PassChords: Secure Multi-Touch Authentication for Blind People

Shiri Azenkot*, Kyle Rector*, Richard E. Ladner*, and Jacob O. Wobbrock†
Computer Science & Engineering*, The Information School†
DUB Group
University of Washington
Seattle, WA USA 98195
{shiri,rectorky,ladner}@cs.washington.edu, wobbrock@uw.edu

ABSTRACT

Blind mobile device users face security risks such as inaccessible authentication methods, and aural and visual eavesdropping. We interviewed 13 blind smartphone users and found that most participants were unaware of or not concerned about potential security threats. Not a single participant used optional authentication methods such as a password-protected screen lock. We addressed the high risk of unauthorized user access by developing *PassChords*, a non-visual authentication method for touch surfaces that is robust to aural and visual eavesdropping. A user enters a PassChord by tapping several times on a touch surface with one or more fingers. The set of fingers used in each tap defines the password. We give preliminary evidence that a four-tap PassChord has about the same entropy, a measure of password strength, as a four-digit personal identification number (PIN) used in the iPhone's Passcode Lock. We conducted a study with 16 blind participants that showed that PassChords were nearly three times as fast as iPhone's Passcode Lock with VoiceOver, suggesting that PassChords are a viable accessible authentication method for touch screens.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: User Interfaces – *Input devices and strategies, Voice I/O.*; K.4.2 [**Computers and society**]: Social issues – *assistive technologies for persons with disabilities.*

Keywords

Blind, mobile devices, touch screens, security, privacy.

1. INTRODUCTION

Mobile devices pose different security risks than traditional computers and require alternative security measures [1, 4, 13, 18]. For example, the small size and mobile nature of handheld devices increase the risk of loss or theft. Yet people routinely access email communications, contacts' information, online banking, and other private data without adequate user authentication mechanisms. Password entry on small touch keyboards is a common frustration for people [13], resulting in the use of shorter passwords, or avoidance of password protection entirely. Much recent work in the security literature has discussed such challenges, as well as the importance of mobile device security in general.

Figure 1: When entering passwords with an iPhone and VoiceOver, a user's input is spoken as she touches the screen, posing a severe security risk.

To the best of our knowledge, there are no published explorations of mobile device security for people with disabilities. Use of access technology on-the-go poses unique security risks for blind people that do not arise when sighted people use mobile devices, or when blind people use traditional computers. Blind people commonly interact with mobile devices via screen readers, such as Apple's VoiceOver for iOS devices, which read the contents of the screen and the user's input. Moreover, mobile computing with screen readers is often performed in public places, raising the risk of bystanders eavesdropping on one's private information. Suppose a blind person checks her email at a bus stop. A bystander may hear the blind person's device speaking the contents of an email, or information about the blind user's travel destination.

Another security issue that differs for blind and sighted users is accessibility of password entry. User authentication is an effective and common way to protect private data [15]. A recent study found that when smartphones were left

ASSETS'12, October 22–24, 2012, Boulder, Colorado, USA.
Copyright 2012 ACM 978-1-4503-1321-6/12/10 ...$15.00.

unattended in public places, 89% of people who found the phones attempted to access the phone owner's private information[1]. Use of a password to unlock the device screen protects against unauthorized user access. Yet password entry is likely to be an obstacle for blind users, since even sighted users find password entry on small touch screens to be a major frustration [14]. Moreover, screen readers introduce a severe vulnerability by speaking touched keys during password entry (see Figure 1). Over the past decade, the security community has explored the use of graphical authentication techniques as an alternative to alphanumeric passwords [16, 21, 25, 26]. These techniques do not require text entry but are inaccessible to blind people.

In this paper, we explore security issues that arise for blind people when using mobile devices. We focus on smartphone use, because of the wealth of private information that is accessed on these devices. We interviewed 13 blind smartphone users to discover their attitudes and specific behavior patterns that affect security risks. Most participants were not concerned with security issues, and none used optional authentication mechanisms to protect their information.

We sought to improve mobile device security by presenting a new accessible and secure authentication method called *PassChords*. PassChords are based on Input Finger Detection [3] and consist of several multi-point touches, defined by the set of fingers touching the screen. The PassChords algorithm determines which fingers touch the screen in each tap based on an initial set of reference points which the user inputs anywhere on the screen. Reference points indicate the approximate position of the user's fingers. PassChords have no audio feedback, so they are robust to aural eavesdropping. In a study with 16 blind people, we found that PassChord entry was nearly three times as fast as entry of accessible personal identification numbers (PINs) and had about the same authentication failure rate.

In summary, we present two contributions: (1) a study of security risks for blind mobile device users, and (2) PassChords, a new authentication technique for touch screens that is accessible, fast, and robust to aural eavesdropping.

2. RELATED WORK

Related work falls into two categories: security issues for blind people and mobile authentication techniques for the general population. Our work is the first, to our knowledge, to focus on security issues for blind mobile device users and develop and evaluate an accessible touch screen authentication method.

Kane et al. [17] discussed patterns and challenges of mobile device use for people with visual impairments and briefly mentioned users' privacy concerns. The authors did not delve into potential security problems. The study was conducted in 2009, before the iPhone introduced VoiceOver[2], the built-in screen reader on iOS devices. Since blind people now use touch screen devices, new security challenges have arisen, which we focus on in this paper.

Some work has been done in the area of accessible security, but, to our knowledge, none has focused on mobile devices. Kuber and Sharma proposed accessible authentication methods for desktop computers using a tactile mouse [19]. Several papers discussed the accessibility of CAPTCHA's [6, 12, 24], which are used to verify human users, but do not protect against unauthorized access. Our work concerns user authentication with accessible and secure password techniques.

The security community has widely acknowledged the inadequacy of alphanumeric passwords, and alternative authentication methods have been proposed. Graphical passwords [25] have been studied extensively over the past decade, including techniques that require users to select a sequence of photos that are displayed on the screen [10], to select a sequence of points in displayed images [26], or to draw a "secret" shape or design on a grid [16, 21]. These techniques are generally inaccessible to blind people.

One potentially accessible technique is TapSongs [27], a rhythm-based authentication method for devices with a single binary sensor (e.g., button). (TapSongs were later utilized and extended by Nokia researchers in their Rhythm-Link system; they named such rhythm-based passwords "tapwords" [20].) A difference between TapSongs and PassChords is that the duration of a TapSong was about 6-8 seconds, while PassChords tended to be less than 4 seconds long. Also, it is not clear what the entropy of TapSongs is so it is difficult to evaluate their security strength, although the Nokia researchers made some attempt to do so [20].

Biometric authentication offers another potentially accessible alternative to graphical or alphanumeric passwords [29]. Robust biometric techniques (e.g., iris scans, hand and fingerprint recognition) often require special hardware, that has not been adopted on mainstream mobile devices. Our approach is lightweight and requires only a touch surface.

3. THREATS AND DEFENSES

We outline security threats for blind mobile device users and possible defenses against them. Like sighted people, we assume blind people access private data such as email communications, text messages, social networking, online banking, contacts information, and travel directions. We also assume blind people use their devices in public places like buses, street corners, and cafes, where others are present nearby. Unlike for sighted people, however, we believe the following threats pose far greater risks for blind people because of screen reader technology or the lack of security features available in specialized access technologies.

We consider the following threats in this paper:

Aural eavesdropping. Casual or malicious bystanders may overhear private information spoken by screen readers. Additionally, as a user enters input, the screen reader echoes the user's button selections. This occurs when a user enters a password as well, as shown in Figure 1. The threat of aural eavesdropping has been studied in the security literature for more subtle audio feedback such as keystroke sounds [5, 11, 2], highlighting the severity of the threat for screen reader output.

Visual eavesdropping. Casual or malicious bystanders may oversee private information displayed on a mobile device screen. If a person with low-vision is using large fonts or screen magnification, people may see the screen's contents from an extended distance.

Unauthorized user access. Both blind and sighted people face this threat, which occurs when a device is mis-

[1] StreetWise Security Zone. 2012. The Honey Stick Project. http://www.streetwise-security-zone.com/members/streetwise/adminpages/honeystickproject

[2] Apple, Inc. iPhone Accessibility. http://www.apple.com/accessibility/iphone/vision.html

placed, lost, or stolen. We are interested in this threat because, as we discuss below, blind people may find it far more challenging to defend against it.

To assess the risk posed by the threats listed above, we enumerate possible defenses. In the following section we discuss how and when these defenses are used through an interview study, and asses threat risk.

Headphones. One can mitigate the risk of aural eavesdropping by using headphones when listening to screen reader output. However, when on-the-go, blind people use their hearing to understand their environment and using headphones may be unsafe or inconvenient. A blind person may not want to use headphones every time she enters a password to unlock her screen.

Screen occlusion. It is possible to physically cover a screen with a hand or use software such as the iPhone's Screen Curtain[3]. Some access technologies such as Braille displays or audio recorders may be used instead of smartphones, as they do not have screens at all. Not displaying visual output would mitigate the risk of visual eavesdropping but may be impractical or difficult to use. Also, people with some functional vision may benefit from visual output.

Password protection. Protecting a device with a password that requires a user to authenticate herself before using a device is an effective defense against unauthorized user access. Many access technologies do not have password locks, however. People using smart devices that do have such features may find the standard password techniques to be too slow and error-prone (in addition to being insecure, because of screen readers speaking the input password).

4. SECURITY-RELATED USAGE PATTERNS

Defenses against security threats have trade-offs and may negatively impact a user's experience with a device. We conducted interviews with blind people to understand how and why possible defenses were practiced. This enabled us to asses the risk of the security threats in our model.

4.1 Method

4.1.1 Participants

We recruited 13 participants (6 male, 7 female). The average participant age was 51 years (age range 26–64). We required that participants (1) were legally blind and (2) used smartphones daily. Two participants had some functional vision, one had light perception, and the remaining 10 were completely blind. Participants were recruited through email lists that catered to blind people.

4.1.2 Procedure

We conducted a semi-structured interview with each participant. All interviews were conducted over the phone and lasted about 20 minutes. We began by asking participants for demographic information such as gender and age. Then, we asked questions in the following categories: (1) context and frequency of mobile device use, (2) types of information accessed on mobile devices, (3) use of passwords on mobile devices, (4) use of headphones, and (5) use of screen occlusion techniques.

4.1.3 Analysis

The interviews were transcribed, coded, and then organized based on interview questions.

4.2 Results

All participants owned iPhones that they used with the VoiceOver screen reader. When on the go, 6 participants also carried a Braille notetaker, 2 carried accessible GPS systems, 1 carried a portable CCTV, and 1 carried a laptop. All devices were used on a daily basis in various contexts, including public places such as streets, cafes and restaurants, and also at home and at an office.

As expected, participants stored a wealth of private and personal information on their devices:

> *Gosh, you know [my iPhone] is just a part of me. I can't think of anything I don't do [on it].*

Participants regularly accessed private information, including email communications, social networking sites, and location-tracking applications such as Four Square. Nearly half of the participants used banking applications on their iPhones. One participant expressed a preference for accessing private data on her Braille notetaker, because others could not hear or see what she was reading.

None of the participants used optional authentication features to protect the information on their devices. In fact, the iPhone was the only device mentioned that *had* an authentication feature. All but one of the participants were aware of the iPhone's password protection feature, the Passcode Lock, and had decided not to use it. Some participants stated using the Passcode Lock was inconvenient: "No, [Passcode entry] is inconvenient—I don't want to do that"; others thought it was unnecessary: "...because I have my [iPhone] with me all the time."

Passwords were entered only when required by some applications that participants used, such as Facebook and Netflix. These passwords were usually stored by the applications, however, and did not require repeated entry. One participant expressed concern regarding aural eavesdropping, noting that VoiceOver spoke a key label as it was touched during password entry.

All participants used headphones when listening to screen readers in public spaces; 12 participants used headphones regularly (but not exclusively), and the remaining participant used them occasionally. Three participants (partly) attributed headphone use to concerns about aural eavesdropping, but most used headphones to avoid disturbing others around them or simply for better sound quality. There was a trade-off between the advantages of headphones and the need to hear sounds in one's environment.

> *I like to listen on the headphones but I don't like to have my hearing completely blocked out because it's hard to hear a bus stop and if there is something happening on the bus I need to be hearing. You know, like a fight or who knows?*

The iPhone's Screen Curtain feature, which disables visual output, was used by 10 participants; not being able to see the screen may serve as a security advantage for them. Four participants used the Screen Curtain to prevent visual eavesdropping, and most participants cited the desire to save battery power (the advertised purpose of the Screen Curtain).

[3] Apple, Inc. iPhone Accessibility. http://www.apple.com/accessibility/iphone/vision.html

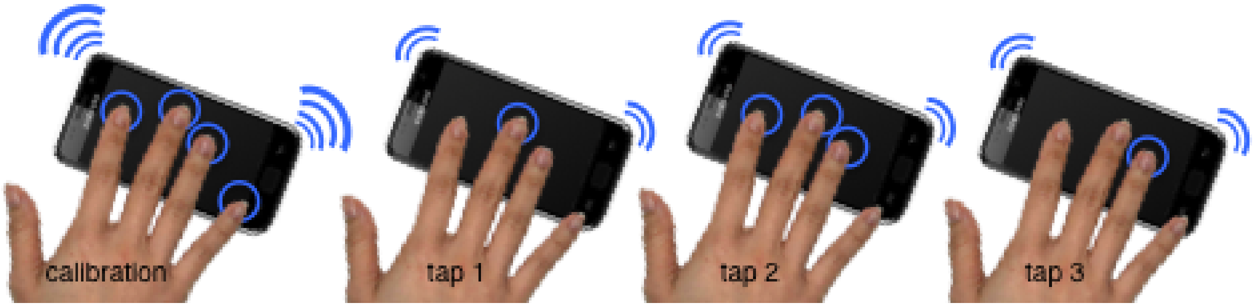

Figure 2: A user calibrates (left) and enters a 3-tap PassChord. The blue circles show which fingers contact the screen in the figure but do not appear as output to the user. Note that the fingers are not striking bounded regions like buttons; rather, the finger locations are interpreted probabilistically, meaning some flexibility in their hit-location is allowed, while the number and identity of the fingers is appropriately strict.

> *I love that people can't look over my shoulder and see what I'm doing.*

No other screen occlusion techniques (e.g., holding the device close to one's chest) were used.

While participants occasionally mentioned security threats, their primary concerns were related to iPhone accessibility. Participants had difficulty inputting text and accessing information from applications that were not compatible with VoiceOver. Several participants noted the physical challenge of interacting with their devices while using a cane. Only three mentioned the security risks associated with online banking, location tracking, and aural and visual eavesdropping. One participant acknowledged the need for better security mechanisms, although, like other participants, he did not use optional authentication methods.

> *I feel like I should use [security features on [my iPhone] and I'll probably be sorry one day that I didn't.*

4.3 Discussion

Our results indicate that a minority of users are aware of security threats, including aural and visual eavesdropping, and unauthorized user access. This is disturbing, but not surprising given that related work found that the general population lacks awareness and understanding of security threats [9, 15, 22]. We concur with this prior work that users should receive better training—whether from Orientation & Mobility instructors or blindness organizations in general—about potential mobile device security risks.

The finding that our participants did not use optional authentication methods like the Passcode Lock to protect their devices from unauthorized user access was most alarming. Clarke and Furnell [9] report that one third of 297 (all sighted) participants locked their phones with PIN-based authentication, noting that this ratio was low. The fact that no participants used a Passcode Lock in our study was egregious, highlighting the severe risk of unauthorized user access. Text entry rates with VoiceOver were only about 4 words per minute (WPM) [3], so it may be infeasible for blind people to enter a PIN every time they unlocked the screen of their phone.

Security threats from aural and visual eavesdropping were mitigated by use of headphones and the Screen Curtain. Although all participants used headphones, they acknowledged their disadvantages. Security defenses should, therefore, not solely rely on headphone use, especially for highly private information such as passwords. Screen Curtains were not used by all participants, and participants were generally unaware of the need for protect against visual eavesdropping. It would be interesting to interview people who used magnification rather than screen readers, since magnification increases the risk of visual eavesdropping.

5. SECURE AUTHENTICATION WITH PASSCHORDS

The most severe security problem we identified from our study is the risk of unauthorized user access, which may be attributed to lack of user awareness, and the inaccessibility and insecurity of current password techniques. To address this problem, we developed a new touch screen authentication method that is entirely non-visual, faster than PIN techniques, and robust to aural eavesdropping.

5.1 Design Principles

When developing an authentication method, we considered several design principles based on our interview study, our threat model, and standard authentication guidelines [1, 23]. These principles emphasize both security and usability.

1. Speed. Users should be able to enter a password quickly.
2. Robust to aural eavesdropping. Users should be able to input a password without audio feedback that broadcasts their input.
3. Robust to visual eavesdropping. There should be little or no visual indication of the user's input.
4. High password strength. Password strength should not be sacrificed and the technique should be robust to guessing or brute-force attacks.
5. High recall. Passwords should be easy to remember.

5.2 The PassChords Technique

PassChords are a new authentication technique based on Input Finger Detection [3], where a user taps a touch surface several times with 1 to 4 fingers (see Figure 2). The PassChord is defined by the set of fingers used in each tap. At the beginning of a PassChord entry, the user calibrates the touch surface by entering reference points, which the PassChords algorithm uses to model the true locations of the fingers on the screen.

The PassChords algorithm determines which fingers touched the screen using Maximum Likelihood (ML) detection given the finger reference points. In Input Finger Detection [3], the variance of each finger is tracked and used in the ML detection. Since PassChords are short and we assume that, unlike in text entry, a user will not enter many PassChords in succession, we do not track variance. Instead, we assume equal variance for each fingers. ML thus reduces to finding the set of reference points that have the minimum combined distance from the set of input points.

As the user enters a PassChord, she receives only vibration feedback with no visual or audio output. A short vibration is produced when the user touches the screen. To calibrate, a user presses 4 fingers to the screen until a second vibration is produced less than a second later. No further feedback is needed because, as with any chording technique, people can discern their input through proprioception. Techniques that rely on a fingertip at a certain position require audio feedback because different inputs "feel" the same.

We believe that PassChords would be easy to remember because the chording nature of the technique is evocative of playing a piano or another chording instrument. Also, people may associate numbers with the fingers used, allowing similar recall techniques to numeric passwords.

5.3 Entropy

Information entropy is a commona measure of password strength, indicating how robust a technique is to guessing or brute-force attacks [8]. In this metric, the information entropy of a password of n symbols from a symbol set of size m is $\log_2 m^n$, measured in bits. In other words, the information entropy of a password technique is the minimum number of bits needed to encode the set of all possible passwords, assuming all symbols are equally likely.

In one tap of a PassChord, there are 15 possible finger combinations. Each of 4 fingers is either touching the screen or not, and a tap where all fingers are not touching the screen is invalid. A PassChord with 4 taps therefore has information entropy $\log_2 15^4 \approx 15.6$ bits. By contrast, consider a standard PIN's information entropy. Each digit in the PIN has 10 possible inputs, so a 4-digit PIN has information entropy $\log_2(10^4) \approx 13.3$. Both the 4-tap PassChord and the 4-digit PIN require the same number of symbols as input, but the information entropy of the PassChord technique is higher, indicating it may be more robust to attacks.

The information entropy assumes that all symbol entries are equally likely, which is probably not true for PIN entry and certainly not true for tap entry. As we will see in our study, some finger combinations are more likely than others because of the physiology of the hand. For example, simultaneously tapping the middle and pinky fingers is more difficult than tapping the index finger. A better estimate of the entropy of password strength is the first-order entropy:

$$H = n \sum_{i=1}^{m} p_i \log_2(1/p_i), \tag{1}$$

where p_i is the probability of symbol i occurring in any position in a password. We will empirically calculate H from user data to estimate the security strength of PassChords.

5.4 Evaluation

To evaluate the PassChords authentication technique, we sought to compare PassChords to a standard password technique. We chose the iPhone's Passcode Lock with VoiceOver as a basis for comparison, which consists of a 4-digit PIN that is entered with an on-screen number pad.

5.4.1 Method

Participants. We recruited 16 blind participants (8 male, 8 female), with an average age of 51 (age range 27–61). While all were legally blind, five participants had some vision and were able to identify numbers on an iPhone's number pad. The remaining 11 had no functional vision. Eight participants had experience with VoiceOver on iOS devices. We recruited participants through mailing lists that communicated with blind people.

Apparatus. We built prototype applications for PassChord and PIN entry. We did not use an iPhone's built-in Passcode so we could instrument the application. The PIN application was visually similar to the iPhone's Passcode Lock, enabling split-tap and double-tap selection of keys. As with the iPhone, the PIN application spoke button labels as they were touched, but did not provide feedback when a number was entered. Both applications logged every user input.

A Samsung Galaxy phone was used for all user studies, with a 4-inch screen.

Procedure. Participants completed two sessions, one with each authentication method. The beginning of each session included a training period, where we taught participants how to use the method for the current session. Participants practiced the method until they were able to authenticate with three different passwords.

After training, participants entered three passwords: the first was prescribed by the experimenter and the other two were created by the user. We sought to simulate a realistic password creation and entry scenario, so we asked participants to create a password, confirm it, and then enter it 20 times. The confirmation of a password allowed participants to practice their new password and ensure they had created it as intended.

The first PIN was a randomly generated sequence of 4 digits. The first PassChord included three touches, each consisting of one randomly selected finger. We anticipated certain multi-finger combinations would be difficult for participants, so we gave them a PassChord where each touch included only one finger. For the next two PassChords, we instructed participants to create a PassChord where at least one of the touches had more than one finger. For both methods, participants were instructed to create passwords that were "realistic."

Participants were able to correct errors during password entry. The VoiceOverPIN number pad included a BACKSPACE key. A PassChord could be "reset" if the user made an error by calibrating and re-entering the PassChord. Such errors and corrections were included in the time measured for a given password entry.

After entering three PassChords repeatedly, we asked participants to create yet another PassChord which they were tasked to memorize. Two days after the study we called each participant and asked them to repeat the memorized PassChord. We instructed participants to behave as though

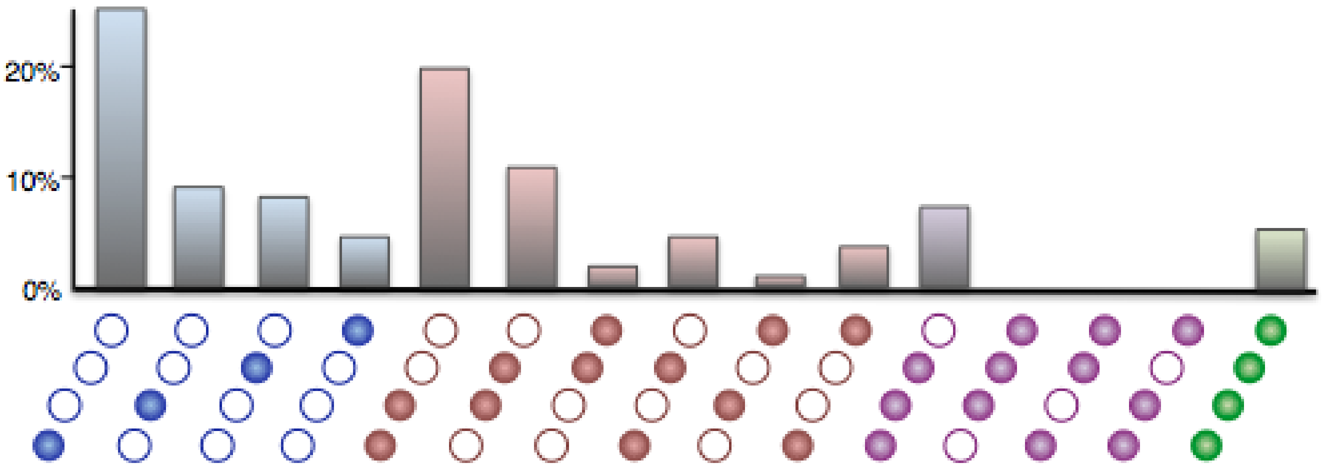

Figure 3: PassChord pattern frequencies. A sequence of circles represents a tap pattern, with the index finger shown on the bottom left and the pinky finger on the top right. Certain patterns were chosen far more often than others.

this was a "real" password, and use whatever memorization technique seemed appropriate.

Design and Analysis. The study was a within-subjects factorial design with two factors, *Method* and *Order*. The levels of *Method* were (PassChords, VoiceOverPIN) and the levels of *Order* were (1, 2). The *Order* factor indicated whether the current *Method* was performed first or second in the study, allowing us to evaluate possible crossover effects.

We analyzed two measures: authentication time and failure rate. The former was measured as the difference between the time of the first and last touch events of a password (including PassChord calibration), and the flatter was the proportion of times the user failed to authenticate. The failure rate included completed passwords that turned out to be incorrect, not counting errors that were corrected by the user with the BACKSPACE key or a re-calibration. Such errors were subsumed by the password entry time. Both measures were analyzed with mixed-effects model analysis of variance, with a fixed effect for *Method* and a random effect for *Participant* to account for correlated measurements for different methods within subjects. Authentication times were averaged for trials in each method. We used a significance level of $\alpha = 0.05$.

Neither authentication time nor failure rate was normally distributed ($W = 0.90$, $p < 0.001$ for time; $Shapiro - WilkW = 0.89$, $p < 0.001$ for failure rate). Therefore, we used the nonparametric *Aligned Rank Transform* procedure [28], which enables the use of ANOVA after alignment and ranking, while maintaining the integrity of interaction effects.

5.4.2 Results

Authentication time. PassChords were nearly three times as fast as VoiceOverPINs. The mean authentication time for PassChords was 2.67 seconds ($SD = 0.722$), while that for VoiceOverPIN was 7.52 seconds ($SD = 2.40$). This difference resulted in a significant effect of *Method* on authentication time ($F_{1,13} = 113.6, p < 0.001$).

The number of taps per PassChord ranged between 3 and 6 taps, and the mean time per tap was 0.62 seconds ($SD = 0.17$). The mean time for a VoiceOverPIN input was 1.89 seconds ($SD = 0.60$). Thus, it is evident that PassChords would have outperformed VoiceOverPINs if we had required an equal number of inputs for each. The large difference was not surprising since participants often had to search for the correct VoiceOverPIN input by moving their finger across the screen while listening to screen reader output.

Strangely, there appeared to be an asymmetric skill transfer between methods. Participants who entered PassChords after they had entered VoiceOverPINs performed better with PassChords than participants who entered PassChords first. This resulted in a significant effect of *Order* ($F_{1,13} = 12.8, p < 0.01$) and a significant interaction of *Method* by *Order* ($F_{1,13} = 10.0, p < 0.01$). As Figure 4 shows, however, the difference between method entry times was incontrovertible, in spite of the effect of order.

Failure rate. There was no speed-accuracy trade-off, as the failure rate was slightly lower for PassChords than for VoiceOverPIN. Participants failed to authenticate 16.3% of the time with PassChords ($SD = 14.5\%$) and 20.2% of the time with VoiceOverPIN ($SD = 17.3\%$). This differences were not significant, however ($F_{1,13} = 1.49, n.s.$).

Recall. Twelve of the 16 participants (75%) remembered their PassChord two days after they were asked to memorize it. Most participants tapped the password several times to memorize its "feel," and associated the fingers in each tap with numbers to memorized their pattern.

Password strength. We assess password strength by observing common patterns in the 32 user-generated PassChords. Our prior discussion of entropy assumed a uniform distribution of possible inputs. This is not the case, however, for user-generated passwords. Prior work shows that the most common digit in alphanumeric passwords is 1, and the most common letters are *a*, *e*, *o*, and *r* [7]. Such patterns reduce the difficulty of guessing or brute-force attacks, so they are important to identify and avoid [8].

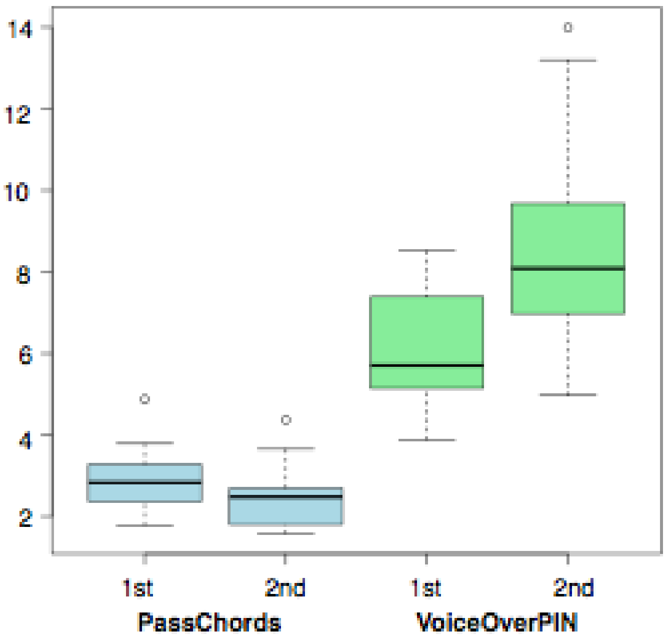

Figure 4: Boxplots of password entry times (in seconds) for the first and second half of the study and for each method. Although there is an asymmetric skill transfer, PassChords were irrefutably faster than VoiceOverPINs.

Figure 3 shows the frequency of each tap pattern in the user-generated PassChords. A striking trend was the frequent use of the index finger, which was present in 66.5% of taps. The pinky finger was used least, in only 14.6% of taps (see Table 5.4.2). Users tended to create passwords with repeating finger combinations and individual taps were often made with adjacent fingers. The most common PassChord length was three taps, although this may be attributed to the length of the initial, prescribed PassChord that served as an example.

Finger	Frequency
Index	66.5%
Middle	51.7%
Ring	36.6%
Pinky	14.6%

Table 1: Frequencies of finger use in PassChord taps. There was a strong preference for using the index finger, which is often used for touch screen input.

5.5 Discussion

We have shown through the design and evaluation of PassChords that our design principles were satisfied. In terms of usability, PassChords are nearly 75% faster to enter than accessible PINs, with comparable authentication failure rates. While merely preliminary, our study of PassChord recall demonstrated that there were no unexpected obstacles with PassChord memorization.

The security of PassChords was considered in their design and evaluation. Unlike accessible PINs, PassChords produce no audio feedback, so they are more resistant to aural eavesdropping. PassChords also display no visual feedback, making visual eavesdropping more challenging. It would be interesting in future work to assess the threat of "shoulder-surfing" attacks that occur when an adversary eavesdrops by looking over a user's shoulder and observing her finger motions.

The data collected in our study, which included 112 PassChord taps and 128 PIN digits, yields preliminary estimates of the security strength in terms of first-order entropy using Equation (1). The first-order entropy of 4-tap PassChords was $H \approx 12.6$, comparable to the first-order entropy of 4-digit PINs of $H \approx 12.7$. Our sample size was too small to produce these estimates with high confidence, but they give a rough idea for the security strength of both methods.

The security strength of PassChords can be improved by ensuring that the distribution of taps is as close to a uniform distribution as possible and using as many taps as possible. This leads us to several guidelines to help users create more secure PassChords:

1. Use each finger at least once in your PassChord.
2. Use taps of one, two, and three fingers.
3. Use four or more taps in your PassChord.

Since knowledge-based passwords are common authentication mechanisms, we believe PassChords will impact the security of mobile devices for blind people. They are an important first step at addressing security challenges for blind mobile device users, as discussed in our threat model. Since entering passwords on small touch keyboards is challenging for sighted users as well, we believe PassChords would benefit people with all visual abilities.

6. FUTURE WORK

There is much potential for future work in the area of security for people with disabilities. It would be interesting to explore security risks for people with other disabilities, such as deaf people or those with motor impairments. Users with low-vision may experience security and privacy threats related to magnification that vary greatly from those for people with little to no functional vision, which we have focused on in this work.

We plan to deploy PassChords and study user password behavior in the field. It would be interesting to see how performance improved with practice, and analyze the guessing entropy with a larger data set of user-generated passwords. We are interested to determine how robust PassChords are to "shoulder-surfing" attacks.

Finally, we plan to address other security risks discussed in this paper. The PassChords technique aims to prevent unauthorized user access and password eavesdropping, but open questions remain regarding the prevention of aural and visual eavesdropping in general.

7. CONCLUSION

We have presented (1) an investigation of security issues related to blind mobile device users and (2) the new PassChords authentication technique that addresses the threat of unauthorized user access. The PassChords technique is unique because it provides no audio or visual feedback, making it robust to eavesdropping attacks yet fully accessible to blind people. We have shown through an evaluation with 16 blind people that PassChords were significantly faster to enter than accessible touch screen PINs. We believe PassChords will be useful for both blind and sighted people, and hope that this work will shed light on security issues for people with various disabilities.

8. ACKNOWLEDGMENTS

The authors thank Alan Borning and Tadayoshi Kohno. This work was supported in part by the National Science Foundation under grant CNS 0905384 and grant IIS-0952786, and by the US Department of Education under grant H327A100014.

9. REFERENCES

[1] N. Asokan and C. Kuo. Usable mobile security. In *ICDCIT*, pages 1–6, 2012.

[2] D. Asonov and R. Agrawal. Keyboard acoustic emanations. In *IEEE Symposium on Security and Privacy*, pages 3–11, 2004.

[3] S. Azenkot, J. O. Wobbrock, S. Prasain, and R. E. Ladner. Input finger detection for nonvisual touch screen text entry in perkinput. In *Proc. GI'12*, New York, NY, USA, 2012. ACM.

[4] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller. On the need for different security methods on mobile phones. In *Proc. MobileHCI'11*, pages 465–473, New York, NY, USA, 2011. ACM.

[5] Y. Berger, A. Wool, and A. Yeredor. Dictionary attacks using keyboard acoustic emanations. In *Proc. CCS'06*, pages 245–254, New York, NY, USA, 2006. ACM.

[6] J. P. Bigham and A. C. Cavender. Evaluating existing audio captchas and an interface optimized for non-visual use. In *Proc. CHI'09*, pages 1829–1838, New York, NY, USA, 2009. ACM.

[7] M. Burnett. *Perfect passwords*. Syngress Publishing, Rockland, Massachusetts, 2006.

[8] W. E. Burr, D. F. Dodson, W. T. Polk, and D. L. Evans. Electronic authentication guideline. In *NIST Special Publication*, 2004.

[9] N. Clarke and S. Furnell. Authentication of users on mobile telephones: A survey of attitudes and practices. *Computers Security*, 24(7):519–527, 2005.

[10] R. Dhamija and A. Perrig. Deja vu: A user study using images for authentication. In *Proc. USENIX Security Symposium*, pages 45–58, Berkeley, CA, USA, 2000. USENIX Association.

[11] D. Foo Kune and Y. Kim. Timing attacks on pin input devices. In *Proc. CCS'10*, pages 678–680, New York, NY, USA, 2010. ACM.

[12] J. Holman, J. Lazar, J. H. Feng, and J. D'Arcy. Developing usable captchas for blind users. In *Proc. ASSETS'07*, pages 245–246, New York, NY, USA, 2007. ACM.

[13] M. Jakobsson. Why mobile security is not like traditional security, 2011. http://www.markus-jakobsson.com/wp-content/uploads/fc11jakobsson.pdf.

[14] M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit authentication for mobile devices. In *Proc. HotSec'09*, pages 9–9, Berkeley, CA, USA, 2009. USENIX Association.

[15] W. Jansen, K. Scarfone, C. M. Gutierrez, D. Patrick, D. Gallagher, and D. Director. Guidelines on cell phone and pda security recommendations of the national, 2008.

[16] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. The design and analysis of graphical passwords. In *Proc SSYM'99*, pages 1–1, Berkeley, CA, USA, 1999. USENIX Association.

[17] S. K. Kane, C. Jayant, J. O. Wobbrock, and R. E. Ladner. Freedom to roam: a study of mobile device adoption and accessibility for people with visual and motor disabilities. In *Proc. ASSETS'09*, pages 115–122, New York, NY, USA, 2009. ACM.

[18] V. Kostakos. Human-in-the-loop: rethinking security in mobile and pervasive systems. In *CHI EA '08*, pages 3075–3080, New York, NY, USA, 2008. ACM.

[19] R. Kuber and S. Sharma. Toward tactile authentication for blind users. In *Proc. ASSETS'10*, pages 289–290, New York, NY, USA, 2010. ACM.

[20] F. X. Lin, D. Ashbrook, and S. White. Rhythmlink: securely pairing i/o-constrained devices by tapping. In *Proc. UIST'11*, pages 263–272, New York, NY, USA, 2011. ACM.

[21] P. C. v. Oorschot and J. Thorpe. On predictive models and user-drawn graphical passwords. *ACM Trans. Inf. Syst. Secur.*, 10(4):5:1–5:33, Jan. 2008.

[22] K. Poulsen. Mitnick to lawmakers: People, phones and weakest links, 2009. http://www.politechbot.com/p-00969.html.

[23] B. Schneier. The secret question is: why do IT systems use insecure passwords? *The Guardian*, 2009. http://www.guardian.co.uk/technology/2009/feb/19/insecure-passwords-conflickerb-worm.

[24] S. Shirali-Shahreza and M. H. Shirali-Shahreza. Accessibility of captcha methods. In *Proc. AISec'11*, pages 109–110, New York, NY, USA, 2011. ACM.

[25] X. Suo, Y. Zhu, and G. Owen. Graphical passwords: a survey. In *Computer Security Applications Conference, 21st Annual*, page 472, dec. 2005.

[26] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. In *Proc. USENIX Security Symposium*, pages 102–127, Berkeley, CA, USA, 2005. USENIX Association.

[27] J. O. Wobbrock. Tapsongs: tapping rhythm-based passwords on a single binary sensor. In *Proc. UIST'09*, pages 93–96, New York, NY, USA, 2009. ACM.

[28] J. O. Wobbrock, L. Findlater, D. Gergle, and J. J. Higgins. The aligned rank transform for nonparametric factorial analyses using only anova procedures. In *Proc. CHI'11*, pages 143–146, New York, NY, USA, 2011. ACM.

[29] Q. Xiao. Security issues in biometric authentication. In *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, pages 8–13, june 2005.