Is Implicit Authentication on Smartphones Really Popular? On Android Users' Perception of "*Smart Lock for Android*"

Masoud Mehrabi Koushki
The University of British Columbia
Vancouver, Canada
mehrabi@ece.ubc.ca

Borke Obada-Obieh
The University of British Columbia
Vancouver, Canada
borke@ece.ubc.ca

Jun Ho Huh
Samsung Research
Seoul, Republic of Korea
junho.huh@samsung.com

Konstantin Beznosov
The University of British Columbia
Vancouver, Canada
beznosov@ece.ubc.ca

ABSTRACT

Implicit authentication (IA) on smartphones has gained a lot of attention from the research community over the past decade. IA leverages behavioral and contextual data to identify users without requiring explicit input, and thus can alleviate the burden of smartphone unlocking. The reported studies on users' perception of IA have painted a very positive picture, showing that more than 60% of their respective participants are interested in adopting IA, should it become available on their devices. These studies, however, have all been done either in lab environments, or with low- to medium-fidelity prototypes, which limits their generalizability and ecological validity. Therefore, the question of "how would smartphone users perceive a commercialized IA scheme in a realistic setting?" remains unanswered. To bridge this knowledge gap, we report on the findings of our qualitative user study (N = 26) and our online survey (N = 343) to understand how Android users perceive Smart Lock (SL). SL is the first and currently only widely-deployed IA scheme for smartphones. We found that SL is not a widely adopted technology, even among those who have an SL-enabled phone and are aware of the existence of the feature. Conversely, we found unclear usefulness, and perceived lack of security, among others, to be major adoption barriers that caused the SL adoption rate to be as low as 13%. To provide a theoretical framework for explaining SL adoption, we propose an extended version of the technology acceptance model (TAM), called SL-TAM, which sheds light on the importance of factors such as perceived security and utility on SL adoption.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**; **User studies**; *Usability testing*; • **Security and privacy → Usability in security and privacy**.

KEYWORDS

implicit authentication; user perceptions; smart lock; android; user survey; cognitive walkthrough with users

ACM Reference Format:
Masoud Mehrabi Koushki, Borke Obada-Obieh, Jun Ho Huh, and Konstantin Beznosov. 2020. Is Implicit Authentication on Smartphones Really Popular? On Android Users' Perception of "*Smart Lock for Android*". In *22nd International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '20), October 5–8, 2020, Oldenburg, Germany*. ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3379503.3403544

1 INTRODUCTION

The burden of unlocking smartphones has left millions of devices unsecured. Studies have shown that on average, smartphone users unlock their devices over 30 times a day [32, 39], and each unlocking attempt requires an action from the user, which takes 2-3 seconds [32] to perform. Users find this experience too cumbersome. These efforts increase the cognitive and physical overhead of using devices, creating incentives for users to weaken, or even disable, authentication [22, 40]. Consequently, various studies have shown that more than 40% of smartphone users do not use any authentication mechanism on their devices, and most users cite "inconvenience" as the reason [13, 21, 35].

Both the smartphone manufacturers and the research community have made efforts to address this problem. Phone makers have supplied biometric unlocking solutions, such as fingerprint scanners and face detection, on their phones to lessen the unlocking burden on users. However, such solutions have been found to suffer from usability issues [6], such as the awkwardness of holding the phone in front of one's face [11]. Alternatively, the research community has proposed schemes that leverage behavioral biometrics or contextual data to unlock smartphones [1, 9, 14, 19, 42, 44, 50] without requiring any explicit action from users. Often referred to as implicit authentication (IA), this approach is deemed promising [25, 27].

The technical aspects of IA on smartphones have been well studied [1, 9, 14, 42, 44], demonstrating several IA schemes, such as Touchalytics [15] and SilentSense [2], as both feasible and usable [25–27]. However, not much research has been conducted on studying smartphone users' perceptions of IA technologies. A few existing studies suggest that smartphone users are interested in adopting IA: more than 60% of the study participants indicated

MobileHCI '20, October 5–8, 2020, Oldenburg, Germany

ACM ISBN 978-1-4503-7516-0/20/10.
https://doi.org/10.1145/3379503.3403544

a strong interest in adopting IA [8, 27]. However, the findings of these studies have limited generalizability, as they involve mostly lab studies with low- to medium-fidelity prototypes.

This paper reports on our investigation of how Android users perceive a real-world IA solution called "Smart Lock" (SL), which is the first, and currently only, widely deployed IA solution on smartphones. We conducted a mixed-method qualitative study, composed of cognitive walkthroughs (N = 10) and think-alouds with interview sessions (N = 16). To confirm our observations from the previous two studies, we surveyed 343 participants using Amazon Mechanical Turk (MTurk). Our key observations are summarized below:

- Despite its 5-year history, Smart Lock is not a widely adopted technology. Only around 13% of SL-capable participants in our survey reported that they were using SL (an SL-capable participant is someone who knows about SL and has a phone that supports it).
- Lack of availability is not a major barrier to SL adoption for Android users. As part of the Google Play Services package, Smart Lock has been deployed on hundreds of millions of Android devices over the past 5 years. More than 91% of our survey participants were using phones that supported SL.
- Lack of awareness is not a major barrier to SL adoption either. Nearly 60% of our survey participants had some knowledge about SL before participating in our study.
- Perceived lack of utility is one of the main factors that deters potential users from adopting SL. The majority of our SL-novice participants (those who have not used SL before) indicated that they did not see enough value in adopting SL and thought that fingerprint unlocking was more convenient.
- Perceived lack of security is another deterrent for SL use. The majority of SL-novice participants were unwilling to use SL because they thought adopting SL could allow unauthorized access to their phones.

Through these findings, our work makes the following novel contributions to the field of IA:

- We provide the first empirical evidence of how smartphone users perceive commercial IA in a realistic setting. Our results suggest that SL is not widely adopted because it is not perceived to be secure or convenient.
- We provided the first technology acceptance model for reasoning about Android users' decision-making around adopting SL. The model (called SL-TAM) sheds light on several factors that affect users' intention to adopt SL.
- We uncover unexplored avenues of research for the perception and use of IA by smartphone users. Exploring these avenues can help the community gain better insight into how to design the IA user experience (UX).

The rest of this paper is structured as follows: in section 2 we provided an overview of the existing literature on IA, a brief introduction to Smart Lock for Android, and related papers on technology adoption. Section 3 presents the methodology of our studies. In section 4, we present our results and discuss their implications. In section 5 we present our SL-TAM. Section 6 discusses the limitations of our studies, and, finally, section 7 concludes our paper.

2 BACKGROUND

2.1 Implicit Authentication

Smartphone users' attitudes toward unlocking their devices have been well-studied, and research shows that users perceive unlocking to be a burden. This perception seems to be justified, as it has been estimated that 80% of short phone sessions is spent unlocking the phone [32].

Implicit authentication (IA) is a promising solution to alleviate this unlocking burden [9, 25]. This is because IA does not require explicit action from the user. There have been numerous studies examining the feasibility of various modalities for IA on smartphones. For instance, Frank et al. [15] demonstrated how a machine learning classifier could continuously authenticate users, based on the way that they interact with the touchscreen of a smartphone. Other proposed modalities (contextual or behavioural data) for IA include gait patterns [12], body movements [38], biomedical signals [36], and app usage [16].

When it comes to smartphone users' perceptions of IA, however, the existing literature is much more limited. Khan et al. [27] conducted a two-part study, consisting of lab-based experiments and a three-day field study where participants used IA on their own smartphones (for experimental control, both parts used a low-fidelity IA scheme). They reported that 81% of their participants were satisfied with the level of security that IA provided. They found that 63% of participants were interested in using IA, but 30% were not sure whether they would use it, and 7% did not want to use it. Similar work was conducted by Crawford and Renaud [8]. They asked 30 participants to complete a series of tasks on a smartphone that was protected with a pseudo-IA scheme. They found that 90% of their participants indicated that they would consider using IA on their mobile devices, should it become available. These studies, however, were either conducted in lab settings or used low- or medium-fidelity prototypes, which limits their ecological validity.[1]

2.2 Smart Lock for Android

SL is the first, and currently only, widely deployed IA scheme used on smartphones. Other commercial IA solutions for smartphones also exist, such as the UnifyID [46] or Kryptowire [29], but due to their centralized design, these schemes are not suited for smartphone unlocking. SL was first introduced during the keynote of the 2014 Google I/O conference [17]. In its essence, SL is designed to reduce the number of times users have to unlock their phones by automatically unlocking the phone (or at least keeping it unlocked) when the surrounding environment is deemed "secure." The following three implicit unlocking methods are included in Google's implementation of SL:[2]

- **On-body Detection (*BODY*)** uses several behavioral biometrics (i.e., gait and body-movement patterns) to keep the phone unlocked as long as it is in motion. It can also automatically lock the phone if no movement is detected.

[1] Ecological validity refers to the extent to which the experimental conditions of the study are representative of real tasks being done by real users in their natural environment [28].

[2] SL provides two other unlocking methods called Trusted Face (*FACE*) and Voice Match (*VOICE*) as well. These methods, however, are explicitly biometric-based unlocking methods, and, as such, are beyond the scope of our studies.)

- **Trusted Places (*PLACE*)** uses GPS and Wi-Fi signals to unlock the phone in specific locations (e.g., a user's home) automatically. It can also automatically lock the phone when the device leaves the trusted location.
- **Trusted Devices (*DEVICE*)** uses Bluetooth signals to lock and unlock the phone. Using *DEVICE*, users can designate already paired Bluetooth devices as trusted, allowing them to unlock the phone automatically when connected. This can also automatically lock the phone when it loses connection with all trusted devices.

SL is considered by Google to be an important part of Android operating system, as it is actively advertised on Android devices. For example, whenever a new Bluetooth device is paired with an SL-capable phone, a notification is shown encouraging the user to add the device as a trusted for Smart Lock. Other manufacturers may opt to either not include SL on their phones, remove some SL methods (e.g., Samsung phones do not provide *FACE*), add other methods (e.g., Wear Recognition on Huawei smartphones), or provide SL as is.

To the best of our knowledge, there are no previous studies that analyzed users' perception of SL.

2.3 Technology Acceptance

Why people accept or reject new technologies and the factors that affect their decisions have been heavily researched for decades. Numerous theories, such as the technology acceptance model (TAM) [10], diffusion of innovations theory [41], unified theory of acceptance, usage of technology [48], have been put forward to try to explain users' behavior with technology adoption. Among these theories, TAM has gained a lot of traction and has been examined, expanded, and applied to various domains, such as OpenID [43] and online shopping [49].

In the original version of TAM proposed by Davis et al. [10], two main factors are shown to affect users' attitudes toward adopting a new technology: *perceived usefulness* and *perceived ease of use*. *Perceived usefulness* is defined as the degree to which an individual believes that a particular system would enhance his or her performance [7]. *Perceived ease of use* is defined as "the degree to which an individual believes that using a particular system would be free of physical and mental effort" [7].

TAM is frequently used as a tool to explain users' acceptance or rejection of new technologies [7]. To expand TAM's applicability to different domains, numerous extensions to it have been proposed. For example, Venkatesh and Davis [47] proposed TAM2, which included an additional set of variables (e.g., relevance to the user's task, and subjective norm) that could influence users' technology adoption decisions. Another noteworthy extension was proposed by Vijayasarathy [49], who used TAM to predict consumer intentions for using online shopping. Vijayasarathy introduced several new variables, such as privacy and security, that can potentially affect users' adoption intentions.

3 METHODOLOGY

Our methodology was designed to answer the following research questions:

(1) **RQ1**: How widely is SL adopted by Android users?
(2) **RQ2**: What are the factors that attract or deter potential users from adopting SL?

3.1 Qualitative Studies

Since there were no previous studies on SL to inform our investigation, we performed a qualitative user study to gain preliminary insight into how smartphone users would perceive SL. We opted to conduct a cognitive walkthrough with users (CWU) study [18, 30, 31]. The study was made up of cognitive walkthrough (CW) sessions with participants proficient in HCI, and think-aloud sessions with regular smartphone users (not proficient in HCI or usability).

We preferred CWU over other alternative methodologies (e.g., semi-structured interviews or quantitative user satisfaction studies) due to its task-oriented nature and its focus on the learnability of the user interface (UI). The focus on learnability was important to us, as we believe that most potential users find out about the semantics of SL UI through exploratory learning, which is shown to be a primary method for users to discover new features on smartphones [45]. Further, we chose to use the CWU method because it addresses the shortcomings of the traditional cognitive walkthrough (for instance, lack of user involvement and narrow focus) by adding think-aloud sessions with users. We combined the results of these two studies to provide more breadth and depth in usability evaluation [31].

We further refined our study design by introducing a new set of questions to the CWU method. We asked the participants about how they thought each SL method locked or unlocked the phone, what they thought SL was good for, whether they would consider adopting any SL methods, and the reasons for their decisions. All materials that we developed for our CWU study (e.g., persona definition, task lists, etc.) are presented in Appendices A, B, and C.

To test the methodology, we recruited 9 participants through word-of-mouth advertising and conducted 2 pilot cognitive walkthroughs (5 participants in one session and 2 in the other) and 2 pilot think-aloud sessions. Pilot studies showed that think-aloud participants had less opportunity to explain their SL adoption attitudes than did the CW participants.[3] Therefore, we decided to conduct a semi-structured interview with each think-aloud participant to allow them to explain their SL adoption attitudes in their own words. We included this change in the consent form, specifying that the study investigators might ask participants clarification questions about their answers in the reporting form.

For the final study, we used both online (Facebook, Craigslist, and mailing lists) and offline (word-of-mouth) channels to recruit participants for our CW and think-aloud sessions. Overall, we recruited 26 participants: 10 for CW and 16 for think-alouds. We compensated the cognitive walkthrough participants with CAD 20 cash and refreshments, and the think-aloud participants with CAD 30 cash only. We offered refreshments to CW participants to reduce fatigue, as each CW session lasted for more than 2 hours (compared to 40-minute-long think-aloud sessions). We conducted all CW and think-aloud sessions in person between September 2018 and February 2019. We performed data collection and analysis concurrently and continued until we reached theoretical saturation

[3] In the initial design, think-aloud participants submitted written answers to questions about their adoption attitudes, as part of the handout.

(no new codes emerged as a result of the last two data collection sessions).

To analyze the data from our qualitative studies, we transcribed the audio recordings from all sessions, then anonymized and analyzed the transcripts. While we conducted CW sessions before recruiting for and conducting think-aloud sessions, the collected data were analyzed collectively. The average duration of Cognitive walkthrough sessions was 2 hours, while think-aloud sessions lasted for 40 minutes, on average. Overall, we analyzed the transcripts of approximately 14 hours of audio recordings. We chose thematic analysis [3, 20] as our analysis method for these two datasets. To increase the validity of the results, all of the transcripts were coded by two researchers, who used an agreed-upon shared codebook. We calculated the inter-coder reliability and found that it was satisfactory (80%).

3.2 Quantitative Study

Based on the findings of our qualitative studies, we developed a series of hypotheses about **RQ1** and **RQ2** and then conducted a confirmatory online survey to evaluate the hypotheses and answer the research questions.

In our survey, participants were first asked a series of demographic questions, followed by questions about their smartphone usage habits and the screen unlocking methods that they had enabled on their phones. Afterward, participants watched an introductory video about SL, prepared by us, which we used to remind participants about what SL was.[4] We carefully crafted the video to use the exact words that are already used in existing SL setup UI.[5]

After the participants watched the video, we asked them questions about how familiar they were with SL before our study, their experiences of using SL, and their attitudes toward adopting it. Based on the answers to these questions, participants were asked to rank, in order of importance to them, a list of potential reasons for their attitudes toward adopting SL. The list of potential reasons was informed by the findings of our qualitative studies. Participants could also choose not to rank a reason, or to add a new reason and rank it.

Afterward, participants were asked to rank the common smartphone unlocking methods (fingerprint, face unlock, and PIN/password) against all SL methods, based on how convenient they thought each method was. The same procedure was repeated for the perception of security, and the speed of the unlocking methods (i.e., we asked participants to rank the methods in order of how secure and how fast they thought these methods were). The complete list of survey questions is provided in Appendix D.

Finally, to calculate an SL adoption rate, we needed to know whether each participant's phone supported SL. To do so, we asked our survey participants to enter the model number of their phone so we could determine if SL was supported on their device. Since we anticipated that some non-tech-savvy participants might not know the model number of their device, we suggested them to use their main mobile phone to visit the study webpage and to enter their assigned participant ID. This webpage reflected the name of the phone model back to the participant. This was done by examining the user agent field of the HTTP header of their requests. Our web server did not store any user data.

To test our survey design, 7 HCI researchers reviewed our survey questions and provided feedback. We also conducted a pilot study on MTurk with 10 participants. Based on the findings, we made minor adjustments to the wording of some survey questions.

We conducted the main survey on MTurk in September 2019. We chose MTurk as its participants samples are shown to provide meaningful results for the area of usable security [21]. Our advertisement message mentioned a study about Smart Lock for Android, but stated that Turkers (MTurk workers) did not need prior experience with Smart Lock to participate in the study. The survey was only visible to Turkers living in North America[6] and had an approval rating higher than 90%. Non-Android users were excluded from the study. It took the participants 17 minutes on average to complete the survey, and each participant was compensated with USD 4. Overall we received 407 responses to our survey, but eliminated 64 responses due to either inconsistencies in their answers (39), using IP addresses outside North America (10), or being flagged as duplicates or bots by our survey platform (15).

Without assuming any particular distribution for our data, we used chi-squared tests of association and binomial logistic regression to analyze how our hypothesized factors correlated with our outcome variables. To analyze our rank-order data, we used Friedman and Durbin-Conover tests. All pair-wise comparisons were corrected using Bonferroni.

Our university's ethics research board approved the data collection and analysis of all of our studies before any data collection took place.

4 RESULTS AND DISCUSSION

4.1 Demographics

Our CWU sample was diverse in terms of participant age, gender, familiarity with SL, and occupation. While all CW participants were graduate students, only about one-third of the participants in the think-aloud sessions were students. As for their familiarity with SL, some 50% of the participants had never heard of SL; around 20% had heard of it but had never used it; about 10% previously experimented with it but had never used it; 7% had previously used it regularly but had stopped since then; and 7% were using SL regularly at the time of the study. More detailed demographics of our CWU participants are presented in Table 1.

Our survey sample was diverse in terms of gender (58% males and 41% females), and age (min = 19, max = 75, mean = 36, median = 34). In terms of education, 33% of survey participants had high school degrees, 58% had college education, and 9% had master's or PhD degrees. Participants were also diverse in terms of occupation, with computer and mathematical occupations having the highest frequency (around 17%). Table 1 presents more detailed demographics of our survey participants (occupation was omitted due to the great diversity of responses).

[4] Based on our experience with our qualitative study participants, we believed that participants might not necessarily remember what SL was, or that SL might be named differently on their phones.

[5] The video is publicly available on YouTube through this link: https://www.youtube.com/watch?v=N-pC6-kWW0c.

[6] We opted to only include North American participants in our survey because otherwise it would be difficult for us to account for cultural differences and their potential effects on the results.

Table 1: Participant demographics for our CWU and survey studies.

Parameter	Property	CWU Study (N = 26) **% (#) of participants**	Survey Study (N = 343) **% (#) of participants**
Gender	Female	53.8 (14)	58.3 (200)
	Male	46.2 (12)	41.4 (142)
	Other	0.0 (0)	0.3 (1)
Age	19-24	38.5 (10)	5.8 (20)
	25-34	57.7 (15)	46.6 (160)
	35-44	3.8 (1)	28.9 (99)
	45-54	0.0 (0)	14.3 (49)
	55-64	0.0 (0)	3.8 (13)
	65-74	0.0 (0)	0.3 (1)
	75-84	0.0 (0)	0.3 (1)
Education	Less than high school	0.0 (0)	0.3 (1)
	High school	7.7 (2)	33.2 (114)
	University (bachelor's)	38.7 (10)	58.3 (200)
	Master's or PhD	53.4 (14)	8.2 (28)

To gauge the representativeness of our survey sample, we compared the distribution of demographic factors (age, gender, and education) among our participants to the smartphone population in the US reported by the Pew Research Center [5]. Chi-squared tests revealed no significant differences between distributions of the two samples, in terms of age (p = 0.21), gender (p = 0.19), or education levels (p = 0.16). Hence, we believe that our sample is fairly representative.

4.2 Adoption, Rejection, and Interest Rates

To address *RQ1*, we reported on the adoption rate of each SL method, based on the results of our survey study. We defined adoption rate as the ratio of the number of participants who reported using a particular SL method to the number of participants who could have been using that method. We referred to these participants as SL-capable participants. There is a distinction between participants who knew SL was available on their phones and those who knew about SL but did not know it was on their phones. In calculating the SL adoption rate, we used the former. We referred to a participant as SL-capable if they were using a phone that supported SL and they reported having prior knowledge of SL before participating in the study.[7] While a high adoption rate would indicate a high degree of acceptance and adoption of the technology, a low adoption rate would likely indicate the existence of external barriers to adoption of the technology, or the existence of other factors that deterred potential users from adopting SL.

We found that 91.3% (N = 313) of our participants were using phones that supported SL. Among those participants, 60% (N = 184) reported having had prior knowledge of SL before participating in our study (as depicted in Figure 1), making them SL-capable participants.

To get a better understanding of the participants' overall attitudes toward SL, we also reported on the rejection rate of each SL method in our survey study. We defined the rejection rate as the ratio of participants who decided to not use an SL method to SL-capable participants. Participants who rejected the SL method had either experimented with the method but decided not to use it, or used the method for a while but then stopped using it. A high rejection rate would likely indicate the prevalence of highly important adoption barriers (deal-breakers) for potential users.

Finally, we also reported on the interest rate for each SL method in our survey study. We defined the interest rate as the ratio of SL-capable participants who were undecided about the SL method but indicated their willingness to adopt it to the total number of undecided participants. Undecided participants were those who had neither rejected nor accepted SL. Since interested participants have not had any real experience with SL, a low interest rate among them could likely indicate the existence of external factors (e.g., a perceived lack of added convenience when compared to biometric-based phone unlock methods) that deterred them from using SL.

Figure 1 shows the number of survey participants who reported that they had either: (1) been unaware of, (2) adopted, (3) rejected, (4) stated interest in, or (5) stated no interest in, each SL method. Based on this data, Table 2 presents the adoption, rejection, and interest rates of each SL method. As indicated, the adoption rate for all SL methods is less than 20% and the rejection rate is unanimously higher than the adoption rate. Also, the interest rate is higher than either the adoption or the rejection rate for all SL methods. These findings suggest the following:

- SL is not a widely adopted technology, with an average adoption rate of 13.7%. In comparison, the PIN, fingerprint, and pattern phone unlocking methods had adoption rates of 68%, 47%, and 26% respectively, among the SL-capable participants in our study. This finding likely indicates the existence of barriers to the adoption of SL.
- SL had a relatively high rejection rate, with an average of 22.5%. This likely indicates that there are deal-breakers that deter potential users from adopting SL.

[7] We excluded participants who were not using an SL-enabled phone, or who reported not having prior knowledge of SL before the study, from the SL adoption/rejection rate calculations. This was because we believed that the adoption attitude data from such participants (without awareness) would be of low ecological validity.

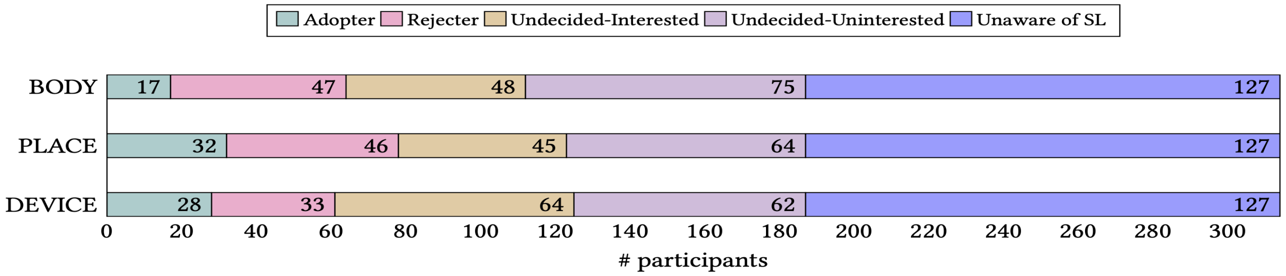


Figure 1: Experience with and attitudes toward adopting each SL method, for survey participants who had SL-capable phones and indicated having prior knowledge of SL before the study.

Table 2: Adoption, rejection, and interest rates for different SL methods in our survey study.

SL Method	Adoption Rate (%)	Rejection Rate (%)	Interest Rate (%)
BODY	9.1	25.1	39.0
PLACE	17.1	24.6	41.3
DEVICE	15.0	17.6	50.8
Average	13.7	22.4	43.7

- The interest rate in SL among SL-capable participants was 44%. Our observed interest rate is lower than that of the existing IA perception studies, where more than 60% of their participants indicated a willingness to adopt IA [8, 27]. We suspect that this is due to the low ecological validity of such studies, where the participants only experimented with a pseudo-IA scheme that did not suffer from reliability issues, and where the participants did not have to put in the effort to set up IA on their phones.

Hence, to answer **RQ1**, it seems that with an adoption rate of only 13.7%, SL is not a widely adopted technology. This finding reiterates the importance of investigating **RQ2**, which can help the research community gain insight into possible real-world barriers to IA adoption.

To address **RQ2**, we report on how our survey participants ranked the reasons for their interest in and adoption of each SL method. Based on the findings of our CWU study, we placed these reasons into 5 categories: "utility," "security," "privacy," "reliability," and "other reasons." Figure 2 depicts the average rank that the adopters/rejecters or the interested/uninterested participants of each SL method assigned to each category of reasons to justify their decisions. In sections 4.3 to 4.7, we examine in detail the role of each category as a potential barrier to the adoption of SL.

4.3 Security

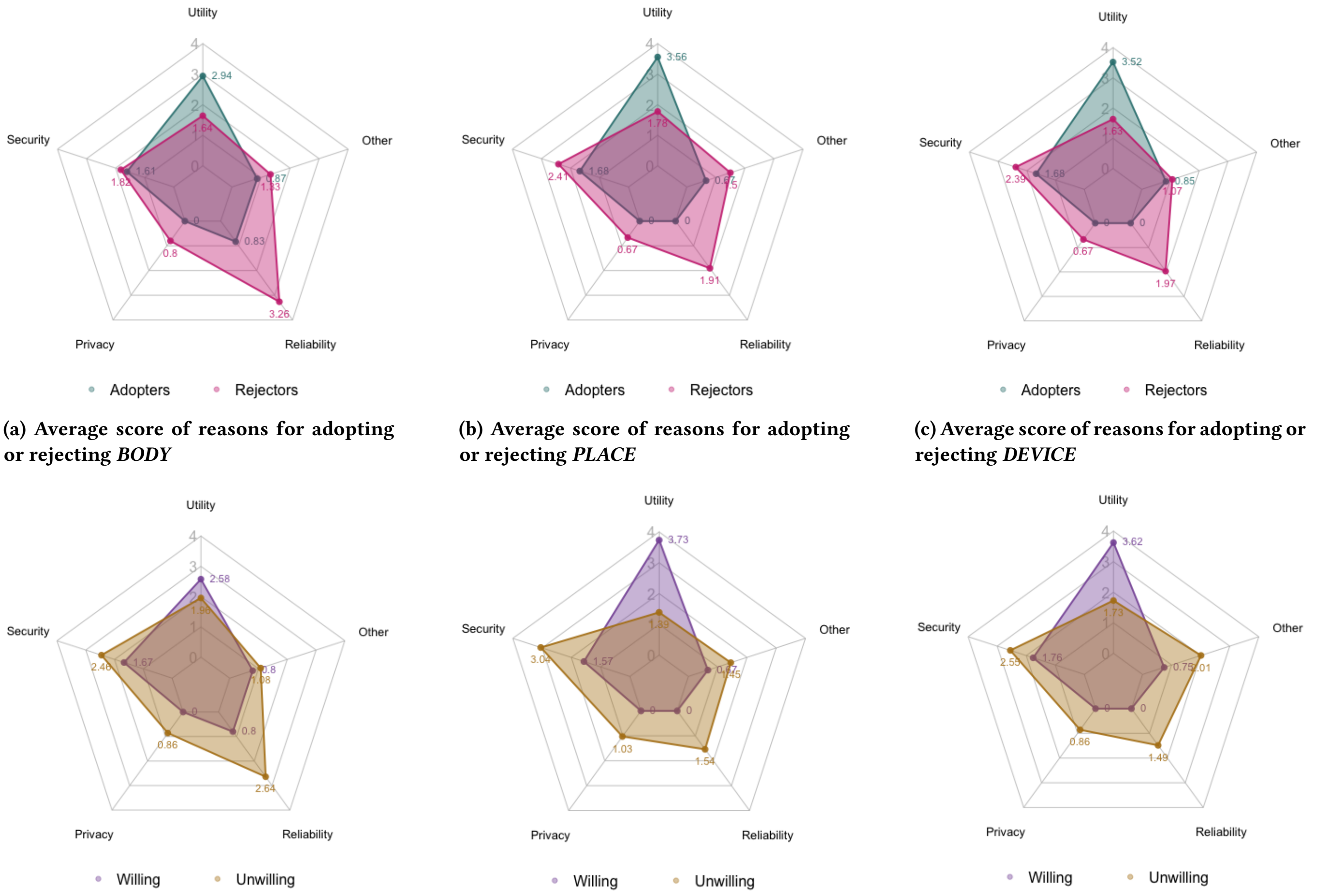
Perceived lack of security has been shown to be a major deterrent for adoption of new technologies. For example, this has been the case with Apple Pay [23] and face unlock [11]. In the case of SL, we observed a perceived lack of security (i.e., the possibility of someone gaining access to the phone without the owner's authorization) to be a major adoption barrier as well.

First, we found evidence in our qualitative data that perceived insecurity deters participants from adopting SL. Some of the CWU participants justified their unwillingness to adopt SL by explicitly citing insecurity as the reason. For example, when asked whether he would adopt *BODY*, one of our think-aloud participants (P-TA-15, male, student) said: *"I think [in the case of] the on-body detection [the answer] is no. Even when you're not at home, like you're at the mall or something like that. It's still possible [for someone to unlock the phone]."*

Our survey study confirmed the role of a perceived lack of security as a major deterrent. Among our undecided SL-capable participants, those who indicated an unwillingness to adopt *BODY*, *PLACE*, or *DEVICE* ranked insecurity as one of the top two highest-ranking reason (alongside reliability, as depicted in Figures 2d, e, and f) as to why they were unwilling to adopt the SL methods. They ranked it significantly higher than any other category of reasons ($p < 0.05$, Durbin-Conover test). This seems to be a valid concern, as those of our participants who reported having stopped using these methods also ranked insecurity as one of the top three highest-ranking reasons (as depicted in 2a, b, and c) for their decision to abandon the feature, again ranking it higher than any other remaining category of reasons ($p < 0.05$, Friedman test).

As further evidence in support of our hypothesis, when we asked participants to rank SL methods against PIN and fingerprint phone unlocking methods, we found that participants who indicated unwillingness to adopt SL ranked fingerprint and PIN as significantly more secure than SL ($p < 0.05$, Durbin-Conover test). We found these results to be in contrast to Khan et al. [27], who reported that 81% of their participants were satisfied with the level of security that their pseudo-IA scheme provided.

One illustrative case of security concerns with SL was that most of our think-aloud participants expressed that SL might allow their family members or co-workers to access their phones without their permission. One such participant (P-TA-13, male, student) explained: *"I don't think it [DEVICE] is something that I would use at*



(a) Average score of reasons for adopting or rejecting *BODY*

(b) Average score of reasons for adopting or rejecting *PLACE*

(c) Average score of reasons for adopting or rejecting *DEVICE*

(d) Average score of reasons for being (un-)interested in *BODY*

(e) Average score of reasons for being (un-)interested in *PLACE*

(f) Average score of reasons for being (un-)interested in *DEVICE*

Figure 2: The average importance score that participants assigned to each category of reasons for adopting, rejecting, or being (un-)interested in adopting SL methods.

all, because even if it's at my home and a friend is over or something, they can just unlock my phone. It'll be easy for them to do it. It could be even ... my brother!" Considering that snooping on mobile devices is both frequent [34] and antagonizing [33], this finding indicates that it is important to further investigate whether "increased risks of social-insider attacks" is a serious concern and barrier for IA adoption. To the best of our knowledge, this question has not been studied before and merits future research.

4.4 Privacy

Studies have shown that privacy is a major concern for smartphone users when it comes to authentication [24, 37]. In the case of SL, we hypothesized that privacy concerns may also be a barrier for adopting it.

Our CWU study study partially supported our hypothesis. Some of our CWU participants expressed direct privacy concerns with SL. For example, P-TA-3 (female, health specialist) remarked about SL: *"This [SL] is a potential security asset because if your phone is stolen or lost, your information will not be as easily hacked as if you use the regular lock. I think that it is a toss-up between having your data for the smart lock feature recorded by your phone provider versus potential loss of information."* In general, we observed privacy concerns among our participants to be about manufacturers' unauthorized use of user's data. Also, as discussed in Section 4.3, we found security concerns among the CWU participants that, if realized, could lead to a violation of the users' privacy.

Our survey study, however, did not support the role of privacy for SL adoption. Survey participants did not rank privacy as a major reason for abandoning the technology or being unwilling to adopt it (depicted in Fig 2).

Caution needs to be used when drawing conclusions about the role of privacy in SL adoption. Since we used ranking (instead of rating) in our survey to test the link between security, privacy and SL adoption, security ended up always being the most important factor, potentially masking the effect of privacy. Studies are needed to further investigate the correlation between privacy and intent to use SL.

4.5 Reliability

The themes of perceived unreliability (i.e., accidental unlocking or locking the user out) of SL methods and, as a consequence, lack of trust in the technology, kept reappearing in our collected data. While interrelated with security and privacy, these themes deserve their own analysis in relation to SL and its users. Given the problems discussed in those sections, it is not surprising that our participants often found SL unreliable and hard to trust.

The participants in our qualitative studies found that SL lacked reliability, precision, and accuracy. For example, several participants expressed their belief that GPS lacks the precision necessary to be trusted as an unlocking factor. One of our think-aloud participants (P-TA-16, female, unemployed) expressed such concern by stating: *"I think, for example, if I add my home as a trusted place, then if I go to a coffee shop downstairs beside my place, it might still think I'm at home [and unlock the phone]."*

Our survey data confirmed the role of unreliability as a major adoption barrier. Among our SL-capable participants, those who indicated an unwillingness to adopt *BODY* ranked accidental unlocking as one of the top two (alongside security) most important reasons (depicted in Fig 2a) for their unwillingness to adopt SL, ranking it significantly higher than other reasons ($p < 0.05$, Durbin-Conover test). This seems to be a valid concern, as observed unexpected behavior by *BODY* and accidental unlocking were the top two highest-ranking reasons that our *BODY* abandoners stopped using it, ranking them higher than any other reason ($p < 0.05$, Durbin-Conover test). The same trend was observed with *PLACE* and *DEVICE* as well (depicted in Fig 2b and c).

Overall, our results seem to suggest that a perceived lack of reliability is a major factor that deters potential users from SL. This finding reaffirms the importance of reliability in technology adoption, as shown by Butler and Sellbom [4], and reiterates the importance of minimizing authentication false positive and negative rates when designing IA schemes for smartphones.

4.6 Utility

Perceived utility is an important factor when it comes to technology adoption. Previous studies, such as those by Zhang and Xu [51] and by Huh et al. [23], have shown that users' perceptions of the usefulness of a new technology correlates positively with their intention to adopt it.

In the case of SL, the results of our qualitative study suggest that the main utilities of SL are:

- **Convenience**: SL can make it easier to unlock smartphones or keep them unlocked, at least under certain circumstances, when compared to conventional explicit smartphone unlocking methods (e.g., PIN or fingerprint).
- **Speed**: SL can make it faster to unlock smartphones, at least under certain circumstances, as compared to conventional unlocking methods.
- **Redundancy (backup)**: SL can be used as a backup method to unlock phones when users cannot unlock their phones (e.g., because they forgot their PINs or patterns).

The importance of these utility aspects was further corroborated by our survey study, where SL adopters cited convenience and speed as the top reasons for their decision to adopt SL. These two reasons were ranked significantly higher than any of the other reasons ($p < 0.05$, Durbin-Conover test).

However, our results also showed that the majority of the participants were not convinced of the added benefits of SL and that this was a major adoption barrier for them. The first evidence of this was observed in our CWU study, where some participants cited a perceived lack of *added* convenience as the reason for their unwillingness to adopt SL. For example, one of our think-aloud participants (P-TA-11, male, language teacher) remarked about *DEVICE*: *"I probably wouldn't use it, because I can't think of a use for it. I can play music from my phone even though it is locked. So I don't need the trusted device feature."*

Our survey data corroborated this finding, where those participants who either had rejected SL, or were unwilling to use it, ranked a perceived lack of utility as the most important reason (depicted in Figure 2) for their choice ($p < 0.05$, Durbin-Conover test). In addition, when asked to rank SL against the PIN and fingerprint methods, in terms of the speed and the convenience of unlocking, these participants ranked the fingerprint method to be significantly faster and more convenient than any of the SL methods ($p < 0.05$, Durbin-Conover test). They also ranked the PIN method as significantly more convenient, but slower than SL ($p < 0.05$, Durbin-Conover test).

Overall, our results suggest that it is difficult for Android users to understand or perceive the utility of SL, especially its convenience or speed advantages over the fingerprint method. This contributed significantly to the participants' unwillingness to adopt SL. We believe that there is a potential usability misconception, in that using SL to keep phones unlocked (in trusted places or near trusted devices) will be faster than having to explicitly touch fingerprint scanners and wait a moment for phones to become unlocked. Further research is necessary to determine more effective ways to communicate the usability benefits of SL (and IA in general) to smartphone users. Also needed is research on whether users will adopt IA if they understand that it can help them unlock faster and avoid having to unlock in the first place.

4.7 Other Adoption Barriers

In addition to the discussed adoption barriers, our participants occasionally expressed other interesting reasons for not using SL. While these barriers are not as important due to the low importance score assigned to them by the participants, we believe that some of them are worth discussing, as they might have higher indirect impacts on smartphone users' attitudes toward SL. These barriers include the following:

I) Semantics: As discussed in Section 4.7, some of our CWU participants expressed difficulty with understanding the semantics of SL (i.e., how each SL method locked or unlocked the phone), and this made them unable to correctly judge when their phone would be locked by SL. As it has been shown that the compatibility of mental models between old and new technologies correlates positively with users' intention to switch to the latter [51], we theorized that difficulty with understanding SL semantics might have contributed to the low adoption rate of SL. However, our survey participants rarely cited difficult semantics as an important reason for being unwilling to adopt SL, or deciding to abandon it, which suggests that ease of understanding semantics does not play a significant role (either as a attractant or as a deterrent) for SL adoption. Despite this finding, we still believe it is important that further studies be conducted to gain insight into how smartphone users understand the semantics of IA. During our CWU study, we observed that a misunderstanding of semantics can lead to a misjudgment of when the phone would be locked. This can have dire consequences, and to the best of our knowledge, no study on how smartphone users understand IA semantics has been reported so far.

II) Use of Unlocking: Some of our CWU participants stated that they were unwilling to adopt SL because they were satisfied with their current unlocking method. While most of such participants were using fingerprint unlocking, we occasionally observed PIN users who expressed the same sentiment. As such, we hypothesized that SL might be more appealing to those who are not locking their phones. Our survey data, however, did not support this hypothesis: 17.5% (N = 55) of our survey participants reported not using any locking on their phones. A chi-squared test of association showed that such participants are not significantly more likely to be willing to adopt SL ($p > 0.05$, chi-squared test).

III) Usability of the SL UI: Through our cognitive walkthrough, think-aloud, and interview sessions, we found various usability issues with the SL UI (e.g., inconsistencies and ambiguities) that caused confusion for our participants. For example, the UI for *PLACE* lacked a tutorial screen to explain to the user how the SL method worked, whereas *BODY* and *DEVICE* had such screens. We found that such usability issues affected participants' trust in the technology, which can be a major barrier to its adoption. For example, after experiencing the SL UI, one of our CW participants (P-CW-8, male, student) mentioned: *"All these inconsistencies make you wonder if the Android team at Google cares at all ... I don't trust this [SL] at all."* While our survey participants rarely cited the usability of the SL UI as a reason for their decision to reject SL, we observed that misunderstanding the semantics can lead to users forming inadequate mental models. Unfortunately, to the best of our knowledge, there are no guidelines or heuristics reported for designing or evaluating the UI for IA on smartphones. Providing such guidelines or heuristics can help system designers communicate the semantics of IA and its capabilities more efficiently, to avoid user frustration and dangerous errors. We believe this to be an important knowledge gap and a good avenue for future work.

5 SMART LOCK TECHNOLOGY ACCEPTANCE MODEL (SL-TAM)

In this section, we structured all of our findings into a framework for reasoning about smartphone users' SL adoption decision. Providing such framework is valuable because while the existing literature, e.g., the technology adoption model (TAM) [10], could be used for predicting SL adoption, resulting conclusions would not be supported by existing empirical data. Also, due to the abstract definition of predictors in TAM, it would be difficult to interpret what they entail in the context of IA. As explained below, TAM would also miss the link between security and SL adoption.

To devise our framework, we first investigated how our CWU findings conformed with TAM [7, 10] and how TAM needed to be extended for the case of SL, in Section 5.1. This provided us with an extended TAM we called SL-TAM. Afterward, in Section 5.2, we used our survey data to test SL-TAM.

5.1 Devising SL-TAM with CWU Findings

As discussed in Section 2.3, TAM introduces two factors that influence adoption attitudes toward a new technology: *perceived usefulness* and *perceived ease of use*. In the following, we examined how these factors manifested themselves in our CWU study and how they affected participants' adoption decision:

(1) **Perceived usefulness**: TAM theorizes that to adopt a new technology, potential users must find it useful. Our CWU results (discussed in Section 4.6) showed us that the usefulness of SL translates to whether users think it can make unlocking easier or faster, or can be used as a backup unlocking method. Subsequently, as TAM would predict, we found that users' perception of these SL benefits directly correlates with their willingness to adopt it. Based on this observation, we hypothesized that *perceived usefulness* indeed is linked to the intention to use SL, and it is determined by the unlocking convenience, speed, and backup use of SL (depicted as *H1* in Figure 3).

(2) **Perceived ease of use**: TAM predicts that the intention to adopt a new technology correlates with the amount of cognitive and physical effort that is needed to use it. In the case of SL, our CWU investigations showed that this effort is divided into two main components: (1) the initial effort to set up SL, and (2) the effort that takes to unlock the phone manually if SL fails to operate as expected. The setup effort manifested itself as the usability of the SL UI: how difficult was it for participants to set up SL and understand how it works? The second component manifested as one of the reliability issues in our study (discussed in Section 4.5), where unexpected behaviors (e.g., failing to unlock the phone) caused CWU participants to lose trust in SL. Therefore, we hypothesized that *perceived ease of use* is indeed a predictor of users' intention to adopt SL and that this factor is determined by the setup effort and reliability of SL. This hypothesis is depicted as *H2* in Figure 3.

In addition to the factors above, we found another deterrent keeping our CWU participants from adopting SL to be security and privacy concerns. Such concerns, however, do not seem to be related to either *usefulness* or *ease of use*. Thus, it seems that TAM neglects the effect of security and privacy risks in predicting users' adoption intention. We discovered that a similar observation has been made by other studies that applied TAM to specific domains, such as Sun et al. [43] who applied it to OpenID, or Vijayasarathy [49], who applied it to online shopping. Inspired by their results, we expanded our SL-TAM to include a new predictor called "perceived security and privacy" (depicted as *H3* in Figure 3), which is determined by the following factors:

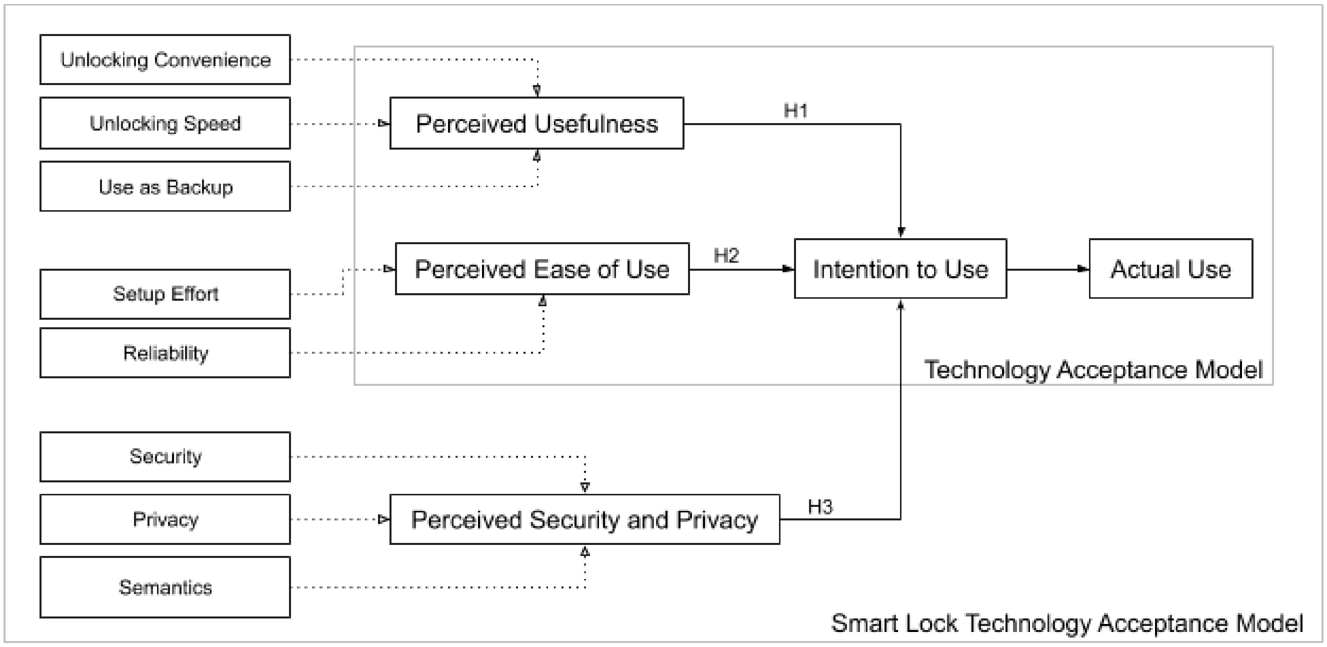


Figure 3: Smart Lock technology acceptance model.

(1) **Security**: As we discussed in Section 4.3, some of our CWU participants explicitly cited insecurity as the reason they were unwilling to adopt SL, showing it directly influences users' SL adoption intention.
(2) **Privacy**: As discussed in Section 4.4, some CWU participants cited lack of privacy as a potential drawback of SL, showing that privacy concerns could lead users to hesitate to adopt SL.
(3) **Semantics**: As discussed in Section 4.7, we observed, in our CWU study, that (in-)correct understanding of SL semantics can lead to misconceptions about SL security, which directly affected users' willingness to adopt SL.

5.2 Testing SL-TAM with Survey Data

We tested SL-TAM by evaluating how our survey data conforms with it for the adoption of each SL method. To this end, we evaluated how our hypothesized factors ("perceived usefulness," "perceived ease of use," and "perceived security and privacy") correlated with SL-experienced participants' decision to either use SL or abandon it (to preserve ecological validity, we focus on this group of participants alone). First, Figure 2 depicts the average importance score that the participants assigned to each group of reasons for their decision to adopt or reject SL. We used these scores in the following way to test SL-TAM: the utility score was used to represent "perceived usefulness," (as it is an aggregated score of perceived convenience, speed, and backup use of SL); the reliability score was used to represent "ease of use," (our survey is not capable of evaluating "setup effort"); and the sum of the security and privacy and semantics scores was used to represent "perceived security and privacy." To formally evaluate how these predictors correlated with SL adoption decisions, we report the results of three binomial logistic regression (BLR) tests (one for each method). In each test, the decision to adopt the SL method was the dichotomous dependent variable, and the hypothesized factors were the preceptors. To ensure the validity of our tests, we checked for multicollinearity between variables but found that this was not an issue ($1.0 < \text{VIF} < 1.2$). Also, the model fit measures were satisfactory for all three BLR tests ($R^2 = 0.505$ for BODY, $R^2 = 0.561$ for PLACE, and $R^2 = 0.571$ for DEVICE).

Table 3 presents the results of our BLR tests. They show:

- **Testing H1**: Perceived usefulness was a statistically significant predictor for BODY, PLACE and DEVICE adoption ($p < 0.01$ in all three tests). The high odds ratios (OR) further demonstrated the strength of this correlation. With BODY, for example, one unit increase in the "usefulness" ranking (e.g., by improving the unlocking speed of SL methods) increased the chances of adoption nearly seven-fold.
- **Testing H2**: Perceived ease of use was a significant predictor of BODY and DEVICE adoption ($p < 0.01$ in the corresponding BLR tests). The ORs further affirmed that the observed correlations are strong. In case of DEVICE, for example, a one-unit increase in the "ease of use" ranking resulted in a 3.29 times higher chance of adoption. In the case of PLACE, while the correlation was not statistically significant, the OR still showed a strong association between "ease of use" and PLACE adoption.
- **Testing H3**: Perceived security and privacy was shown to be a significant predictor of PLACE and DEVICE adoption ($p < 0.05$ in the corresponding BLR tests). Furthermore, ORs showed the correlations to be strong. For example, in the

Table 3: Results of the binomial logistic regression (BLR) tests to validate the correlation between SL-TAM predictors and survey participants' intention to adopt SL.

SL-TAM Predictor	**Dependent Variable**		
(Independent Variable)	BODY	PLACE	DEVICE
Perceived Usefulness	p-value = 0.001 Odds ratio = 7.16	p-value = 0.001 Odds ratio = 3.27	p-value = 0.001 Odds ratio = 9.40
Perceived Ease of Use	p-value = 0.016 Odds ratio = 9.82	p-value = 0.275 Odds ratio = 3.27	p-value = 0.090 Odds ratio = 3.29
Perceived Security and Privacy	p-value = 0.744 Odds ratio = 1.09	p-value = 0.001 Odds ratio = 5.22	p-value = 0.019 Odds ratio = 2.34

case of PLACE, a one-unit increase in "security and privacy" ranking increased the chances of adoption by 5.22 times. In case of BODY, "perceived security and privacy" was not a statistically significant predictor of adoption (p > 0.05 in BD BLR test). As discussed in Section 4, the main deterrent for BODY was shown to be reliability (accidental unlocks), which is reflected in the "perceived ease of use" predictor.

In conclusion, BLR testing showed that our survey data conformed highly with our SL-TAM model, demonstrating the feasibility of our hypothesized factors, namely "perceived usefulness," "perceived ease of use," and "perceived security and privacy" for predicting SL adoption. We hope that this model can inform the design of future SL-like authentication schemes by shedding light on the important factors that can attract or deter smartphone users from IA-based unlocking.

6 THREATS TO VALIDITY

Any generalization of our findings needs to be made carefully, due to the following study limitations:

(1) We mentioned "Smart Lock" in the study advertisement, and therefore our sample might have been skewed toward participants who are using or interested in SL. This bias could have potentially caused an overestimation of SL adoption and awareness rate. However, even with the adoption rate being overestimated, the results (14%) still suggest that SL is far from being widely adopted.

(2) The cross-sectional design of our qualitative study might have prevented us from investigating the effects of prolonged use of SL on participants' perceptions of it. We believe, however, that directly surveying SL adopters addressed this possible weakness.

(3) As with all qualitative usability studies, the limited size and diversity of our CWU participant sample might have prevented us from uncovering all potential factors that can affect smartphone users' perceptions of SL. Even though we reached theoretical saturation, the chance of unforeseen biases causing us to miss some adoption barriers still exists.

(4) Even though SL is the first, and currently only, widely deployed IA scheme, it is difficult to determine the extent to which users' perceptions of SL can be extrapolated to their perceptions of IA in general. And while some SL concerns may be easily applicable to any IA scheme (e.g., security and privacy concerns), some others might be specific to SL (e.g., usability of the SL UI).

(5) Our participants self-reported their prior awareness of, and experiences with, SL. As is common with self-reported data, it is possible that the participants' answers might not be completely reflective of their real-world behavior. While we eliminated those responses that showed clear inconsistencies in the data (See section 3.2), there is still the chance that some participants might not have answered truthfully. This might limit the external and ecological validity of our results.

7 CONCLUSION

Smart Lock is the first massively deployed and commercialized IA solution that allows smartphones to be automatically unlocked using a combination of contextual (e.g., location) and behavioral (e.g., body movement) authentication factors. To understand how this first widely deployed IA method is perceived by Android users, we conducted a multi-method qualitative study with 27 participants, composed of cognitive walkthroughs, think-aloud sessions, and interviews, followed by an online survey on Amazon Mechanical Turk involving 343 Android-using participants.

Our results suggest that perceived lack of reliability, utility, and security negatively affected Android users' intention to adopt SL, leading to a low (14%) adoption rate. Reliability-wise, participants were concerned that SL could lead to frequent accidental unlocks and pocket dialing. Utility-wise, SL was perceived as not being of enough value as it could not increase the unlocking convenience (the required physical and cognitive effort) or speed, or be used as a backup unlocking method. Finally, as far as security was concerned, participants were worried that adopting SL could lead to unauthorized access to their phone, by their family members or co-workers, for example.

To provide a framework for reasoning about SL adoption intentions, we structured our findings into an SL-specific extension of technology acceptable model (TAM). Our SL-TAM theorizes that there are three main factors affecting users' intention to adopt SL: "perceived usefulness," "perceived ease of use," and "perceived security and privacy." "Perceived usefulness" is determined by the convenience and speed of unlocking with SL and whether it is possible to using it as a backup unlocking method. "Perceived ease of use" is determined by the amount of effort it takes to setup SL, and its reliability. And, "perceived security and privacy" is determined by the actual security and privacy of SL and how difficult its semantics are for users to grasp. We tested SL-TAM using our survey data, which showed high predictive power.

Based on the findings, we recommend that, to improve how smartphone users perceive an IA scheme like SL, its added value (in terms of speed or convenience of unlocking) needs to be communicated to users in a clear and accessible way. The scheme also needs to be reliable and trusted by the users, and the chances of malfunction (e.g., failure to lock the phone automatically) should be minimized and disclosed. In addition, to help users develop and maintain adequate mental models of the technology, the semantics of any IA scheme should be clearly communicated to users, so that they can become comfortable with it, learn how to use it effectively, and avoid dangerous errors.

8 ACKNOWLEDGMENTS

This research has been supported in part by a research grant from Samsung and by a gift from Scotiabank to UBC. We would like to thank members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE), who provided their feedback on the reported research and earlier versions of the paper. We thank our anonymous reviewers for all the feedback and suggestions they provided to improve the paper. Stylistic and copy editing by Eva van Emden helped to improve readability of this paper.

REFERENCES

[1] Shatha J Alghamdi and Lamiaa A Elrefaei. 2018. Dynamic authentication of smartphone users based on touchscreen gestures. *Arabian journal for science and engineering* 43, 2 (2018), 789–810.

[2] Cheng Bo, Lan Zhang, Taeho Jung, Junze Han, Xiang-Yang Li, and Yu Wang. 2014. Continuous user identification via touch and movement behavioral biometrics. In *2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC)*. IEEE, Austin, TX, USA, 1–8.

[3] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[4] Darrell L Butler and Martin Sellbom. 2002. Barriers to adopting technology. *Educause Quarterly* 2, 1 (2002), 22–28.

[5] Pew Research Center. 2019. Mobile Technology and Home Broadband 2019. https://www.pewinternet.org/2019/06/13/mobile-technology-and-home-broadband-2019/. Accessed: 2019-07-26.

[6] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the Impact of Touch {ID} on iPhone Passcodes. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. USENIX, Ottawa, Canada, 257–276.

[7] Mohammad Y Chuttur. 2009. Overview of the technology acceptance model: Origins, developments and future directions. *Working Papers on Information Systems* 9, 37 (2009), 9–37.

[8] Heather Crawford and Karen Renaud. 2014. Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management* 1, 1 (2014), 7.

[9] Heather Crawford, Karen Renaud, and Tim Storer. 2013. A framework for continuous, transparent mobile device authentication. *Computers & Security* 39 (2013), 127–136.

[10] Fred D Davis, Richard P Bagozzi, and Paul R Warshaw. 1989. User acceptance of computer technology: a comparison of two theoretical models. *Management Science* 35, 8 (1989), 982–1003.

[11] Alexander De Luca, Alina Hang, Emanuel Von Zezschwitz, and Heinrich Hussmann. 2015. I feel like I'm taking selfies all day!: towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, Seoul, Republic of Korea, 1411–1414.

[12] Mohammad Omar Derawi, Claudia Nickel, Patrick Bours, and Christoph Busch. 2010. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, Darmstadt, Germany, 306–311.

[13] Serge Egelman, Sakshi Jain, Rebecca S Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are you ready to lock?. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Arizona, USA, 750–761.

[14] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunar, Yifei Jiang, and Nhung Nguyen. 2012. Continuous mobile authentication using touchscreen gestures. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for.* IEEE, Waltham, MA, USA, 451–456.

[15] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2013. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security* 8, 1 (2013), 136–148.

[16] Lex Fridman, Steven Weber, Rachel Greenstadt, and Moshe Kam. 2017. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal* 11, 2 (2017), 513–521.

[17] Google. 2019. Google I/O 2014 Keynote. https://www.youtube.com/watch?time_continue=1659&v=biSpvXBGpE0. Accessed: 2019-02-14.

[18] T Granollers and J Lorés. 2005. Cognitive Walkthrough With Users: an alternative dimension for usability methods. In *Proc. HCI International, Las Vegas*. HCI International, Las Vegas, Nevada, USA, 38.

[19] Alexandru-Cosmin Grivei. 2015. Touch based biometric authentication for Android devices. In *Electronics, Computers and Artificial Intelligence (ECAI), 2015 7th International Conference on*. IEEE, Bucharest, Romania, WSD–15.

[20] Greg Guest, Kathleen M MacQueen, and Emily E Namey. 2011. *Applied thematic analysis*. sage, USA.

[21] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *Symposium on usable privacy and security (SOUPS)*. USENIX, Menlo Park, CA, USA, 213–230.

[22] Eiji Hayashi, Oriana Riva, Karin Strauss, AJ Brush, and Stuart Schechter. 2012. Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, Washington, DC, USA, 2.

[23] Jun Ho Huh, Saurabh Verma, Swathi Sri V Rayala, Rakesh B Bobba, Konstantin Beznosov, and Hyoungshick Kim. 2017. I Don't Use Apple Pay because it's less secure...: perception of security and usability in mobile tap-and-pay. In *Proceedings of the Workshop on Usable Security (USEC)*, Vol. 12. Internet Society, San Diego, CA, USA, 1–12.

[24] Sevasti Karatzouni, Steven M Furnell, Nathan L Clarke, and Reinhardt A Botha. 2007. Perceptions of user authentication on mobile devices. In *Proceedings of the ISOneWorld Conference*. Citeseer, Las Vegas, NV, USA, 11–13.

[25] Hassan Khan, Aaron Atwater, and Urs Hengartner. 2014. A comparative evaluation of implicit authentication schemes. In *International Workshop on Recent Advances in Intrusion Detection*. Springer, Switzerland, 255–275.

[26] Hassan Khan, Aaron Atwater, and Urs Hengartner. 2014. Itus: an implicit authentication framework for android. In *Proceedings of the 20th annual international conference on Mobile computing and networking*. ACM, New York, NY, United States, 507–518.

[27] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2015. Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying.. In *SOUPS*. USENIX, Ottawa, Canada, 225–239.

[28] Suzanne Kieffer, Ugo Braga Sangiorgi, and Jean Vanderdonckt. 2015. Ecoval: A framework for increasing the ecological validity in usability testing. In *2015 48th Hawaii International Conference on System Sciences*. IEEE, Kauai, HI, USA, 452–461.

[29] Kryptowire. 2019. Kryptowire Continuous Authentication. https://www.kryptowire.com/continuous-authentication/. Accessed: 2019-02-20.

[30] Wallace Lira, Renato Ferreira, Cleidson de Souza, and Schubert Carvalho. 2014. Experimenting on the cognitive walkthrough with users. In *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services*. ACM, New York, NY, United States, 613–618.

[31] Thomas Mahatody, Mouldi Sagar, and Christophe Kolski. 2010. State of the art on the cognitive walkthrough method, its variants and evolutions. *Intl. Journal of Human–Computer Interaction* 26, 8 (2010), 741–785.

[32] Ahmed Mahfouz, Ildar Muslukhov, and Konstantin Beznosov. 2016. Android users in the wild: Their authentication and usage behavior. *Pervasive and Mobile Computing* 32 (2016), 50–61.

[33] Diogo Marques, Tiago Guerreiro, Luís Carriço, Ivan Beschastnikh, and Konstantin Beznosov. 2019. Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, United States, 589.

[34] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on mobile phones: Prevalence and trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Vol. 2. USENIX, Denver, CO, USA, 77.

[35] Nicholas Micallef, Mike Just, Lynne Baillie, Martin Halvey, and Hilmi Güneş Kayacik. 2015. Why aren't users using protection? investigating the usability of smartphone locking. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, Copenhagen Denmark, 284–294.

[36] Arsalan Mosenia, Susmita Sur-Kolay, Anand Raghunathan, and Niraj K Jha. 2017. CABA: Continuous authentication based on BioAura. *IEEE Trans. Comput.* 66, 5

(2017), 759–772.

[37] Salil Prabhakar, Sharath Pankanti, and Anil K Jain. 2003. Biometric recognition: Security and privacy concerns. *IEEE security & privacy* 1, 2 (2003), 33–42.

[38] Abena Primo, Vir V Phoha, Rajesh Kumar, and Abdul Serwadda. 2014. Context-aware active authentication using smartphone accelerometer measurements. In *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*. IEEE, Columbus, Ohio, USA, 98–105.

[39] Lina Qiu, Alexander De Luca, Ildar Muslukhov, and Konstantin Beznosov. 2019. Towards Understanding the Link Between Age and Smartphone Authentication. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, United States, 1–10.

[40] Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos. 2012. Progressive Authentication: Deciding When to Authenticate on Mobile Phones.. In *USENIX Security Symposium*. USENIX, Bellevue, WA, USA, 301–316.

[41] Everett M Rogers. 2010. *Diffusion of innovations*. Simon and Schuster, New York, NY, USA.

[42] Aditi Roy, Tzipora Halevi, and Nasir Memon. 2014. An hmm-based behavior modeling approach for continuous mobile authentication. In *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*. IEEE, Florence, Italy, 3789–3793.

[43] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. 2011. What makes users refuse web single sign-on?: an empirical investigation of OpenID. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, New York, NY, United States, 4.

[44] Zahid Syed, Jordan Helmick, Sean Banerjee, and Bojan Cukic. 2019. Touch gesture-based authentication on mobile devices: The effects of user posture, device size, configuration, and inter-session variability. *Journal of Systems and Software* 149 (2019), 158–173.

[45] James Tiongson. 2015. Mobile app marketing insights: How consumers really find and use your apps.

[46] UnifyID. 2019. UnifyID Implicit Authentication Platform. https://unify.id/product/. Accessed: 2019-02-20.

[47] Viswanath Venkatesh and Fred D Davis. 2000. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science* 46, 2 (2000), 186–204.

[48] Viswanath Venkatesh, Michael G Morris, Gordon B Davis, and Fred D Davis. 2003. User acceptance of information technology: Toward a unified view. *MIS quarterly* 27 (2003), 425–478.

[49] Leo R Vijayasarathy. 2004. Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model. *Information & management* 41, 6 (2004), 747–762.

[50] Hui Xu, Yangfan Zhou, and Michael R Lyu. 2014. Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. In *Symposium On Usable Privacy and Security, SOUPS*, Vol. 14. USENIX, Menlo Park, CA, USA, 187–198.

[51] Wei Zhang and Peng Xu. 2011. Do I have to learn something new? Mental models and the acceptance of replacement technologies. *Behaviour & Information Technology* 30, 2 (2011), 201–211.

A CWU MATERIAL

- **User Profile**: It is important to define the profile correctly because any unreasonable assumption about the abilities of the user can negatively influence the CW findings to be unrealistic, and not representative of the interaction between a user and the UI in reality. In case of SL, based on Google's description of the technology, we assumed that the UI caters for users that have some experience with a smartphone but no particular knowledge or training in SL authentication, or any other aspect of computer security or privacy. Therefore, throughout the course of the CW sessions, we asked our HCI-proficient participants to put themselves in the shoes of a computer-science-illiterate regular smartphone user.
- **Task List**: We chose those tasks that are more likely to be performed by a first-time SL user. The tasks included enabling/disabling on-body detection, adding/removing a new trusted place, adding/removing a trusted device, adding/removing a new trusted face, setting up/removing a voice model for Voice Match.
- **Action Sequences**: To the best of our ability, we designed the action sequences to be as simple as possible and to resemble real usage. When possible, we also used steps outlined in the SL help page to design the action sequences.
- **CW Problem Reporting Form**: We designed a form that allowed each participant to answer typical CW Yes/No questions, in addition to providing space for them to write down their comments about each step in the action sequence and each task in general. The handouts also include all the tasks we defined and (in case of CW) the action sequence for each task.
- **UI Representation**: For participants in the group sessions, we projected in real-time the UI of an Android phone (Google Nexus 6P) on a large TV screen using a Google Chromecast. This was done so that all the participants can see on the screen the task being carried out and the corresponding UI. For think-aloud sessions, we handed the same Android smartphone to participants.

B COGNITIVE WALKTHROUGH HANDOUT

Consent: Please read the consent form carefully and sign it before starting with the study. Feel free to ask any questions you might have.

Task scenario: You just heard about Android's Smart lock feature, you want to explore it and set it up for use on your mobile device.

Instructions: For each Action Sequence below:

- Look at the UI on the TV and pretend to do the action and ask yourselves Q1-Q4; write down Yes/No
- If answer is No for any question:
  - Write down the problem (Possible solutions if you have ideas)
  - Then assume it's fixed; go on to next step

Answer these question after you've gone through all the action sequences:

- What do you think Smart Lock is supposed to do? What is it good for?
- How do you think each of the smart lock methods (On-body detection, Trusted devices, Trusted places, Trusted face and Voice match) function?

In the end, please write any comments or suggestions you have regarding this study, the Smart Lock functionality or the UI.

Questions:

- **Q1**: Will the user try to achieve the right action? (Does the user know what to do?)
- **Q2**: Will the user notice that the correct action is available? (Is the action e.g menu/button/... visible to the user?)
- **Q3**: Will the user associate the correct action with the effect that the user is trying to achieve? (Does the action have good labeling and suitable signifiers?)
- **Q4**: If the correct action is performed, will the user see that progress is being made toward solution of the task? (Will the user understand the system's response? Is the feedback understandable? And will the interpretation be correct?)

Action sequence for opening Smart Lock settings:

(1) Click on "Settings" on your smart phone
(2) Click on "Lock screen and security"
(3) Click on "Smart Lock"
(4) Draw the current security pattern

Action sequence for enabling On-Body Detection:

(1) Open Smart Lock settings
(2) Click on "On-body detection"
(3) Slide the slider to "On" for Task 1 or to "Off" for Task 2
(4) Click on "Continue" (Only for Task 1)
(5) Click on the "Back arrow"
(6) Click the "Home" button

Action sequence for adding a new trusted place:

(1) Open Smart Lock settings
(2) Click on "Trusted Places"
(3) Click on "Add Trusted Place"
(4) Select a location
(5) Click on the "Back arrow"
(6) Click the "Home" button

Action sequence for deleting a previously added trusted place:

(1) Open Smart Lock settings
(2) Click on "Trusted Places"
(3) From the list of locations, click on the one you want to delete
(4) Click on "Delete"
(5) Click on the "Back arrow"
(6) Click the "Home" button

Action sequence for adding a new trusted device:

(1) Open Smart Lock settings
(2) Click on "Trusted Devices"
(3) Click on "Add Trusted Device"
(4) Choose a device
(5) Click on the "Back arrow"
(6) Click the "Home" button

Action sequence for deleting a previously added trusted device:

(1) Open Smart Lock settings
(2) Click on "Trusted Devices"
(3) From the list of devices, click on the one you want to delete
(4) Click on "Remove Trusted Device"
(5) Click on the "Back arrow"
(6) Click the "Home" button

Action sequence for adding trusted face:

(1) Open Smart Lock settings
(2) Click on "Trusted Face"
(3) Click on "Setup"
(4) Click on "Next"
(5) Hold your face inside the circle drawn on screen
(6) Click on "Done"
(7) Click on the "Back arrow"
(8) Click the "Home" button

Action sequence for improving trusted face detection:

(1) Open Smart Lock settings
(2) Click on "Trusted Face"
(3) Click on "Improve face-matching"
(4) Click on "Next"
(5) Hold your face inside the circle drawn on screen
(6) Click on the "Back arrow"
(7) Click the "Home" button

Action sequence for deleting trusted face:

(1) Open Smart Lock settings
(2) Click on "Trusted Face"
(3) Click on "Remove trusted face"
(4) Click on "Remove"
(5) Click the "Home" button

Action sequence for enabling Voice Match:

(1) Open Smart Lock settings
(2) Click on "Voice Match"
(3) Slide the slider for "Say 'Ok Google' any time"
(4) Click on "Next"
(5) Say "Ok Google" three times
(6) Click on "Yes, I'm in"
(7) Draw the security pattern
(8) Click on the "Back arrow"
(9) Click the "Home" button

Action sequence for deleting voice match:

(1) Open Smart Lock settings
(2) Click on "Voice Match"
(3) Click on "Delete voice model"
(4) Click on "Ok"
(5) Click on the "Back arrow"
(6) Click the "Home" button

Followup Questions:

(1) What do you think Smart Lock is supposed to do? What is it good for?
(2) How do you think each of the smart lock methods (On-body detection, Trusted devices, Trusted places, Trusted face and Voice match) authenticate you?
(3) Please write any comments or suggestions you have regarding this study, the Smart Lock functionality or the UI.

C THINK-ALOUD HANDOUT

Consent: Please read the consent form carefully and sign it before starting with the study. Feel free to ask any questions you might have.

Task scenario: Imagine that you just heard about Android's Smart lock feature, you want to explore it and set it up for use on your mobile device. Note that the we are evaluating the system, not you. As such, there is no right or wrong answer for any of the questions asked. Follow your intuition whenever you are in doubt.

Instructions:

- For each task:
  (1) Perform each task using the phone that is temporarily handed out to you.
  (2) Speak your thoughts about the functionality, look and feel, difficulties, possible changes to improve the user interface, or any other aspect of the experience out loud as you are interacting with the phone.

(3) Remember to return to phone's home screen after you finish each task.

- Answer additional questions presented after each set of tasks.
- After going through all the tasks, answer the follow-up questions on the last page of the handout.

On-body detection tasks:

(1) Open "Smart Lock" settings.
(2) Enable "On-Body detection".

On-body detection questions:

(1) In general, when does "On-Body detection" unlock your phone?
(2) In general, when does "On-Body detection" lock your phone?

Trusted places tasks:

(1) Add current location as a "Trusted place".
(2) Remove current location as a "Trusted place".

Trusted places questions:

(1) In general, when does "Trusted places" unlock your phone?
(2) In general, when does "Trusted places" lock your phone?

Trusted devices tasks:

(1) Add "Mi Band 2" as a trusted device to unlock the phone.
(2) Remove "Mi Band 2" as a "Trusted device" to unlock the phone.

Trusted devices questions:

(1) In general, when does "Trusted devices" unlock your phone?
(2) In general, when does "Trusted devices" lock your phone?

Trusted face tasks:

(1) Add your face as the "Trusted face" to unlock the phone.
(2) Improve the accuracy of face detection.
(3) Remove your face as the "Trusted face" to unlock the phone.

Trusted face questions:

(1) In general, when does "Trusted face" unlock your phone?
(2) In general, when does "Trusted face" lock your phone?

Voice Match tasks:

(1) Add your voice as the trusted voice to unlock the phone.
(2) Remove your voice as the trusted voice.

Voice Match questions:

(1) In general, when does "Voice Match" unlock your phone?
(2) In general, when does "Voice Match" lock your phone?

Followup Questions:

(1) In 2-3 sentences, tell us what you think Smart Lock feature it good for.
(2) Would you consider using any of the following Smart Lock methods on a regular basis? Please explain in 1-2 sentences.
(3) Please write down any comments or suggestions you have regarding this study, the Smart Lock functionality or the Smart Lock UI.

D SURVEY QUESTIONS

Demographics

(1) What is your age?
(2) What is your gender?
(3) What is the highest level of education you completed?
(4) What is your current occupation?
(5) What is your ethnicity?

Smartphone Usage:

(1) What is the model number of your phone?
(2) On average, how many hours do you spend on your phone each day?
(3) Which of the following unlocking methods do you use on your phone?
   - PIN / Password
   - Fingerprint
   - Face detection
   - Iris scanning
   - None
(4) On average, how frequently do you unlock your phone?

Smart Lock Intro:

(1) Please watch the video below about"Smart Lock for Android."

Smart Lock Familiarity

(1) Prior to taking part in this study, how familiar were you with Smart Lock for Android?
   - I had no idea what Smart Lock was and how it worked.
   - I knew what Smart Lock was, but didn't know how it worked.
   - I knew what Smart Lock was, and had some idea as to how it worked.
   - I knew what Smart Lock was, and had a good understanding of how it worked.
(2) If you knew about Smart Lock prior to this study, how did you learn about the existence of Smart Lock?
   - I didn't know about Smart Lock before this study.
   - Through notification about Smart Lock on my phone.
   - Through browsing in the settings menu on my phone.
   - On the internet.
   - Through friends and family.
   - Other (please specify).
(3) For each Smart Lock method (On-body Detection, Trusted Places, Trusted Devices, Trusted Face, and Voice Match), please select an option which best describes your past or potential experience with Smart Lock:
   - Never used it, and would not use even if it were available on my phone.
   - Never used it, but would use if it were available on my phone.
   - Experimented with it, but never fully set it up and used it.
   - Used it for a while, but stopped using it.
   - Am currently using it.
   - I don't know what this means.

On-Body Detection:

(1) (Only if willing to use or are using) Previously, you answered that either you are using or would use On-Body Detection. Why did you choose so? Rank the options below in order of importance to you (with 1 being the most important):
   - It is secure.
   - It makes unlocking the phone easier for me.
   - It provides an additional way of unlocking my phone.

- It makes unlocking the phone faster.
- Other [can add reason].

(2) (Only if not willing to use or experimented but did not set up) Based on your previous answers, you decided not to use On-Body Detection. Why did you choose so? Rank the options below in order of importance to you (with 1 being the most important):
- It is not secure (a.k.a., can be tricked into unlocking the phone).
- It might cause accidental unlocks and pocket dialling.
- I don't think it makes unlocking easier for me.
- I don't understand how it works.
- Other [can add reason].

(3) (Only if were using before but stopped) Based on your previous answers, you were using On-Body Detection before, but have stopped. Why did you choose so? Rank the options below in order of importance to you (with 1 being the most important):
- It was not secure (a.k.a., could be tricked into unlocking the phone).
- It caused accidental unlocks and pocket dialling.
- I didn't make unlocking easier for me (a.k.a., wasn't useful).
- I didn't understand how it worked.
- I found my phone to be locked when I expected it to be unlocked or vice versa.
- I changed phones.
- Other [can add reason].

(4) (Only if were using before but stopped) For how long were you using On-Body Detection before stopping?

(5) (Only if were using before but stopped) When did you stop using On-Body Detection?

(6) (Only if using) For how long have you been using On-Body Detection?

Trusted Places:

(1) (Only if willing to use or are using) Previously, you answered that either you are using or would use Trusted Places. Why did you choose so? Rank the options below in order of importance to you (with 1 being the most important):
- It is secure.
- It makes unlocking the phone easier for me.
- It provides an additional way of unlocking my phone.
- It makes it easier for me to share my phone with others.
- It makes unlocking the phone faster.
- Other [can add reason].

(2) (Only if not willing to use or experimented but did not set up) Based on your previous answers, you decided not to use Trusted Places. Why did you choose so? Rank the options below in order of importance to you (with 1 being the most important):
- It is not secure (a.k.a., can be tricked into unlocking the phone).
- It might allow my family members or co-workers to access my private information.
- It might cause accidental unlocks and pocket dialling.
- I don't understand how it works.
- I don't think it can make unlocking the phone easier for me.
- I can't think of a place to add as a trusted place.
- Other [can add reason].

(3) (Only if were using before but stopped) Based on your previous answers, you were using Trusted Places before, but have stopped. Why did you choose so? Rank the options below in order of importance to you (with 1 being the most important):
- It was not secure (a.k.a., could be tricked into unlocking the phone).
- It caused accidental unlocks and pocket dialling.
- I didn't make unlocking easier for me (a.k.a., wasn't useful).
- I didn't understand how it worked.
- I found my phone to be locked when I expected it to be unlocked or vice versa.
- I changed phones.
- Other [can add reason].

(4) (Only if were using before but stopped) For how long were you using Trusted Places before stopping?

(5) (Only if were using before but stopped) When did you stop using Trusted Places?

(6) (Only if using) For how long have you been using Trusted Places?

Trusted Devices:

(1) (Only if willing to use or are using) Previously, you answered that either you are using or would use Trusted Devices. Why did you choose so? Rank the options below in order of importance to you (with 1 being the most important):
- It is secure.
- It makes unlocking the phone easier for me.
- I provides an additional way of unlocking my phone.
- It makes it easier for me to share my phone with others.
- Other [can add reason].

(2) (Only if not willing to use or experimented but did not set up) Based on your previous answers, you decided not to use Trusted Devices. Why did you choose so? Rank the options below in order of importance to you (with 1 being the most important):
- It is not secure (a.k.a., can be tricked into unlocking the phone).
- It might allow my family members or co-workers to access my private information.
- It might cause accidental unlocks and pocket dialling.
- I don't understand how it works.
- I don't think it can make unlocking the phone easier for me.
- I can't think of a Bluetooth device to add as a trusted device.
- Other [can add reason].

(3) (Only if were using before but stopped) Based on your previous answers, you were using Trusted Devices before, but have stopped. Why did you choose so? Rank the options below in order of importance to you (with 1 being the most important):

- It was not secure (a.k.a., could be tricked into unlocking the phone).
- It caused accidental unlocks and pocket dialling.
- I didn't make unlocking easier for me (a.k.a., wasn't useful).
- I didn't understand how it worked.
- I found my phone to be locked when I expected it to be unlocked or vice versa.
- I changed phones.
- Other [can add reason].

(4) (Only if were using before but stopped) For how long were you using Trusted Devices before stopping?

(5) (Only if were using before but stopped) When did you stop using Trusted Devices?

(6) (Only if using) For how long have you been using Trusted Devices?

Smartphone Unlocking Convenience, Speed and Security:

(1) Please rank the following screen unlocking methods in order of how convenient you think they make smartphone unlocking: (With 1 being the most convenient)
- PIN / Password / Pattern Unlock
- Fingerprint
- On-Body Detection
- Trusted Places
- Trusted Devices
- Trusted Face
- Voice Match

(2) Please rank the following screen unlocking methods in order of how fast you think they make smartphone unlocking: (With 1 being the fastest)
- PIN / Password / Pattern Unlock
- Fingerprint
- On-Body Detection
- Trusted Places
- Trusted Devices
- Trusted Face
- Voice Match

(3) Please rank the following screen unlocking methods in order of how secure you think they make smartphone unlocking: (With 1 being the most secure)
- PIN / Password / Pattern Unlock
- Fingerprint
- On-Body Detection
- Trusted Places
- Trusted Devices
- Trusted Face
- Voice Match