rhythm, or amplitude) that users perceive, recognize, and associate with specific digital content.

In many ways, haptic and audio recognition approaches to PIN entry resemble numerical PINs. Users identify and select specific sequences of items (in the form of tactile or audio sensations rather than numbers) from limited sets of possibilities. Differences emerge in the expressiveness of the modality of cue presentation and the affordances this creates for selection mechanisms. In addition, to ensure resistance to observation, these approaches repeatedly randomize the relationship between selection mechanisms and displayed cues.

Figure 2 shows three prototypes that use the recognition approach: the haptic keypad, haptic wheel, and phone lock.

Haptic keypad. This prototype leverages users' familiarity with keypad entry.[5] As Figure 2a shows, the keypad has a row of three hardware keys, each consisting of a push button to detect item selection, a pressure sensor to detect finger presence, and a vibrotactile motor to render tactons. The system uses no audio cues and only three tactons so the full set can be displayed on the hardware simultaneously. The three tactons are randomly assigned to the three keys. Users explore the keys with their fingertips to locate the next tacton in their PIN and select the relevant button. The tactons are then randomized over the keys again, and users seek for and enter the next PIN item. The system uses data from the pressure sensors to ensure that tactons are only rendered on a key when a user touches it. The randomization process ensures that no relationship exists between the keys pressed, an observable action, and the tactons selected, the PIN's actual contents.

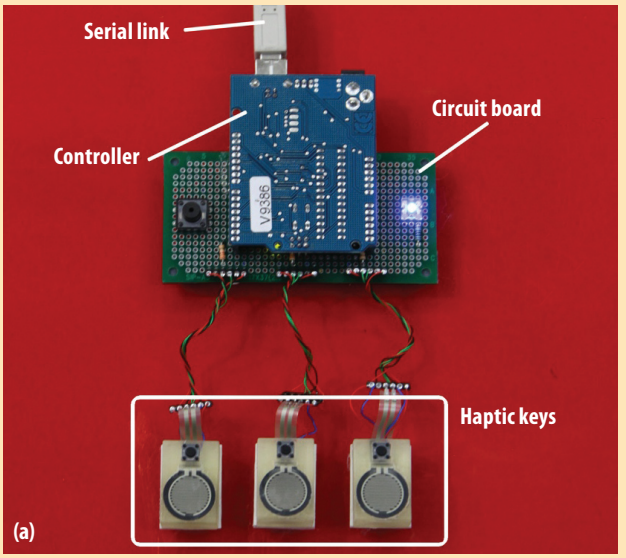
The system's key strength is its simplicity: password items are located via haptic exploration, and, after recognition, users simply press the corresponding key and make a selection. It requires no complex processing of the haptic information. Its limitations lie in scalability and expressiveness. Because the number of cues must match the number of keys, adding tactons requires creating new physical keys and will lengthen the time and difficulty of finding and selecting PIN items.

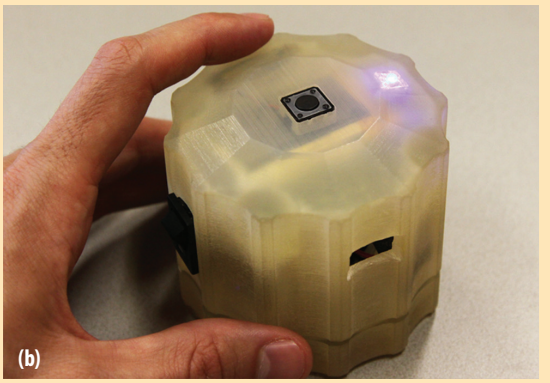
Haptic wheel and phone lock. The haptic wheel (Figure 2b)[11] and phone lock (Figure 2c)[12] prototypes extend the recognition-based paradigm introduced in the haptic keypad but attempt to address scalability. In both systems, tactons (and audio icons) are arranged in specific human-recognizable sequences, such as cues ranging from low to high pulse frequencies. Preserving a sequence in a selection interface helps users sense one item from the set and infer another item's relative location. Both the haptic wheel and phone lock use a dial arrangement in which the rotational space is divided into equally sized targets. The cues are then arranged sequentially around the targets, and randomization of the cue locations simply adjusts the starting point for the series of cues. The cue order is always maintained.

The haptic wheel is a freestanding electromechanical dial (resembling a safe's rotary control) that can make continuous revolutions in both directions, produce vibrotactile cues, and accept explicit input from a button mounted on its top surface. It cannot render audio cues.

The phone lock is a circular widget on a mobile device's touchscreen divided into several targets. By making gestures or touching the screen, users can select and explore these targets. In addition to tactile cues, phone lock renders audio cues in the form of spoken numerals. Both variants of the phone lock use haptic cue sets comprising 5 to 10 items of ascending frequency.

Conceptually, the two systems operate in the same way. First, the system randomly assigns the initial item in the cue sequence to a rotational target and allocates the other cues sequentially in a clockwise order. Next, users explore the targets (by rotating the physical wheel or selecting different on-screen segments) to find the next PIN item. To select an item, users press a dedicated button in the wheel center. Finally, the system randomizes the location (but not





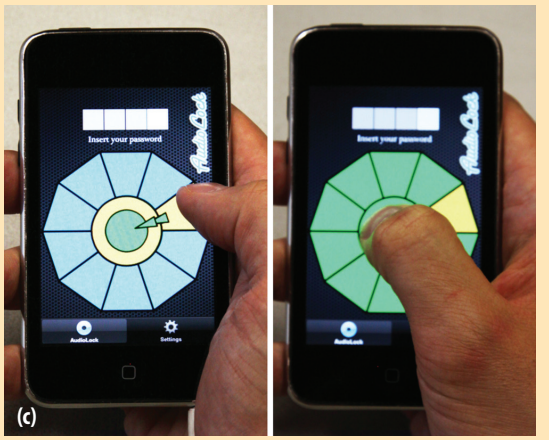


Figure 2. Prototypes using recognition techniques for PIN entry. (a) The haptic keypad has a row of three hardware keys, each consisting of a push button to detect item selection, a pressure sensor to detect finger presence, and a vibrotactile motor to render tactons. (b) The haptic wheel is a freestanding electromechanical dial that can make continuous revolutions in both directions, produce vibrotactile cues, and accept explicit input from a button mounted on its top surface. (c) With phone lock, users operate the touchscreen to select and explore targets displayed in a circular widget on a mobile device.

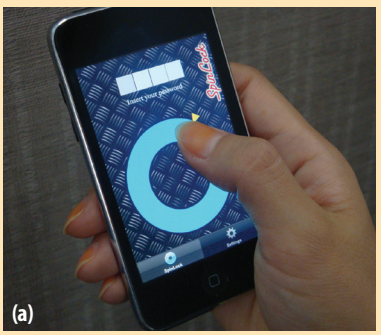
order) of the cue series over the targets once again. The randomization ensures that there is no correspondence between the selected targets and the entered PIN.

Counting techniques

Counting the number of simple, short, pulse-like stimuli in a temporal sequence is another way to communicate structured nonvisual information. Examples of devices that use such counting techniques include dial lock safes, which require users to enter their passwords as a sequence of ticks occurring in response to rotation, and the clicks that delimit menu items in haptic or audio-enabled dials such as the Apple's iPod Classic and the BMW iDrive. Counting such elementary stimuli (simple pulses of sound or vibration) has potential as a mechanism for encoding information in the haptic and audio PIN entry processes. Indeed, research suggests that humans can accurately and easily count up to 10 rapidly delivered sequential tactile and audio cues.[13] Figure 3 shows two prototypes that implement interfaces for counting-based PIN entry.

The interaction techniques required to support counting techniques in PIN entry differ substantially from those required to support recognition.

Spinlock. Spinlock, a counting-based prototype for touchscreen smartphones, was inspired by the interface of a dial lock safe.[14] This system, shown in Figure 3a, displays a rotational ring-shaped widget on the screen. Users start at



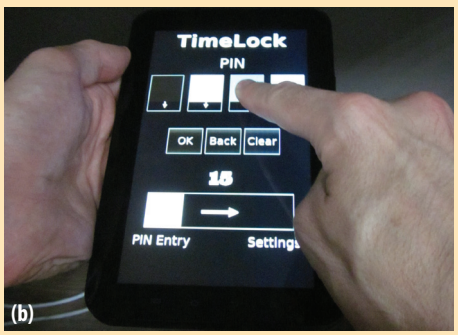


Figure 3. Prototypes using counting techniques for PIN entry: (a) spinlock, a counting-based prototype for touchscreen smartphones, and (b) timelock, which delivers cues by dwell duration and uses an entry sequence that serves as an additional security parameter that is secure against brute-force attacks and resistant to observation.

any point along the ring's circumference and move a finger around it, receiving simple, identical tactile and audio cues in response. Rather than divide cues into specific equally distanced targets or segments, spinlock randomly presents cues as the length of the gesture increases. When the finger is removed, the widget and screen stop presenting cues, and the system records the number of nonvisual cues (beeps or buzzes) that have been displayed to user.

Spinlock PIN items consist of gesture direction (clockwise or counterclockwise) and stimuli count pairs. For example, a PIN item could be four cues clockwise or two cues counterclockwise. A sequence of such pairs comprises a complete PIN. Although a gesture's direction is observable information, the presentation of the haptic and audio cues occurs at random spatial intervals. Thus, because there is no direct mapping between gesture length and the PIN item selected, the system is resistant to casual observation attack.

Unimodal systems rely on cues delivered in a single modality, or they combine input tasks with sensing tasks.

Timelock. Timelock extends the counting interaction model but delivers cues by dwell duration. As Figure 3b shows, the screen displays four button widgets, each representing one PIN item. Users select and hold these buttons to enter PIN items. During button presses, timelock delivers cues at randomly selected temporal intervals. When the user releases the button, the system notes the number of delivered cues.

The direct entry of PIN data into specific widgets also affords a range of new interaction possibilities. For example, users can correct PIN errors by re-entering their PIN (by simply reselecting a target) or using the back button to delete a single PIN item. Direct mapping also allows the order in which PIN items are entered to be a password parameter. In timelock, users can enter PINs from leftmost item to rightmost item, vice-versa, or any other order. The entry sequence serves as an additional security parameter that is secure against brute-force attacks (such as guesses) but not observation.

DESIGNING INVISIBLE PASSWORDS

Table 1 summarizes the designs and study results for the systems discussed in this article. It also shows the systems' resistance to two types of attacks. The "brute force" column shows the system's resistance to attacks based on an attacker randomly guessing the PIN. To protect against this attack, a designer would typically create an input space of 10,000 PINs, equivalent to that in a standard numerical 4-digit ATM system. The "observation" column shows the systems' susceptibility to repeated observations—that is, whether watching the PIN entry process two or more times will let an attacker infer the password. All of these systems maintain a reasonable level of security against brute-force attacks, but have divergent performance against repeated observation.

Our main focus here is user performance. However, rather than dwell on the details and numbers, we discuss the system design parameters and how they impact performance as recorded in user studies to distill guidelines for designing nonvisual authentication systems. In particular, we seek to identify lessons illustrating how researchers should design nonvisual input to maximize speed and minimize errors. These guidelines will be applicable to the design of high-workload, high-demand nonvisual interaction tasks beyond the security domain. We structured the guidelines as a series of tradeoffs between the various design parameters that have been explored in the literature: haptic versus audio, unimodal versus multimodal, recognition versus counting, and physical versus virtual interfaces.

Haptics versus audio

Haptics benefits from a "walk up and use" scenario—simply holding or touching a device can establish a private, unobservable perceptual connection. Haptic authentication systems exploit this fact, and users reportedly view haptics as "more private,"[14] although audio is arguably a richer perceptual channel. To avoid the fate of the 40 thieves' password, however, audio systems must use a private delivery system, such as headphones.

Three of the systems discussed here directly present PIN entry systems with otherwise equivalent haptic and audio modes. The phone lock and spinlock systems demonstrate audio performance that is 22 to 38 percent faster and 28 to 60 percent more accurate than haptic performance. The third, timelock, shows equivalent performance for the two modalities.

If we view audio as peak performance, we can extract two practical lessons for designing haptic cues and interactions to optimal levels. First, haptic performance in item-recognition tasks (in phone lock, for example) is generally inferior to audio performance. Second, it is preferable to avoid movement during input when using interfaces based on haptic or audio perception (as in spinlock). Using techniques such as dwell time (as in timelock) can optimize haptic performance and achieve levels equivalent to audio.

Unimodal versus multimodal

Most of the systems discussed here are unimodal. They rely on cues delivered in a single modality, or they com-

Table 1. Interface performance and security results.

Name	Security		Technique	Modality	Time (seconds)	Errors (%)
	Brute force	Observation				
4-digit PIN (keypad); current standard for ATMs	1 in 10,000	No security	Unimodal	Vision	~1.5	~0
Undercover[6]	1 in 10,000 or less	1 in 10,000 or less	Multimodal recognition	Haptic + vision	~35–45	~26-52
Vibrapass[2]	1 in 10,000 or less	1 in 10,000 or less; weak against two or more observations	Multimodal direction	Haptic + vision	~6–19	8
Tactile Authentication System[9]	1 in 6,561 or less	1 in 6,561 or less	Unimodal recognition	Haptic	~38	~6
Haptic keyboard[5]	1 in 10,000 or less	1 in 10,000 or less	Unimodal recognition	Haptic	33.8	6.7
Haptic wheel[11]	1 in 10,000 or less	1 in 10,000 or less	Unimodal recognition	Haptic	23.2	16.4
Phone lock[12]	1 in 10,000 or less	1 in 10,000 or less	Unimodal recognition	Haptic	19.9	6.6
			Unimodal recognition	Audio	12.2	4.7
Spinlock[14]	1 in 10,000 or less	1 in 10,000 or less	Unimodal counting	Haptic	13.8	8.3
			Unimodal counting	Audio	10.8	3.3
Timelock (work in progress)	1 in 10,000 or less	1 in 625	Unimodal counting	Haptic	~8	2
			Unimodal counting	Audio	~8	7

bine input tasks (for example, selecting targets or gesture directions) with sensing tasks (that is, perceiving cues) such that these activities are sequential, and task elements in different modalities do not overlap temporally. On the other hand, in the Undercover multimodal system, the user simultaneously perceives, identifies, and relates haptic cues to a dynamic set of visual targets.[6] Similarly, in the Vibrapass system there is a synchronous relationship between sensing haptic cues and selecting visual targets.[2]

None of the systems demonstrate a direct comparison between unimodal and multimodal performance. However, the literature suggests that in attention-demanding, highly focused tasks, unimodal performance improves on multimodal performance.[8] Examination of the data from the full set of studies appears to support this observation. The fastest unimodal authentication times are less than 9 seconds (timelock), whereas multimodal times are either substantially greater (for example, 35 or more seconds in Undercover) or highly varied depending on the security level (for example, 6 to 19 seconds in Vibrapass). Error rates follow a similar pattern.

We argue that together these findings point to the superiority of unimodal approaches for nonvisual PIN entry tasks. They also suggest that unimodal approaches will be beneficial in other application domains featuring demanding, front-of-focus nonvisual interaction.

Recognition versus counting

Six of the systems in Table 1 use the recognition-of-nonvisual-cues approach to nonvisual PIN entry. The other three—Vibrapass, spinlock, and timelock—involve a user detecting a single simple cue or counting the number of cues presented over time. Despite their many variations, recognition systems clearly show inferior performance to nonrecognition systems: the entry times are 12 to 45 seconds compared to 6 to 19 seconds, and the error rates are 4.7 to 26 percent compared to 2 to 8.3 percent.

This effect is likely due to the fundamental nature of the recognition task—the system must perceive, recognize, and map cues to a mental representation of a PIN item. Consider the perceptual task in Vibrapass, which is limited to cue detection, and in spinlock and timelock, which uses both detection and counting. In such activities, there is minimal involvement of memory or of the mapping between perceptual and abstract representations (for example, between perception and the PIN item).

A second factor impacting the performance of recognition systems relates to the need for a search task. To achieve resistance to observation, TAS, the haptic keypad, the haptic wheel, and phone lock incorporate search: to find their next PIN item, users explore an input space in which the system renders different haptic cues. This is a time-consuming process, and, indeed, as the number of nonvisual cues in a system increases, the overhead of this search time dominates overall system performance.[12] Such preliminary exploration activities are absent in detection and counting tasks in which users can provide meaningful input and respond to output immediately.

The cognitive simplicity of detection and counting tasks strongly supports their use in future nonvisual interaction systems. Moreover, such approaches avoid the need for serial search tasks to locate key items. Consequently, system designers can leverage such simple feedback mechanisms to enable rich and compelling interactions.

The complexities of creating high-quality haptic hardware support designing future PIN interfaces around existing platforms.

Physical versus virtual

The haptic interfaces in Undercover, the haptic keypad, and the haptic wheel use bespoke hardware platforms, whereas the other haptics-based systems rely on standard hardware, including commercial actuators such as Braille cells and the vibrating elements integrated into mobile phones. We term these two approaches as physical and virtual systems.

Generally, empirical user performance has been higher with virtual systems. This reflects the fact that physical systems involve a challenging task—the construction of precise, reliable, and robust haptic displays. For example, the haptic wheel and phone lock have the same underlying interaction model, but the former is implemented on a dedicated stand-alone hardware device and the latter on a smartphone. Phone lock offers a 15 percent improvement in task time and 60 percent fewer errors. Other factors likely to have contributed to this performance delta include user familiarity with haptic output on smartphones and the richer input modality of the touchscreen surface. The haptic wheel's physical dial restricts users to rotating the device to move among targets; phone lock's virtual wheel also lets users hop between targets simply by touching different areas of the screen.

Generally, the complexities of creating high-quality haptic hardware support designing future PIN interfaces around existing platforms. Developing bespoke devices is time-consuming and costly, and they might provide suboptimal performance. However, custom hardware designs open the door to many interesting new application areas such as authentication interfaces for smart objects, tangible tools on tabletops, and ubiquitous systems. In sum, both approaches have strengths, but if performance is the key criterion, virtual interfaces are recommended.

LIMITATIONS

This work has two limitations: scope and novel forms of observation attack.

The first limitation relates to the fact that we constrain our discussion to two sensory modalities and a single domain: haptics and audio for PIN entry. A wide range of authentication techniques use technologies such as eye trackers, biometrics, graphical-pictorial passwords, bar codes, encoded light, and cognitive games in diverse application scenarios. A wider consideration of the performance of the systems we describe against the broad security literature will improve understanding of the strengths and weaknesses of authentication systems based on nonvisual cues.

The second limitation relates to the inherent susceptibility of haptics and audio to nonvisual sensor-based attack. Directional microphones, for example, might capture the noise generated by vibration motors or the sounds emitted from headphones, and an attacker could use this information to infer PINs. Exploring the feasibility of such attacks and the ease of defending against them via techniques such as generating disruptive noise are clear directions for future work. However, rather than consider these issues in detail here, we argue that nonvisual PINs increase the difficulty of observing PIN entry processes in public and that this represents progress toward more secure authentication compared to current PIN entry systems.

The guidelines presented here provide an initial structure for future work investigating nonvisual PINs. In addition, because PIN entry exemplifies the general constraints that apply to challenging, attention-demanding, nonvisual tasks, these guidelines and tradeoffs can help researchers studying cognitively intensive activities in other domains such as medical simulation and automotive interaction.

Although researchers have made significant progress in the design and performance of nonvisual PINs, extensions to this work are necessary. The most recent systems result in authentication times of 8 seconds and error rates of 2 percent. Although these figures are acceptable for occasional or high-security tasks (such as pairing devices or accessing secure facilities), they are considerably higher than standard keypad-based PINs. Reducing these figures to the levels required for everyday activities such as ATM access is a current challenge.

Researchers must also consider the feasibility of observation attacks based on nonvisual means—for example, by attackers listening for PINs behind a corner or secreting microphones in and around PIN entry equipment.

Indeed, although Ali Baba's age-old trick can still be fruitful, invisible PINs raise the bar and represent new barriers for even the most determined attackers.

References

1. B. Milligan, "The Man Who Invented the Cash Machine," *BBC News*, 25 June 2007; http://news.bbc.co.uk/2/hi/6230194.stm.
2. A. De Luca, E. von Zezschwitz, and H. Huffmann, "Vibrapass: Secure Authentication Based on Shared Lies," *Proc. Conf. Human Factors in Computing Systems* (CHI 09), ACM, 2009, pp. 913-916.
3. L. Giesen, "ATM Fraud: Does It Warrant the Expense to Fight It?" *Banking Strategies*, vol. 82, no. 6, 2006, pp. 43-46.
4. L. Lamont, "ATM Scam Netted $620,000 Australian," *Risks Digest*, Aug. 2003; www.smh.com.au/articles/2003/08/11/1060588322961.html.
5. A. Bianchi, I. Oakley, and D.S. Kwon, "The Secure Haptic Keypad: Design and Evaluation of a Tactile Password System," *Proc. Conf. Human Factors in Computing Systems* (CHI 10), ACM, 2010, pp. 1089-1092.
6. H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: Authentication Usable in Front of Prying Eyes," *Proc. Conf. Human Factors in Computing Systems* (CHI 08), ACM, 2008, pp. 183-192.
7. B. Malek, M. Orozco, and A. Saddik, "Novel Shoulder-Surfing Resistant Haptic-Based Graphical Password," *Proc. EuroHaptics Conf.*, Canadian Information Processing Soc., 2006, pp. 115-122.
8. C. Spence and J. Driver, "Cross-Modal Links in Attention Between Audition, Vision, and Touch: Implications for Interface Design," *Int'l J. Cognitive Ergonomics*, vol. 1, no. 4, 1997, pp. 351-373.
9. R. Kuber and W. Yu, "Feasibility Study of Tactile-Based Authentication," *Int'l J. Human-Computer Studies*, Mar. 2010, pp. 158-181.
10. S.A. Brewster and L.M. Brown, "Non-visual Information Display Using Tactons," *Proc. Conf. Human Factors in Computing Systems Extended Abstracts* (CHI 04), ACM, 2004, pp. 787-788.
11. A. Bianchi et al., "The Haptic Wheel: Design & Evaluation of a Tactile Password System," *Proc. Conf. Human Factors in Computing Systems* (CHI 10), ACM, 2010, pp. 3625-3630.
12. A. Bianchi et al., "The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods," *Proc. 5th Int'l Conf. Tangible, Embedded, and Embodied Interaction* (TEI 11), ACM, 2011, pp. 197-200.
13. T. Philippi, J.B.F. van Erp, and P.J. Werkhoven, "Multisensory Temporal Numerosity Judgment," *Brain Research*, Nov. 2008, pp. 116-125.
14. A. Bianchi, I. Oakley, and D.S. Kwon, "Spinlock: A Single-Cue Haptic and Audio PIN Input Technique for Authentication," *Proc. 6th Haptic and Audio Interaction Design* (HAID 11), LNCS 6851, Springer, 2011, pp. 81-90.

Andrea Bianchi *is a PhD candidate in the Graduate School of Culture Technology at KAIST, South Korea. His research focuses on the application of human-computer interaction to usability security. Contact him at andrea.whites@gmail.com.*

Ian Oakley *is an assistant professor of human-computer interaction at the University of Madeira, Portugal. His research interests include multisensory interfaces. Oakley received a PhD in human-computer interaction from the University of Glasgow. He is a member of ACM. Contact him at ian@uma.pt.*

Dong-Soo Kwon *is a professor of mechanical engineering and the director of the HRI Research Center at KAIST, South Korea. Kwon received a PhD in mechanical engineering from the Georgia Institute of Technology. Contact him at ptwonds@kaist.ac.kr.*