Coping with Accessibility Challenges for Security - A User Study with Blind Smartphone Users

Sylvan Lobo, Ulemba Hirom, V. S. Shyama, Mridul Basumatori, Pankaj Doke

Coping with Accessibility Challenges for Security - A User Study with Blind Smartphone Users

Sylvan Lobo, Ulemba Hirom, Shyama V S, Mridul Basumatori, Pankaj Doke

Tata Consultancy Services Ltd.

{sylvan.lobo, ulemba.h, shyamav.s, mridul.basumotari, pankaj.doke}@tcs.com

Abstract. Widespread adoption of touchscreen phones among blind users seems inevitable. Blind users face significant challenges in terms of accessibility and inclusion in the smartphone environment, despite prevalence of screen-readers and assistive software. This can lead to a variety of security and privacy risks while using smartphones. This paper presents qualitative research findings of a user study about security and usability aspects of smartphone usage by 51 blind smartphone users of age 18 to 40 years in a metropolitan city of India. We discuss the challenges users face, their coping strategies, and key insights that could inform design for security and usability.

Keywords: Usable Security · Blind · Smartphone · Android · iPhone

1 Introduction

Smartphones are increasingly being adopted in India [1]. As an information device, a smartphone is very personal and portable compared to desktop computers and laptops. Users tend to keep their phone with them at all times for a variety of personal information needs. It is always powered on and available on voice and data networks. This makes the smartphone attractive and vulnerable to security and privacy threats.

There is a large population of visually impaired users, who are increasingly using touchscreen-based smartphones. Visually impaired users earlier used Symbian phones which were quite accessible with their assistive features and tangible keypads. Currently we observe that market forces seem to drive users to shift to touchscreen-based smartphones, primarily Android and iPhone. There has been considerable development [2–4] in accessibility on these smartphone devices, both on iPhone and Android. Yet users still face usability challenges in certain situations where using the phone may be challenging (e.g. public transport, walking, crowded situations) [5] or simply due to unfamiliar or infrequently used interfaces. Considering the accessibility and usability challenges that visually impaired smartphone users face, we feel they are also more vulnerable with regards to privacy and security. E.g. using passwords and phone locks,

or typing itself can be time consuming and error prone with currently available accessibility modes [6]. Users also perceive privacy concerns while using accessibility modes [7].

The global visually impaired population is of a considerable size [10], with around 5 million in India alone (some report 15 million) [11, 12]. The World Health Organization (WHO) reported an estimate of 8 million people with total blindness [13] in India in 2010 [10]. Mumbai, India, is reported to have a visually impaired population of around 0.12 million [14]. We found it imperative to include visually impaired smartphone users in smartphone security studies, to help understand threats that they may be exposed to and their current practices, eventually aiding in building better usable security for smartphones. For this study, we have only considered users with total blindness [52] users (rather than users with other visual impairment. As per American Foundation ® for Blind, total blindness refers to *"an inability to see anything with either eye."* [52]. We feel blind users would face such security and privacy risks and challenges more severely than sighted users and users with other visual impairments. Investigating these challenges would hopefully help in addressing concerns other visually impaired users too.

In this paper, we present the findings of our contextual inquiry based interviews with 51 totally blind smartphone users in Mumbai, India, with regards to their security and privacy practices with smartphones (Android and iPhone), their coping strategies with security measures such as passwords and native access control measures such as PIN, pattern locks and slide locks. We first review the relevant previous research, present the method used in our study and then highlight the outcomes of the affinity analysis of the contextual inquiry discussed from the perspective of security and usability, followed by a discussion of implications for design.

2 Previous research

There have been numerous studies with sighted users [9, 12, 13, 15, 20, 22–24, 27] as well as visually impaired users [1, 2, 4, 10, 11, 21] with smartphones, laptops and internet on various aspects of usability, privacy and security, although we have not found relevant empirical studies with visually impaired or blind users in India with regards to their security and privacy practices and behavior with smartphones.

2.1 Mobile security studies with sighted smartphone users

Studies with sighted users suggest that users are generally concerned about privacy and security on their smartphones (even more so than on laptops). They are often signed in to multiple accounts on their phone, and use the phone to perform financial and other private transactions [9, 24]. The indispensable, personal and highly portable nature of the smartphone demands that it be well protected from threats of data loss, compromise and privacy, including threats such as loss of phone due to damage, theft or misplacing; unauthorized access through malware or physical access; and location tracking [15].

Asokan and Kuo [27], Ben-Asher et al. [28] and Jakobsson [29], all argue that security approaches for mobile phone environments need to be revisited as the environment and usage differs markedly from traditional computers. Smartphones do provide some measures to mitigate risks [23], but the decisions are often delegated to the users themselves, who may not be sufficiently prepared or have the awareness to take correct decisions [22]. However, studies suggest that users are not well informed about security and privacy decisions [23] and may often take inappropriate decisions. Users often do not find security features essential and keep them disabled [22] [16]. People also root or jailbreak their phones (Android and iPhone terminology to enable the phone for root or administrative access), leaving the phones vulnerable [22]. Users avoid regularly upgrading the operating system, missing security patches. There are many apps available from non-official sources in the market places or app stores. In order to make decisions about installing apps, users tend to rely on the price (i.e. free or very cheap) and popularity based on recommendations from friends and user reviews, rather than studying the end user license agreements, privacy policies and app permissions [15]. Users do not pay much attention nor comprehend the policies and app permissions [30]. Uses exhibit a 'click through' behavior when faced with various information prompts. Users trust the app repository with misconceptions that apps are tested for security [22].

One common means of protecting information is using authentication means like passwords or phone locks. Yet many users do not use any phone locking mechanisms such as PINs or pattern locks simply due to usability issues and a need to access the phone quickly, despite the presence of private and sensitive content on the phone [20]. Users would rather keep the phone within sight at all times, without any password protection. This form of lock-based protection on phones provides an all-or-nothing access [19], and is quite risky considering passwords saved within apps are common [20] and users are not required to key-in passwords frequently. Users report that they use simple passwords such as names or dictionary words. Users also store their passwords on their phones as contacts in plain text [20].

Users consider data such as GPS tracking, SMS, Phonebook contacts, Multimedia content (such as videos, photos and recordings), emails, documents and notes as most private, valuable and sensitive [20]. They tend to not trust keeping private data in the cloud, and prefer storing data on their computers or hard disks unless the data is shareable [20]. People do share phones among themselves for music, entertainment and making calls, but would rather have the phone in sight and depend on their relationship with the other users. Users tend to consider it a higher threat to share phones with known people rather than with strangers [20]. Photographs and messages are kept private from known people and contacts private from strangers. Unauthorized access to the phone seems fairly common [21]. Chen et al [31] also discuss Internet security practices of users in the context of users in a developing nation. Recent work by Alsaleh et al. [32] discusses smartphone security practices of users from the dimensions of behavioral change and provide persuasive approaches for addressing unsafe practices.

2.2 Mobile security studies with visually impaired smartphone users

Challenges of usability and accessibility enhance the security challenges faced by visually impaired users. Touchscreens lack tangible feedback, and users mostly depend on aural feedback or assistive devices (screen readers, zoom). There are various studies on security and privacy related aspects for visually impaired users [6, 24–26] and considerable advancement [2–4] in accessibility on touchscreen . Commonly performed activities on smartphones (and computers) include reading and writing emails, browsing internet for entertainment, downloading/uploading files, education, listening to podcasts, instant messaging, and interacting on social media platforms [18]. Users also transact and bank online, but usually prefer using desktops and laptops over smartphones.

Azenkot et al. [6] found that visually impaired users are generally not aware or concerned about security, and often use their phones without password protection primarily due to inconveniences faced. For example, the phone allows passwords to be masked, i.e. the screen reader reads the characters as stars or clicks while the user types in the password. This however makes it near impossible for users to type, i.e. without text entry feedback on a touchscreen device, users are clueless about what they are typing. If the user chooses to not mask the passwords, the screen reader speaks the characters aloud, which is again not desirable for keeping the password private. Users also find password managers, password recovery mechanisms, and typing itself quite difficult [24]. Users often tend to store their password elsewhere written in Braille or in files, or save them within apps [24].

There is also a lack of sufficient feedback while browsing the Internet or using smartphones, using the assistive features available. Some users hence spend less time online [18]. For instance, browser do not highlight phishing in an easily accessible manner, and feedback about errors is poor. Often user interfaces change frequently [24], which means the user needs to learn how to use the interface again.

In terms of privacy, visually impaired users frequently face the risk of being eavesdropped, both aurally and visually, in almost all activities they perform on the phone as they are often not sure when people are in their vicinity [24]. They feel a lack of independence and have to rely on sighted users for assistance, often strangers where they need to disclose private information in various situations such as filling forms, or reading messages or letters. Some users hence prefer online transactions and online shopping over shopping in real stores, although they still have concerns of security [24]. Users have various strategies to maintain privacy like relying on close relations such as spouse, family or close friends; using assistive technology; using screen curtains to black out the display; using headphones; or using the screen reader at low volume or at a very fast talking rate where others would find it difficult to understand.

As seen in the background literature, visually impaired users as well as sighted users face quite a few security and privacy challenges with their smartphones. They risk and often fail to protect their data effectively. The lack of awareness and inconvenience due to which users do not take appropriate measures can be attributed to usability and accessibility issues in interfaces and mechanisms provided for achieving the goals of security and privacy. The security goals in themselves are not primary, although a single

event of compromise of data or privacy can prove disastrous to users. The phone is shipped with security features but in the context of the user they are not usable.

2.3 Usability and security

Usability can be defined as the: *"extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."* (ISO 9241 210:2010) [33, 34].

Products are generally created with goals of usability. There are various methods to assess usability such as Nielsen's [35] usability heuristics or Joshi's [36, 37] Usability Goals Tool (UGT). Usability goals could include: ease of use where the conceptual model is communicated clearly so that there is a match between users' mental model and the product, without entry barriers and unnecessary tasks, minimizing user task load, and always accessible. Operation of the product should be error-free, should not induce errors and the user should be able to recover easily if and when errors do occur. The system should provide appropriate feedback, display current status and should be accessible at all times.

While security is another overarching and important goal, users might take it for granted or consider it coming in the way of their actual goals. So, when usability and security intersect there are additional considerations and methods for usability evaluation [38–40]. Saltzer proposes design principles for data protection among which the following seem relevant for when intersected with usability: *"economy of mechanism"* where the design is to be as simple and small as possible; *"fail-safe defaults"* and *"psychological acceptability"*.

Whitten defines security software as usable, through four points as follows:

"Security software is usable if the people who are expected to use it:

1. are reliably made aware of the security tasks they need to perform;

2. are able to figure out how to successfully perform those tasks;

3. don't make dangerous errors; and

4. are sufficiently comfortable with the interface to continue using it." [40]

Whitten describes properties of security which make it difficult to get user interfaces right or usable, such as: *"unmotivated user"*, *"abstraction"*, *"lack of feedback"*, *"barn door principle"*, and *"weakest link"*. The *unmotivated user* property highlights that security is not the primary goal of the user. Instead, the user wants to achieve other tasks, and would easily not give much thought to security, assuming that they are safe. *Abstraction* refers to abstracted security rules for granting access which may not seem intuitive to most users. The *lack of feedback* property speaks about how it is difficult for security software to perform useful error checking and provide feedback that the user wants. The *barn door property* refers to leaving secrets accidently open, after which one can never be sure if any attacker might have accessed it or not. *The weakest link property* refers to security being strongest as the weakest component, which can be exploited by attackers. User interfaces for security places priority on ensuring that users understand security well enough, and they should be guided through all aspects [40].

We have considered these dimensions of usability and security as per Joshi et al. [36, 37], Whitten [39, 40] and Saltzer [38] in our analysis and discussion of our findings.

3 Method

The objective of this study was to gain insights into how total-blind [13] users used touchscreen-based smartphones, with a focus on privacy and information security issues they faced, their coping strategies and practices, and their conceptual models.

We interviewed 51 total blind smartphone users in Mumbai, India, using a Contextual Inquiry (CI) [41] approach. We chose to interview total blind and not users with other forms of visual impairments to have a homogenous group of users, assisting our analysis of responses and cause of their behavior and practices. The users were in the age group of 18 to 40 (averaging around 25 years). There were 36 male and 15 female participants. More detail about the participants is provided in the table 1 below.

Table 1. Particpants details

	Female	**Male**	**All**
Number of participants	15	36	**51**
Average Age	25	25	**25**
18 to 20 years	3	8	**11**
21 to 25 years	6	16	**22**
26 to 30 years	4	7	**11**
31 to 35 years	2	3	**5**
36 to 40 years	0	2	**2**
Number of Android Users	12	32	**44**
Number of iPhone Users	3	4	**7**
Number of Employed participants	9	13	**22**
Students	5	22	**27**
Unemployed	1	1	**2**

A group of researchers individually visited users at their homes, colleges or workplaces, across Mumbai. The CI method recommends visiting the users in their context. The researchers first briefed the users about the study, sought consent and proceeded with the interview. The researchers simultaneously also noted observations about the user and their immediate environment. The researchers gathered basic information from the users such as their demographic details, phone models and prior experience with smartphones, and then gradually proceeded towards asking contextual questions focusing on their security practices with the smartphone. The interviews had a conversational format and the researchers played the role of an 'apprentice', where the user would demonstrate how they used certain security related features on their phones with as much detail as possible (e.g., how they set a phone lock, or how they unlocked their phone). The users were also nudged to retrospectively recite various security related

situations they might have been in, and were probed to provide details. As far as possible, the researchers avoided speculative situations and relied on past situations which the user actually had been in.

The interviews primarily dwelled on the usability and security related practices and challenges blind users faced in their daily lives – i.e. beliefs, practices and challenges they faced with using the locking mechanisms, with setting locks, managing Privacy, and setting, managing and using Passwords for their online accounts and apps.

The interviews were recorded using voice recorders, and later transcribed where local language were not translated. The interviews were discussed for arriving at structured notes. The researchers read and familiarized themselves with the interview transcripts, photos and videos, and shortlisted notes that were particularly related to the focus on Smartphone Usability and Security for blind users. The notes were printed as paper chits which were shuffled around in a box. Researchers picked a chit from the box, read it out aloud or passed it around. From a discussion that ensued the researchers arrived at a consensus about a model explaining the observation in the note, and noted down the model on a Post-It™ note. The Post-It™ note was put on a table with the chit below it. The researchers continued picking up chits from the box, and arrived at more models or updated existing models on the table, till clusters and categories formed.

Once all notes were categorized, the researchers then identified key categories which had a larger number of chits and seemed highly relevant to our focus, or were novel. The researchers read through the chits one by one under that category and tried explaining it through a model which was written or sketched on Post-It™ notes on a wall. With every chit we either reclassified it with other categories on the table if appropriate or updated the model on the wall till a good understanding of observed phenomena emerged and was captured through models on the wall.

To illustrate with an example: We clustered notes with observations such as how users used Talkback at low volumes, or at very fast rates, or strategies such as touching additional ‘fake’ characters while entering passwords to confuse eavesdroppers. These observations led us to arrive at models such as ‘Obscurity is used as a means to achieve privacy’. Such models after subsequent structuring, also developed into a primary category – ‘Assistive software is used as a layer of security’, which we discuss later in section 4.3. In this way most of the categories and chits on the table were analyzed till we arrived at the most novel or relevant themes, in the views of the researchers, as described in the following sections. Fig. 1 showcases the affinity diagramming.

Fig. 1. Affinity Diagramming

4 Findings

4.1 Accessibility challenges lead to predictable passwords

Users expressed that virtual keypads were more difficult to use as compared to the Symbian based tangible keypad phones that they used earlier. Tangible keypads allowed speed and accuracy in typing as it was easy to find the correct keys. With touchscreen phones however, despite accessibility software such as Talkback or Voiceover, it is a challenge to locate keys accurately without the tangible feedback. Users often face breakdowns by accidentally pressing wrong keys or activating undesired operations. For instance, text entry usually involves three taps: one for scanning and reading out the letters on the keypad followed by a double-tap to enter the last key that was spoken out (there may be other such similar techniques). This is much slower than the tangible keypads where users could find and enter the desired keys easily, simply relying on their cognitive and muscle memory of the location of the key. With phone locks, issues are amplified as the users' desire frequent and quick access to their phones, and the lock gets in the way. Hence we found users opting out of locks or using very simple-to-type PINs and Patterns.

> *"…the screen reader speaks numbers and symbols, but at times we accidently press the small button the side which changes the language… We don't understand what's happening then, and we have to re-enter the password."* – (NJ.U4.06) [1]

Our observations led us to believe that the typing difficulty on virtual keypads led users to keep passwords that are easier to type, which are also hence predictable – those which would have minimal resistance or ease of entry. We thus observe a conscious move towards predictability to lower the entry barrier, indicating that the user goals significantly outweigh behavior towards protection interventions. E.g., User AS03 (Fig. 2) demonstrated how they entered 111111 as a PIN on her iPhone. It simply required her to first scan and locate 1 (which was easy). After that they had to double tap multiple (12) times to enter six 1's, which they did quite rapidly. We thus observe that the coping mechanisms deployed by the users significantly increases risk of compromise.

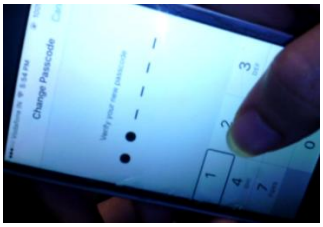
> *"It's better to keep a single digit. I've kept 1 six times."* – (AS03)

Consider an alternate example, 135743. This would require the user to scan and locate each digit followed by a double tap, which is an increase in 5 taps, slowing the user. 111111 reduces the effort required to scan, locate digits and double tap. Users may not keep PINs that require them to move all over the keypad. A similar practice was noticed with using Patterns, where they resorted to starting at edges and preferring straight lines (L's) or squares.

[1] Note: All quotes are translated into English from Marathi and Hindi, for international readers.

"One sleeping line goes over 3 points and one standing line goes over 2 points. I felt this is possible for blind people. I tried a lot, to at least make one sleeping line…on my phone as well on others, but I couldn't figure it out. There are just 3 sleeping lines, but it is difficult. If there was only one sleeping line, then it could help blind people." – (SKU412)

Fig. 2. User sets a PIN using a single digit



It appears that users focus on ease and speed of input for passwords and locking mechanisms, rather than recallability or non-guessability, when using touchscreen devices. If users perceive access control measures as reducing productivity, they deploy weaker protection measures which are predictable based on ease of entry. A related observation about predictability of passwords, was that users kept simple and recallable passwords based on their daily personal contextual data, or rather based on their 'sign-up' information. By this we mean that passwords were combinations of details such phone numbers, account numbers, names of friends, family or places, or names of favourite movies and games, or related to religion or beliefs (such as names of gods, or lucky numbers). This is not very different from what one would expect with sighted users' passwords. The users however did demonstrate attempts to mix and combine names, numbers and characters to try keeping the passwords non-guessable.

"For Facebook, I've kept my password close to my name. In Gmail I have tweaked my phone number a little here and there. So that I don't forget." – (BBU215)

The other specific finding about password choices with blind users was that visually impaired users have a unique code for representing letters by number codes. E.g. User DTU6 encoded their passwords using this strategy, which could be a decent technique for setting a recallable password which is non-guessable at least outside the community.

*"Actually, we speak a number language, which we call 123… I had just kept my name (as password)…in Marathi – C means Cha. We call C (Cha) as 31. So, I had kept the password like 31 ** ** 12* (masked for privacy)." – (DTU614)

Literature highlights how the keyboard layouts and small form-factor of mobiles affect influence password choices [42, 43]. Our observations suggests that accessibility of the touchscreen interfaces also affects the password choices both in case on PINs as well as Patterns.

4.2 Migration across locking mechanisms – No lock to TouchID

Fig. 3 below highlights how we interpreted users' transition across various locking mechanisms, based on three dimensions – security, usability and accessibility. Users tend to start out with no phone locks when the phone is new, and might use the Swipe/Slide Lock or simply the power button to start the screen. Users commonly stated that there is nothing valuable on their phones to justify the absence of locks. They felt locks prevented hassle-free frequent access to their phones. They also feared getting locked out of their phones, in case they forgot the password. One user also believed that passwords would slow down the phone. Some users stated that they did not know how to or had not yet 'learnt' how to set the phone locks and might do so at some later point in time. Some users reported that in case of emergencies, others should be able to use and unlock their phones. They stick to the adopted mechanism (beginning with no-lock as in Fig. 3) till a trigger makes them change and adopt locks. These triggers are either from the dimension of security, usability or accessibility issues. The security trigger is usually an exposure to a risk situation where they may have lost data, faced privacy issues, etc. This prompts users to start employing a security measure, usually a PIN lock. Other reasons could be merely out of curiosity, e.g. trying out Patterns as it appears as an interesting challenge to blind users. Once they have adopted a security measure, again users would stick to it till they feel inconvenienced by usability or accessibility challenges with the mechanism, prompting them to try out other mechanisms or revert to no locks (or easier mechanisms like PINs). In case of biometric fingerprint based locks (Touch-ID on iPhones), we felt users did not revert to other mechanisms. (We did not observe users of biometric fingerprint locks on Android phones). This migration might take place till users find a good enough balance between accessibility, usability and security.

> *"…Once, a family member met with a bike accident. Their phone was locked completely. No one was able to call the family members as the app lock couldn't be unlocked. That's one reason* (for not keeping a lock.)" – (BBU716)

Users seem to need a strong trigger to begin using phone locks. These are often cases of thefts, shoulder surfing and being unable to assess if anyone is watching their screens, or sensitive information/applications such as net banking installed on the phone. Similar triggers also led users to change their current PINs (or passwords). Users explored the various security phone locking options and usually settled on PINs stating that numbers are easy and less tedious compared to Passwords or Patterns. Patterns were treated as impossible to understand for blind users. iPhone users however loved the biometric fingerprint option – TouchID.

> *"I had a friend sitting near me, who saw me opening my phone lock. She asked me for my password. I refused, but she was insistent. Then she said she knows my password. I told her to open my phone then if she could. She unlocked it! She was partially (blind) so she could see. I immediately changed the password."* – (RCU4)

Some users either preferred PINs over Patterns or Patterns over Pins due to perceptions about how they performed on speed and ease, especially during situations/context where the mechanism were difficult to use – such as being sleepy or travelling in public transport where the rides are bumpy.

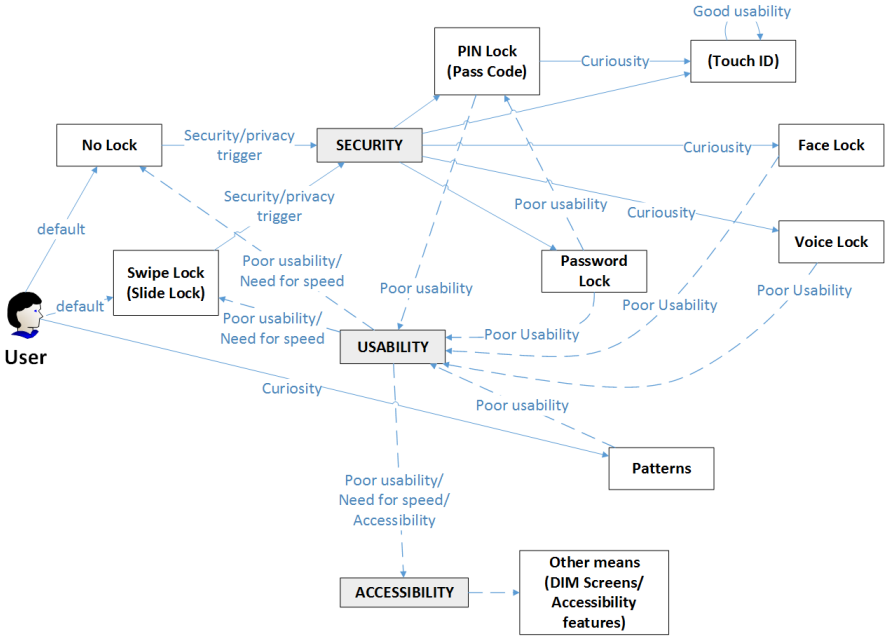
> *"The problem with PIN was you had to double touch every time. I had kept mine (password) as 1234. So you have to type double 1, double 2 double 3, double 4 due to talkback. Talkback requires double touch. Sometimes when I'm on the road, I face difficulties. Then I changed to a Pattern. Since then my problems have reduced, because with this I can open my phone quickly."* – (BBU210)

iPhone users found the fingerprint biometric authentication – Touch-ID, as a very convenient option, despite occasional issues faced in fingerprint recognition. Users who used Touch-ID would not migrate back to no locks. They felt comfort with the presence of a fallback of a PIN when fingerprint recognition failed, so they did not have the fear of getting locked out of the phone. Most other (Android) users either used PINs or reverted to the swipe lock, or no lock or interestingly used accessibility features, such as Dim-Screen as a layer of security (discussed in the next section).

> *"Basically I use TouchID. I also have Passcode in place. The TouchID has a good biometric sensor, it works most of the time. When it doesn't, then I use Passcode. I believe TouchID is the best, you know you need to place the thumb."* – (BBU105)

Existing studies [6, 16, 44] have found that most users (sighted) use locks for security and privacy, with PINs being prevalent. For those who do not use locks, it is usually due to a lack of motivation, lack of concern or inconvenience. Users tend to start using locks when prompted to (usually by a significant other) and would then stick to using the lock, despite inconveniences faced. Users seem to face more errors with Patterns, compared to PINS. Azenkot in an earlier study with visually impaired users found all their participants avoided lock, which is not the case in our study, but those who did not use locks claimed similar reasons of not knowing about it or inconveniences faced. Similarly, the use of Screen Curtain instead of a lock was prevalent in our study too. Users in our study however claimed avoiding headphones in public, contrary to Azenkot's observation. While the studies have discussed users' motivations to use locks, their choices of pass-codes, and also compared common options such as PINS, Patterns and Biometrics, further investigation of how people choose and migrate between various forms of locks might yield interesting insights, especially concerning usability and accessibility of the interfaces with visually impaired users.

Fig. 3. Migration across phone locking mechanisms



4.3 Assistive software as a layer of security

Users may not always find the existing accessibility features on their phone to effectively use the locking and security mechanisms effectively. For instance, the screen readers read the passwords aloud while entering passwords. There are settings where users can disable the screed reader from reading the passwords, but then they do not know what they are typing. This leaves them with the option of using headphones which is not suitable for frequent unlocking, and hence is a discomfort. Users also feel headphones are unsafe to use constantly as they depend on their aural senses for their activities. Users face issues of accuracy and speed with using the unlocking mechanisms as discussed in section 4.1. Users tend to deal with these situations by doing away with phone locks altogether, or entering the code at low volume without headphones.

> *"A long time back I had tried passcode, but it used to just say dot-dot when I would enter any number. I could not know what number was pressed. That's why I never set anything for screen lock."* – (ASU501)

Instead of depending on the locking mechanisms alone, users seem to also use the assistive features as an additional layer for security. For instance, when users are unable to assess if anyone is eavesdropping, then tend to obscure or hide their activity using physical means, i.e. holding the phone in a particular way or covering the screen with their hand. Another interesting way of obscuring was using the accessibility options on

the phone, i.e. the Dim Screen or Screen Curtain option, or the screen reader set at a very fast speaking rate. With the Dim Screen option, the screen is totally turned off while operating so others are unable to see the screen. Hence users also went to the extent of not using a phone lock, as they felt Dim Screen was sufficient protection from snoopers.

> *"I use a feature present in TalkBack, called Dim Screen, so I don't need to keep any password. Nobody can see anything. Because of this feature I do not require any screen security for my phone."* – (NSU215,16)

Again, the screen reader and other alternate gestures that they used when the phone is in accessibility mode were considered difficult for others, mainly sighted users. Hence they felt their phones were safe from others. They felt other users need to be skilled to use the phone with the accessibility mode on. They also kept the speech rate very high, making the speech indiscernible by others. This was another form of obscurity protecting their privacy in public. In the case where the screen readers speak the password/pin aloud, one user intentionally scanned over random keys while entering the password, thus obscuring the actual password. Although not fool proof, an untrained listener would find it difficult to understand which keys were merely scanned and which were actually entered.

> *"If I don't want people to know what my PIN is, I create a false PIN by touching extra numbers. If I don't release the touched numbers, they are not entered. So people do not know what PIN I entered. Generally, I keep in mind that when I enter my PIN, I hold my phone closer to me so that nobody can see anything. Even you didn't get my PIN, did you?"* – (BBU108)

In some cases users felt that keeping the screen reader at a very loud is useful, especially when the phone is not on their person. This allowed them to notice if somebody started interfering with their phone.

However, it is apparent that these approaches of depending on accessibility features for obscurity for privacy and protection is limited. It only protects them from sighted and untrained users. As the phone security features are not amenable out-of-the-box to the blind users, the users have coped up by using assistive features in interesting ways. We feel that it might be interesting and useful if designers could explore this further and consider enhancing assistive features for security and privacy too. While studies have highlighted the use of Screen Curtain for privacy [6], the phenomenon and opportunity of adapting assistive software of smartphones of security and privacy would be interesting to explore further.

4.4 Patterns – a maze

Most users felt Patterns are impossible for them to use as they cannot understand them. They face difficulty in locating the dots and connecting them by gestures (lines). Patterns are not accessible enough although there are soft buzzes when the user touches

the dots. The screen reader also provides a few instructions, but are mostly not helpful enough. Some users had explored patterns but did not adopt them as were unable to use them, despite feeling that Patterns could be faster to use than PINS. We feel users found it challenging to build a mental model of Patterns. It was also a new mechanism which was not available on earlier tangible phones.

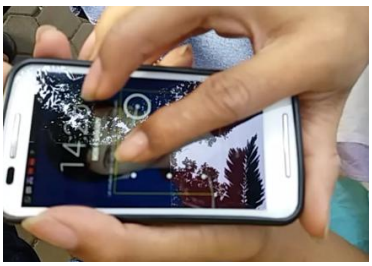
> *"It would just speak 'Pattern Area'. I would draw the wrong pattern. The phone would never unlock. I had to take somebody else's help. So, I stopped using patterns."* – (SKU409)

We found a couple of users who used patterns easily. We observed that user BBU2 had developed a strategy to locate the first dot, after which they could locate the rest and reach a speed similar to sighted users in unlocking the phone. The user held the phone in a unique way with the thumb and fingers positioned possibly to locate the first dot accurately, i.e. on the right top edge of the pattern grid (Fig. 4). However, we noticed that the few users who used Patterns appeared to use quite predictable patterns to enable accurate and quick access. The tendency was to start at edges, as they needed an anchoring point. They relied on straight paths and avoided diagonals, to avoid accidentally touching the wrong dots. This resulted in simple shapes – 'sleeping lines' or L's, and squares (a C) on the 3x3 grid. Similar to the concerns people had with PINS, users also found using Patterns accurately in certain situations where attention is difficult (e.g. sleepy or travelling).

> *"…I would want to connect four dots only. I don't want to connect more. So, I'm telling you that I would keep an L or Square."* – (BBU215)

Despite its apparent difficulty, Patterns could be widely adopted by blind users if the accessibility was improved. Example, it should be easier to locate and anchor to the starting dot in the pattern. E.g. Buzzi et al. have discussed approaches how visually challenges users can orient themselves on touchscreens more easily [45, 46]. Otherwise, for most users the Patterns is currently a maze – they need to be really motivated to attempt to understand and develop a strategy to find their way through.

Fig. 4. User using a Pattern lock accurately identifying the dots



Existing studies [47–49] are inconclusive about preferences of Patterns over PINs. Patterns seem to have a higher rate of errors. Yet users tend to prefer Patterns

as they perceive better feedback, ease of use, efficiency and memorability. We were unable to find detailed studies discussing the use and accessibility of Patterns by visually impaired users. Users seem to need to orient themselves better on the screen to be able to use Patterns more effectively.

4.5 Password backups and fallback users

Users frequently seek assistance from others, usually sighted users, to set up their online accounts for email, Facebook, etc. They often require assistance as they are unfamiliar with the interface, and also find CAPTCHAs challenging. They usually seek assistance from people they consider tech-savvy – e.g. trainers as blind institutions, phone vendors, or family members. While seeking assistance, they often share personal information including passwords. Some users reported that they did not change the passwords later, as they trusted the person who helped them and expected him or her to forget about it. However, some users who appeared more tech-savvy and security paranoid did change the passwords later. Some even deleted their account and set up a new account as they were now familiar with the process.

> *"I had faced a problem with my Gmail account. I had entered username properly, but when I tried to enter password, it would speak out star-star… I didn't know what to do. Then I took a sighted person's help for logging in using email id and password"* – (ASU101)

Users face similar challenges in resetting passwords, and need assistance. To prevent forgetting passwords, especially important ones, users resort to sharing passwords with a trusted person, as a backup. This trusted person is usually a family member or a close friend, who may also sometimes assist the user with operating the account. Sharing passwords is also seen in an existing study by Singh et al. [50] an emerging trend, especially among married couples, disabled users and indigenous communities. The authors [50] also highlight principles for Design considering such a phenomenon.

> *"My friend knows my password because he needs it to fill some forms for me. He is the only person who knows my password."* – (RSU412)

They also resort to keeping the password written down in a diary at home or in a password-protected file on their laptop. Users also maintained a list of passwords that they cycled through across various accounts. Other users however relied on using the "forgot password" option to reset the password instead of taking measures to remember, store or share passwords. Some used drastic measures such as creating a new account, rather than attempting recovery. Similar reactions are reported in a study with less-literate users [51].

The motivation to share or store passwords seems to stem from the difficulty faced in recalling passwords as well as in resetting their passwords. The passwords that were shared or backed up were usually those that were important and infrequently used (e.g. those related to the college/university or banking).

"My university password… I've written it in 2-3 places. It is written on my mobile, at home, and on my wall calendar as well." – (RSU714)

Table 2 provides a summary of number of notes considered supporting the themes that emerged.

Table 2. Key themes and supporting notes considered

Key themes	Supporting notes considered
Accessibility challenges lead to predictable passwords	82
Migration across locking mechanisms	97
Assistive software as a layer of security	42
Patterns – a maze	27
Password backups and fallback users	34

5 Discussion and Design Recommendations

We assessed our findings using the framework of UGT [36, 37] to define the users' usability goals and also considered usable security related aspects from Whitten [39] and Saltzer [38]. We considered the usability and security goals for blind smartphone users as 1) being able to protect their data and privacy using the security mechanisms on their phone appropriately, 2) being able to protect their online accounts with good password practices supported by the phone interfaces.

Users tend to find existing phone locking mechanisms error-prone due to lack of tangibility and ineffective feedback, affecting accuracy, speed and ease of use. Although users are often motivated to learn the locking mechanisms, apparent from how they have explored the various options, they often find it difficult to understand the mechanisms and are not comfortable with the interfaces. Users also face barriers in locating and learning the settings for setting up the locks, especially without assistance from sighted users. This activity of setting a lock is infrequent, and being unfamiliar with the interface, users tend to have a certain amount of fear to set up locks. Frequent errors while using the locks also lead to the fear of getting locked out of their own phone (*'dangerous errors'*). Tapping on areas accidentally also messes up the interaction (*Economy of mechanism'* and *'Psychological acceptability'*). Hence, users either opt to not using locks at all, or adopt very simplistic predictable passwords (*'unmotivated user'*). Additionally they adopt accessibility features as means to obscure and protect privacy. Accessibility concerns seem to be the key issue that affects secure adoption of phone locks by blind users. Improved accessibility and biometric approaches could improve adoption. Among the locking mechanisms available, finger print recognition seems to have the best *'economy of mechanism'* and *'psychological acceptability'*. However, it can be argued that biometric authentication still needs to evolve for better security [52]. Patterns is another promising quick approach, if accessibility could be

improved. Poor accessibility also leads the user to take assistance from others – blind and sighted (*'weakest link'*, *'barn door'*). They even write and sharing their passwords or accounts, leaving themselves exposed and vulnerable to attacks. Hence, improving the accessibility of especially of security features is of prime importance.

We also found that the users have an attitude of continual learning and have a close-knit community among themselves. They are informed about good practices and share tips among themselves via workshops conducted by organizations for blind or via WhatsApp and other online communities. As users seem open to technology and share information and good practices, we feel quick dissemination of security solutions and awareness is possible. Being tech savvy and explorative, alternative interfaces could be explored which might be usable and effective to visually impaired users. Researchers such as Kane, Leporini, Buzzi, Azenkot and Guerreiro have discussed novel approaches for usable and accessible interfaces on smartphones [46, 53–58].

A primary challenge with visually impaired users using touchscreen smartphone interfaces is the lack of tangibility and visual cues. Sighted users usually rely on subtle or direct visual cues while interacting with user interfaces. This channel is blocked out for blind users. Instead they depend on the audio channel, which is either missing or minimal, and is usually incidental and not specifically designed for accessibility. At the most there is minimal haptic feedback through buzzes, and the screen reader but does not provide a sense of a user interface that visual cues do. In current interfaces, there seems to be little or no mapping or information redundancy between the visual and audio channels. A transfer of feedback from the visual to an aural and tangible channel is required for appropriate feedback as recommended for usability of the interfaces. Users could then subconsciously process information while interacting with the interface. Such interfaces could be translated to have a parallel aural and haptic interface. For instance a Morse-like code which vibrates privately in the hand. Vibration and aural standards could be defined as alternatives to visual interfaces, over and above screen reader which are essentially text to speech. For example, some existing studies investigate providing prosodic cues with screen readers [59, 60].

Accessible security interfaces should focus on achieving better speed and ease-of-use. Occasionally used screens such as Settings or Account creation should be accessible enough to avoid assistance from sighted users – or at least designed to allow mediation and assistance but maintaining privacy of the users wherever required.

New accessible phone locks can be explored – again focusing on ease and speed of use for visually impaired or eyes-free access. For existing phone locks, fallbacks could be introduced: e.g. Touch-ID to PIN. Instead of locking out phones after unsuccessful attempts to unlock the phones (caused by errors in input), users could be given a secondary lock interface. Anchoring points could be developed or overlaid on touch screens (as in the mark on the '5'-key on earlier phones) which could assist users to orient and anchor themselves to use visual/spatial interfaces such as PINS. There is scope for the pattern locks to be improved for accessibility. Potentially, there are a lot of cues from the earlier tangible Symbian phones, and how blind users used them, which could transition into the newer touchscreen smartphones.

Users currently use the accessibility settings for privacy, such as a rapidly speaking screen reader or dim screen. The accessibility features could be enhanced to embrace

this behaviour, and designed for better obscurity, allowing privacy from blind and sighted users alike.

6 Conclusions

We believe that the area of security interventions for smartphones in the context of usability can be better aligned. Users face constant difficulties due to accessibility shortcomings. This affects their productivity and they opt out of using locking mechanisms. They cope up by appropriating the assistive features as obscurity for privacy. Improvement in the accessible phone locks, password recovery and account creation, could vastly assist them being independent and secure.

Acknowledgments. We thank all the users, volunteers, and all publication support and staff, especially the reviewers who wrote and provided helpful comments on versions of this document. We thank Interact for supporting and improving our paper through its shepherding process.

References

1. India Ericsson Mobility Report June 2016, https://www.ericsson.com/assets/local/mobility-report/documents/2016/india-ericsson-mobility-report-june-2016.pdf.
2. Irvine, D., Zemke, A., Pusateri, G., Gerlach, L., Chun, R., Jay, W.M.: Tablet and Smartphone Accessibility Features in the Low Vision Rehabilitation. Neuro-Ophthalmol. 38, 53 (2014).
3. Kim, H.K., Han, S.H., Park, J., Park, J.: The interaction experiences of visually impaired people with assistive technology: A case study of smartphones. Int. J. Ind. Ergon. 55, 22–33 (2016).
4. Robinson, J.L., Avery, V.B., Chun, R., Pusateri, G., Jay, W.M.: Usage of Accessibility Options for the iPhone and iPad in a Visually Impaired Population. Semin. Ophthalmol. 32, 163–171 (2017).
5. Abdolrahmani, A., Kuber, R., Hurst, A.: An Empirical Investigation of the Situationally-induced Impairments Experienced by Blind Mobile Device Users. In: Proceedings of the 13th Web for All Conference. p. 21:1–21:8. ACM, New York, NY, USA (2016).
6. Azenkot, S., Rector, K., Ladner, R., Wobbrock, J.: PassChords: Secure Multi-touch Authentication for Blind People. In: Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility. pp. 159–166. ACM, New York, NY, USA (2012).
7. Kane, S.K., Jayant, C., Wobbrock, J.O., Ladner, R.E.: Freedom to roam: a study of mobile device adoption and accessibility for people with visual and motor disabilities. In: Proceedings of the 11th international ACM SIGACCESS conference on Computers and accessibility. pp. 115–122. ACM (2009).

8. Chiti, S., Leporini, B.: Accessibility of Android-Based Mobile Devices: A Prototype to Investigate Interaction with Blind Users. In: Proceedings of the 13th international conference on Computers Helping People with Special Needs - Volume Part II. pp. 607–614. Springer Berlin Heidelberg (2012).
9. Leporini, B., Buzzi, M.C., Buzzi, M.: Interacting with mobile devices via VoiceOver: usability and accessibility issues. In: Proceedings of the 24th Australian Computer-Human Interaction Conference. pp. 339–348. ACM (2012).
10. WHO: Global Data on Visual Impairments 2010, http://www.who.int/blindness/GLOBALDATAFINALforweb.pdf.
11. Office of the Registrar General & Census Commissioner, India: CENSUS OF INDIA 2011 DATA ON DISABILITY, http://www.languageinindia.com/jan2014/disabilityinindia2011data.pdf.
12. IDA - India: Cataract Blindness Control Project, http://web.worldbank.org/WBSITE/EXTERNAL/EXTABOUTUS/IDA/0,,contentMDK:21917842~menuPK:4752068~pagePK:51236175~piPK:437394~theSitePK:73154,00.html.
13. Key Definitions of Statistical Terms - American Foundation for the Blind, http://www.afb.org/info/blindness-statistics/key-definitions-of-statistical-terms/25.
14. Data on Disability, Disabled Population by type of Disability, Age and Sex - C20 Table (India & States/UTs - District Level), http://www.censusindia.gov.in/2011census/Disability_Data/India/C_20-India.xls.
15. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measuring user confidence in smartphone security and privacy. In: Proceedings of the Eighth Symposium on Usable Privacy and Security. p. 1. ACM (2012).
16. Egelman, S., Jain, S., Portnoff, R.S., Liao, K., Consolvo, S., Wagner, D.: Are You Ready to Lock? In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 750–761. ACM Press (2014).
17. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: User attention, comprehension, and behavior. In: Proceedings of the Eighth Symposium on Usable Privacy and Security. p. 3. ACM (2012).
18. Inan, F.A., Namin, A.S., Pogrund, R.L., Jones, K.S.: Internet Use and Cybersecurity Concerns of Individuals with Visual Impairments. J. Educ. Technol. Soc. 19, 28–40 (2016).
19. Karlson, A.K., Brush, A.J., Schechter, S.: Can i borrow your phone?: understanding concerns when sharing mobile phones. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 1647–1650. ACM (2009).
20. Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., Beznosov, K.: Understanding users' requirements for data protection in smartphones. In: Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on. pp. 228–235. IEEE (2012).
21. Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., Beznosov, K.: Know your enemy: the risk of unauthorized access in smartphones by insiders. In: Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services. pp. 271–280. ACM (2013).

22. Mylonas, A., Kastania, A., Gritzalis, D.: Delegate the smartphone user? Security awareness in smartphone platforms. Comput. Secur. 34, 47–66 (2013).
23. Tchakounté, F., Dayang, P., Nlong, J., Check, N.: Understanding of the Behaviour of Android Smartphone Users in Cameroon: Application of the Security. Open J. Inf. Secur. Appl. 2014, 9–20 (2014).
24. Ahmed, T., Hoyle, R., Connelly, K., Crandall, D., Kapadia, A.: Privacy concerns and behaviors of people with visual impairments. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. pp. 3523–3532. ACM (2015).
25. Ashraf, A., Raza, A.: Usability Issues of Smart Phone Applications: For Visually Challenged People. World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng. 8, 760–767 (2014).
26. Dosono, B., Hayes, J., Wang, Y.: "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). pp. 151–168 (2015).
27. Asokan, N., Kuo, C.: Usable mobile security. In: Proceedings of the 8th international conference on Distributed Computing and Internet Technology. pp. 1–6. Springer-Verlag (2012).
28. Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., Möller, S.: On the need for different security methods on mobile phones. In: Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services. pp. 465–473. ACM (2011).
29. Jakobsson, M.: Why mobile security is not like traditional security. (2011).
30. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android Permissions: User Attention, Comprehension, and Behavior. In: Proceedings of the Eighth Symposium on Usable Privacy and Security. p. 3:1–3:14. ACM, New York, NY, USA (2012).
31. Chen, J., Paik, M., McCabe, K.: Exploring Internet Security Perceptions and Practices in Urban Ghana. In: SOUPS. pp. 129–142 (2014).
32. Alsaleh, M., Alomar, N., Alarifi, A.: Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. PLOS ONE. 12, e0173284 (2017).
33. Bevan, N., Carter, J., Harker, S.: ISO 9241-11 revised: What have we learnt about usability since 1998? In: International Conference on Human-Computer Interaction. pp. 143–151. Springer (2015).
34. ISO/DIS 9241-11.2(en), Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts, https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:dis:ed-2:v2:en.
35. 10 Heuristics for User Interface Design: Article by Jakob Nielsen, https://www.nngroup.com/articles/ten-usability-heuristics/.
36. Joshi, A.: Usability goals setting tool. In: 4th Workshop on Software and Usability Engineering Cross-Pollination: Usability Evaluation of Advanced Interfaces, Uppsala (2009).

37. Joshi, A., Sarda, N.L.: Do Teams Achieve Usability Goals? Evaluating Goal Achievement with Usability Goals Setting Tool. In: Human-Computer Interaction – INTERACT 2011. pp. 313–330. Springer, Berlin, Heidelberg (2011).
38. Saltzer, J.H., Schroeder, M.D.: The protection of information in computer systems. Proc. IEEE. 63, 1278–1308 (1975).
39. Whitten, A.: Making security usable, http://reports-archive.adm.cs.cmu.edu/anon/anon/usr/ftp/usr0/ftp/2004/CMU-CS-04-135.pdf, (2004).
40. Whitten, A., Tygar, J.D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8 (1999).
41. Beyer, H., Holtzblatt, K.: Contextual design: defining customer-centered systems. Morgan Kaufmann Publishers Inc. (1998).
42. Genco, E., Kelley, R., Vernon, C., Aviv, A.J.: Alternative Keyboard Layouts for Improved Password Entry and Creation on Mobile Devices. Presented at the Eleventh Symposium On Usable Privacy and Security.
43. von Zezschwitz, E., De Luca, A., Hussmann, H.: Honey, I shrunk the keys: influences of mobile devices on password composition and authentication performance. In: Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational. pp. 461–470. ACM (2014).
44. Harbach, M., De Luca, A., Egelman, S.: The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. pp. 4806–4817. ACM Press (2016).
45. Buzzi, M.C., Buzzi, M., Leporini, B., Paratore, M.T.: Vibro-tactile enrichment improves blind user interaction with mobile touchscreens. In: IFIP Conference on Human-Computer Interaction. pp. 641–648. Springer (2013).
46. Buzzi, M.C., Buzzi, M., Donini, F., Leporini, B., Paratore, M.T.: Haptic Reference Cues to Support the Exploration of Touchscreen Mobile Devices by Blind Users. In: Proceedings of the Biannual Conference of the Italian Chapter of SIGCHI. p. 28:1–28:8. ACM, New York, NY, USA (2013).
47. Andriotis, P., Tryfonas, T., Oikonomou, G., Yildiz, C.: A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In: Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks. pp. 1–6. ACM (2013).
48. Loge, M., Duermuth, M., Rostad, L.: On User Choice for Android Unlock Patterns. In: 1st European Workshop on Usable Security (EuroUSEC) 2016 (2016).
49. von Zezschwitz, E., Dunphy, P., De Luca, A.: Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In: Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services. p. 261. ACM Press (2013).
50. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., Furlong, M.: Password Sharing: Implications for Security Design Based on Social Practice. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 895–904. ACM, New York, NY, USA (2007).

51. Doke, P., Lobo, S., Joshi, A., Aggarwal, N., Paul, V., Mevada, V., Kr, A.: A User Study About Security Practices of Less-Literate Smartphone Users. In: 8th International Conference on Intelligent Human Computer Interaction. pp. 209–216. Springer, Cham (2016).
52. Boult, T.E., Scheirer, W.J., Woodworth, R.: Revocable fingerprint biotokens: accuracy and security analysis. In: 2007 IEEE Conference on Computer Vision and Pattern Recognition. pp. 1–8 (2007).
53. Azenkot, S., Wobbrock, J.O., Prasain, S., Ladner, R.E.: Input finger detection for nonvisual touch screen text entry in Perkinput. In: Proceedings of Graphics Interface 2012. pp. 121–129. Canadian Information Processing Society (2012).
54. Buzzi, M.C., Buzzi, M., Leporini, B., Senette, C.: Playing with geometry: a Multimodal Android App for Blind Children. In: Proceedings of the 11th Biannual Conference on Italian SIGCHI Chapter. pp. 134–137. ACM (2015).
55. Buzzi, M.C., Buzzi, M., Leporini, B., Trujillo, A.: Designing a text entry multimodal keypad for blind users of touchscreen mobile phones. In: Proceedings of the 16th international ACM SIGACCESS conference on Computers & accessibility. pp. 131–136. ACM (2014).
56. Guerreiro, T., Nicolau, H., Jorge, J.A.: From tapping to touching: Making touch screens accessible to blind users. IEEE Multimed. 15, 48–50 (2008).
57. Kane, S.K., Bigham, J.P., Wobbrock, J.O.: Slide Rule: Making Mobile Touch Screens Accessible to Blind People Using Multi-touch Interaction Techniques. In: Proceedings of the 10th International ACM SIGACCESS Conference on Computers and Accessibility. pp. 73–80. ACM, New York, NY, USA (2008).
58. Kane, S.K., Morris, M.R., Perkins, A.Z., Wigdor, D., Ladner, R.E., Wobbrock, J.O.: Access Overlays: Improving Non-visual Access to Large Touch Screens for Blind Users. In: Proceedings of the 24th Annual ACM Symposium on User Interface Software and Technology. pp. 273–282. ACM, New York, NY, USA (2011).
59. Murphy, E., Bates, E., Fitzpatrick, D.: Designing auditory cues to enhance spoken mathematics for visually impaired users. In: Proceedings of the 12th international ACM SIGACCESS conference on Computers and accessibility. pp. 75–82. ACM (2010).
60. Pitt, I.J., Edwards, A.D.: Improving the usability of speech-based interfaces for blind users. In: Proceedings of the second annual ACM conference on Assistive technologies. pp. 124–130. ACM (1996).