It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception

Marian Harbach[1], Emanuel von Zezschwitz[2], Andreas Fichtner[2],
Alexander De Luca[2], Matthew Smith[3]
[1]Usable Security and Privacy Lab, Leibniz University Hannover, Hannover, Germany
[2]Media Informatics Group, University of Munich (LMU), Munich, Germany
[3]Department of Computer Science, Rheinische Friedrich-Wilhelms-Universität, Bonn, Germany
harbach@dcsec.uni-hannover.de, emanuel.von.zezschwitz@ifi.lmu.de,
fichtnera@cip.ifi.lmu.de, alexander.de.luca@ifi.lmu.de, smith@cs.uni-bonn.de

ABSTRACT

A lot of research is being conducted into improving the usability and security of phone-unlocking. There is however a severe lack of scientific data on users' current unlocking behavior and perceptions. We performed an online survey ($n = 260$) and a one-month field study ($n = 52$) to gain insights into real world (un)locking behavior of smartphone users. One of the main goals was to find out how much overhead unlocking and authenticating adds to the overall phone usage and in how many unlock interactions security (i.e. authentication) was perceived as necessary. We also investigated why users do or do not use a lock screen and how they cope with smartphone-related risks, such as shoulder-surfing or unwanted accesses. Among other results, we found that on average, participants spent around 2.9 % of their smartphone interaction time with authenticating (9 % in the worst case). Participants that used a secure lock screen like PIN or Android unlock patterns considered it unnecessary in 24.1 % of situations. Shoulder surfing was perceived to be a relevant risk in only 11 of 3410 sampled situations.

1. INTRODUCTION

Current mobile devices are touch-based, rich in functionality and provide high memory capacity. While early devices needed key locking mechanisms solely to prevent accidental use, current smartphones require protection mechanisms due to the potentially vast amount of private data contained on the phone. As a consequence, authentication on mobile devices has become indispensable and more secure (un)lock screens were introduced. Besides traditional alphanumeric passwords and PINs, current smartphones provide graphical as well as biometric authentication mechanisms.

Research concerning mobile authentication is also very active. One of the most cited dangers for smartphone unlocking mechanisms are shoulder surfing attacks (e.g. [3, 23, 28]). That is, direct observations with and without technical equipment (e.g. camera) aiming to capture a user's password. Based on this assumption, most proposed unlock mechanisms pay particular attention to being resistant against shoulder surfing and consequently accept reduced usability (e.g. [2, 9, 20]).

Interestingly, even though shoulder surfing is often assumed to be a relevant real-world problem, there is almost no data on the occurrence of shoulder surfing attacks in the wild or on users' perceptions of the threat. Furthermore, since lock screen mechanisms are often tested in lab environments, little is known about the users' perceptions and their behavior in real-world situations. Amongst others, important research questions are: How often and in which situations do people use secure lock screens? How often and in which context do people access sensitive data using their phone? How often is this data perceived to be in danger? And to what extent is shoulder surfing perceived to be an issue in everyday mobile device authentication?

To shed light on these questions, we conducted an online survey (n=260) and a field study (n=52), analyzing users' risk perception and behaviors when interacting with smartphone unlock mechanisms. We gathered in-depth insights into the assessment of shoulder-surfing risks and shed light on users' perceptions and daily needs when protecting their smartphone. Our approach allows us to provide a quantitative analysis of real-life unlocking behavior.

Some of our key findings are that users spend up to 9.0 % of the time they use their smartphone on dealing with unlock screens, that a secure lock screen is considered unnecessary in 24.1 % of the situations we sampled, and that shoulder surfing is only perceived to be a relevant risk in 11 of 3140 sampled situations. We also show a very diverse set of justifications for (not) having a secure lock screen, a plethora of physical measures users take to protect their phone, and that losing the smartphone-hardware is the most relevant threat to users.

We believe that the understanding gained from our studies needs to play an important role in the design of future unlocking mechanisms, since the usability/security trade-offs of current mechanisms do not match users' concerns.

2. RELATED WORK

There are two main areas of related work relevant to this paper. We will first outline the very active field of smartphone lock screen research to motivate the need for ground truth on the threats users face in their daily lives. Then, we

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11, 2014, Menlo Park, CA.

discuss existing work on the perception of security measures as well as existing data on the use of security measures on smartphones.

2.1 Unlock Screens

Authentication on mobile devices can be divided into implicit (e.g. [17]) and explicit approaches (e.g. [32]). In addition, there are mixed approaches (e.g. [7]) which add implicit security layers to an explicit authentication challenge. Implicit authentication mechanisms analyze specific time spans of behavioral cues like sensor data and usage patterns to establish a continuous authentication and hence reduce authentication workload. Examples include analyzing gait patterns [30], typing behavior [5], file system access [33], or a combination of factors [26]. Due to noticeable delays, many of them are not suited for direct lock screen mechanisms. Explicit authentication methods can be divided into biometric, token-based and knowledge-based methods [25]. The latter face the threat of shoulder surfing attacks [23].

As a consequence, the goal of finding shoulder surfing resistant solutions for knowledge-based unlock screens has become a very active research area (e.g. [3, 23, 28, 31]). Proposed concepts achieve shoulder surfing resistance either by establishing secret channels [2], by utilizing indirect input [9, 8, 20, 21], by obfuscating the input [34], or by adding additional biometric layers [7, 29].

Developing usable authentication mechanisms, which are secure against attacks such as shoulder surfing is believed to be very important. Nevertheless, to date there is no evidence that the often postulated threat of shoulder surfing attacks holds true in the users' daily lives. All of the above works were evaluated in laboratory settings and established concepts like PIN or patterns solely serve as a baseline. User perception and field performance (even of PIN and patterns), however, remain relatively unexplored. The only published work in this area focused on a quantitative performance analysis of PIN and patterns, but did not analyze real lock screen interactions [32].

Karlson et al. [18] already argued for better support of phone sharing through non-binary locking mechanisms. Prototypes of context-aware or selective authentication mechanisms for smartphones have also been proposed by Hayashi and colleagues [12, 13]. They report being able to reduce the number of authentications by up to 68 %. To date, however, there is only limited data on how these mechanisms relate to users' needs during their everyday smartphone use and which factors drive users' decisions for or against an authentication mechanism. We provide further evidence for the advantages these approaches can have, not only with respect to user workload but also to reduce the attack surface for shoulder surfers.

2.2 Security Perception and Smartphone Use

The core principle of usable security is that security is not the primary goal for regular users of computer systems [27]. Work by Beautement et al. [1] as well as Herley [14] investigated the notion of the "compliance budget" in corporate environments. According to this theory, users have a limited budget for complying with security measures and will evaluate if it is worth spending some of their budget given a particular benefit of a measure. The authors argue that users make a rational choice in rejecting the considerable number of available protection measures given a general lack of tangible benefits. However, the theories presented in these papers do not take the changing context of mobile phone use into account, where users may want to have a protection measure in one situation but not the other.

There also have been several non-academic studies that report how frequently users interact with their smartphones. For example, a study by lock screen advertising provider Locket finds that the users of their app unlock their phones 110 times a day on average[1]. In a recent market research study by Nielsen[2], researchers found that smartphone users in the UK spent almost 42 hours interacting with their smartphones in December 2013. This figure was somewhat smaller in the U.S. (34.3 hours) and Italy (37.2 hours).

3. ONLINE SURVEY

To begin to understand how users think about smartphone locking, we conducted an online survey. The aim of the survey was to get an overview of users' concerns and motivations for locking or not locking their devices. Research questions included: Why do or do not users lock their phone? Which factors play a role in their decision making about this security measure? Which kinds of attack scenarios do users consider? Are users more afraid to lose their phone in general or that someone will actually access their data? Are there any additional measures that users frequently take to protect their phones and how do these relate to having a lock screen or not?

3.1 Method

We used Amazon's Mechanical Turk (MTurk) service to distribute the survey. While MTurk does not allow us to draw representative samples of any population, the people that participate in this service have been shown to generate meaningful results in the area of usable security [19] if appropriate precautions are taken [10]. We advertised a survey about smartphone use in daily life and offered $0.70 of compensation per successfully completed task. We asked participants to only take the survey if they have been using a smartphone regularly for at least three months. They had to prove their ownership of a smartphone at the end of the survey by scanning a QR code with their device and opening the contained link in their phone's browser. The completion code was only displayed, if the HTTP user agent string matched a known mobile browser. Additionally, we included several attention check questions throughout the survey.

The survey consisted of four main parts. First, participants were asked about their smartphone use in general, including why they do or do not use a code to lock their phone and which lock screen they use. In the second part, we captured how participants value their smartphone and which risks they consider when reasoning about their phone's security. Next, we asked participants about extra measures they take to protect their phone and in which situations they take them. In the third part, participants were asked whether or not they previously had security related incidents with their smartphone. If they indicated that someone previously had unwanted access to their smartphone, we invited them to

[1]http://www.npr.org/blogs/alltechconsidered/2013/10/09/230867952/new-numbers-back-up-our-obsession-with-phones – accessed on 07.05.14

[2]http://www.nielsen.com/us/en/newswire/2014/how-smartphones-are-changing-consumers-daily-routines-around-the-globe.html – accessed on 26.02.14.

report on the most severe case, using the critical incident technique [11]. In the last part, we collected demographics and IT experience. The questionnaire can be found in Appendix A.

We used open-ended questions to ask about extra measures, the reasons why participants do (not) lock their phone, as well as critical incidents. While there were too few critical incidents reported to justify coding, we coded the reasons and extra measures using an inductive coding approach. Two of the authors independently went through the answers and created codes. To capture as many facets of participants' answers as possible, codes did not represent complete responses, but certain common aspects, such as protection goals or likely attackers. The codeplans were then discussed and merged before both authors coded all responses, assigning multiple codes to each response. Conflicting codings were again discussed and resolved before a third coder independently coded all responses again using an improved codeplan. The final round of coding yielded no more conflicts. The final codeplan can be found in Appendix B.

3.2 Participants and Results

After pretesting the survey in the lab and on MTurk, 320 workers accepted the task in November 2013. We removed 60 response sets due to incorrect completion codes (i. e. the smartphone check failed), implausible timing, or wrong answers to two or more attention check questions. The demographics are summarized in Table 1. The participants indicated high IT expertise. Almost a quarter worked in or studied IT and 39.6 % reported the highest value when asked to rate their understanding of computers and the Internet. All indicated that they use their smartphones on a daily basis with the majority using them at least once per hour. Mobile operating systems were evenly split between iOS and Android. 51.2 % of participants indicated that they have suffered from a smartphone related incident before.

Overall, 42.7 % of participants indicated that they use some form of lock screen, including PINs, passwords or unlock patterns, but not including the "slide-to-unlock" mechanism. In the remainder of the paper, this will be referred to as "code-lock". Split by operating systems, 55.2 % of iOS users were significantly more likely to have a code-lock compared to only 30.4 % of Android users (Fisher's Exact Test (FET), $p < .001$). Of the 22 Android pattern users, only 2 had made the lines between the dots invisible.

3.2.1 Locking Behavior

We asked the 111 users that use a code-lock, how frequently they think they unlock their phone on an average day. Answers ranged from 1 to 100 with a median of 20 and a mean of 24.3 times. Our field study will show that many participants significantly underestimate their phone use. Additionally, we asked these 111 users to rate their sentiments towards locking on a 5-point scale. 64.9 % were not or mostly not concerned that someone might be shoulder-surfing their code entry. 25.5 % somewhat or fully agreed that they desire an easier way of unlocking their phone, while 69.4 % somewhat or fully agreed that unlocking their phone is easy. Yet, 46.8 % also somewhat or fully agreed that unlocking their phone can be annoying. At the same time, 95.5 % somewhat or fully agreed that they like the idea that their phone is protected. These results already show a certain ambivalence towards the code-lock mechanism.

N	260	
Age	18 – 67 years	
	median 31 years	
Gender	45.4 %	female
	54.6 %	male
Occupation	50.8 %	full-time employee
	13.1 %	part-time workers
	10.0 %	self-employed
	9.2 %	student
	7.3 %	unemployed
	9.6 %	other
IT Experience	22.7 %	have worked in or studied IT
IT Expertise	39.6 %	very high self-rating
Smartphone Use	36	months (median)
Usage Frequency	79.2 %	hourly or more often
Mobile OS	49.0 %	iOS
	48.7 %	Android
	2.3 %	Other
Lock Screen	40.9 %	Slide-to-Unlock
	33.6 %	PIN
	8.5 %	Pattern
	0.8 %	Password
	16.2 %	None
Incidents	21.5 %	phone lost
	11.9 %	unwanted access
	8.5 %	stolen
	28.5 %	broken phone, lost data

Table 1: Online study participant demographics.

3.2.2 Locking Motivation

When asked why the 111 users with a code-lock chose this protection, answers centered around four topics: protection goals, protection of information, protection in specific scenarios, and protection from attackers. An overview of the 318 code instances we tagged answers with can be found in Table 2. Participants provided a very diverse set of reasons across the four main topics. However, individual participants justified their choice using only few of the available aspects (ranging from 1 to 6 codes per participant, Mdn=1.0). While many answers were unspecific ("to protect my information"), other participants provided well reasoned answers, such as increasing the time an attacker needs to access the data. It is also noteworthy that no participant mentioned protecting login credentials or logged-in accounts directly.

We asked the 149 participants without a code-based lock why they chose not to have any protection mechanism for their phone. Table 3 provides an overview of the 236 code instances we attached to the answers. In this case, answers were mostly centered around two issues, namely inconvenience and the absence of a threat. Answers again included reasonable choices, such as choosing not to have a lock screen because the contained data is not considered sensitive by the respondent, while others were less rational, such as "I don't feel like putting a password on it".

3.2.3 Smartphone Risks

To assess which risks to the content on their phones participants are most concerned about, we asked them to select the worst thing that could happen to their phone from a list of six statements (cf. Appendix A). 52.7 % stated that losing the phone itself is worst as they would have to buy a new one. This result shows that, for many users, the monetary value of the hardware is more important than the associated privacy and security risks for accounts and data. However,

Code	Count
Protection Goal	**88**
– Controlling access to phone	32
– "Safety"/"Security"	25
– "Privacy"	15
– Protection in General	6
– Increasing difficulty of unwanted access	8
– Increasing time to recover/remote-lock phone	1
– Enable data encryption	1
Protect information	**75**
– Information in general	38
– *Private* information in general	14
– Emails/Messages	9
– Photos	4
– Other app-specific content	5
– Confidential (work) information	5
Protect from specific scenario	**62**
– Lost phone	27
– Stolen phone	20
– Unattended phone	8
– Pranks/someone "messing up" phone	5
– Misplaced phone	2
Protect from attacker	**55**
– Unspecific	32
– Unwanted person	11
– Own children	11
– Roommates	1
Other	**38**
– Protect certain action	17
– Mandatory lock screen	6
– Context (work/death)	4
– Other motivation	11

Table 2: Reasons for using a code-based locking mechanism. Bold counts are sums of sub-counts.

such risks were mentioned second-most: 20.0 % chose losing the data that is on the phone in general as the worst possible scenario, while 11.9 % chose account abuse on a lost phone and 8.8 % data abuse on a lost phone. Only 4.2 % and 1.2 % chose app abuse and data abuse respectively on an unattended phone. It has to be noted that lock screens cannot protect devices from getting lost and data loss is usually more influenced by backup strategies than authentication mechanisms. Therefore, 26.1 % of these scenarios could probably be prevented using adequate security mechanisms. The remaining 1.2 % of participants stated a combination of these six scenarios or gave another scenario. While the figures only relate to risks participants were most concerned about, these also likely influence users' behavior most.

Participants were also asked to to rate each of the six worst case smartphone risk scenarios in terms of severity and likelihood, the two classic dimensions applied to evaluate risk. We also included a third dimension, presence, that measures how frequently this risk is on a participant's mind. While the first two dimensions can capture a "value" of this risk, the third attempts to quantify how much this value influences day-to-day decision making. A risk that is considered very important by users is not only one that is particularly severe and likely but also one that is frequently present in the users' minds. In terms of presence, all six risks were on users' minds similarly infrequently: for all six risk scenarios, 65 to 82 % of participants indicated that they think of this risk infrequently or very infrequently. A Friedman's ANOVA across the six scenarios did not yield a significant

Code	Count
Absence of threat	**118**
– don't need security	25
– nothing to hide	23
– no sensitive data	16
– keep phone physically secured	29
– use only in private environments	11
Inconvenience	**85**
– Too annoying	3
– Takes too much time	23
– Use phone too frequently	13
– Mental burden	3
Negligence/Carelessness	**8**
Dislike Locking	**7**
Other	**25**
– locking causes problems	12
– protect phone using another measure	6
– Other reason	7

Table 3: Reasons for not using a code-based locking mechanism. Bold counts are sums of sub-counts.

difference ($\chi^2(5) = 7.74$, $p = .17$). Similarly, the likelihood of the six scenarios happening to oneself was rated as likely or very likely only by 14 to 21 % of participants. Again, these values were not significantly different ($\chi^2(5) = 1.96$, $p = .85$). There was, however, a highly significantly different rating of risks in terms of severity ($\chi^2(5) = 62.17$, $p < .001$): Post-hoc tests with Bonferroni correction revealed that losing the phone and having to replace it was considered more severe than losing data or having unwanted access to the phone. In addition, participants believed that risks to data and accounts are more severe when a phone is lost compared to when the phone is unattended.

We also asked participants to compare their individual smartphone worst case to negative situations in other contexts on a 5-point numerical scale from "not as bad" to "similar" to "worse". The situations comprised losing data on their PC, losing their wallet, losing their home or car keys, getting their e-mail account hacked or someone breaking into their home. Someone breaking into one's home was rated as somewhat worse or worse by a majority of 86.5 %. Losing the key to their home or car was rated as not as bad or similar to the worst case smartphone scenario by 60.0 % and 47.7 % respectively. Also, losing data on their PC was rated as not as bad or similar by 56.2 %. Getting their e-mail account hacked or losing their wallet ranged in between someone breaking in and the three other scenarios. This indicates that users may be ready to invest as much effort into protecting their phones as they are to protect themselves from losing the key to their home or data on their PC.

We then asked participants to rate which kinds of attackers are most likely to attempt unwanted access to their smartphones. They rated four potential attackers, known malicious and known curious as well as unknown malicious and unknown curious, on a 5-point scale from very unlikely to very likely. We found a highly significant difference between the four attackers (Friedman's ANOVA, $\chi^2(3) = 40.07$, $p < .001$) and Bonferroni-corrected post-hoc tests showed that the known curious and the unknown malicious attackers where considered more likely than the two other attackers.

For those participants who rated a known attacker as neutral, likely or very likely, we also asked whether or not they

considered eight types of known persons as a potentially curious or malicious person for their rating. The most frequently chosen types of persons are outlined in Table 4.

Curious Attackers		Malicious Attackers	
Attacker	**Freq.**	**Attacker**	**Freq.**
Close Friends	73.2 %	Other known people	68.9 %
Acquaintances	54.3 %	Co-workers	29.3 %
Parents	53.0 %	Acquaintances	25.0 %
Children	51.8 %	Friends of friends	23.2 %
Friends of Friends	46.3 %		

Table 4: Kinds of persons respondents considered as known malicious or curious attackers.

3.2.4 Extra Measures

To see how participants cope with risks to their smartphone besides inbuilt protection measures, we asked them if they sometimes apply extra measures to protect their phone. 83.5 % indicate that they keep the phone on their person or in their bag, 50.8 % leave the phone in a safe place and 33.5 % enable a lock screen or choose a harder unlock code for certain situations. Furthermore, we asked if participants with code-lock screens take some of five measures against shoulder surfing: 27.7 % indicated that they tilt their screen away while entering their unlock code when shoulder surfing is possible, 16.2 % wait a moment, 11.2 % turn around, 8.8 % cover phone, and only 7.3 % have previously changed their unlock code after a potential shoulder surfing happened. We also prompted participants to give up to three situations in which they apply those measures. As participants often not only listed a situation but also additional measures, we coded these responses for both concepts. We attached 701 instances of situation codes and 248 instances of measure codes, while each answer could receive multiple measure and situation codes. The corresponding codeplans can be found in Appendix B.3 and B.4.

In addition to the protection measures we already asked about, the coded responses revealed that in 45 instances participants mentioned to be paying extra attention to their phone. In 19 instances, other technical measures, such as turning the phone off, encrypting data, relying on remote wiping and locking functionality, removing the memory card or having a backup were quoted. With respect to situations, we found that most participants referred to public or semi-public spaces as situations where they would need extra protection. Examples include being "out" in general (59), going to events or concerts (23), while being at a gym or during workout (42), during parties or in bars (35) or at work (52). A feeling of unfamiliarity or unknown spaces were mentioned in 50 instances as were discomforting spaces, such as dark areas or dangerous neighborhoods (24). However, private spaces, such as a home, were also perceived as situations were extra measures may be necessary (16). Leaving the phone in the car (21) or uncontrolled situations where a phone is left unattended or one is less cautious (102) were frequently mentioned. In addition to unspecific unattended situations (71), participants mentioned leaving the phone to charge, while sleeping or drinking or when bags are handed over for example at the airport. Persons were also often a component of situations that were protected with extra measures (overall 61 instances): unfamiliar or untrusted persons (20), other people in general(15), kids (9), (ex-) partners (4), friends (6), and coworkers (2) were all mentioned. Finally, device sharing (5) or having sensitive and inappropriate data (4) were also quoted as situations were extra measures need to be taken.

3.2.5 Critical Incidents

The 31 participants who reported having been victim of unwanted access before, quoted the following critical incidents during which unwanted access happened: children or siblings accessing the phone for fun, snooping (ex-)partners, friends playing pranks and abusing accounts, a thief acquired the phone, friends snooping on private information, a stolen phone that was sold and then returned to the police by the buyer because the phone was not wiped, parents "checking" on their children, and having a virus on the device. We then explicitly asked about the harm that arose in this situation: ten participants stated an invasion of privacy, four got into a conflict with the other person, accounts were abused in three cases, others were offended in three cases and embarrassment was caused in one case. Seven participants reported that they were frustrated or mad and six participants indicated that they saw no harm in this incident. On the other hand, we asked participants what good came from the incident. Responses included clarified relationships and boundaries in five cases, a new phone in one case, five participants stated to have learned to pay more attention to their phone (even though they are still not locking their phone) and one started using a lock mechanism. For eight participants, nothing good came from the incident. In terms of having a code-lock or not, these critical incidents show that many of them could have been prevented by using a code-lock. However, as the previous subsections have shown, a large number of reasons let users choose not to have a code-lock.

4. LONGITUDINAL FIELD STUDY

While the survey results already provide interesting insights, they are based on self-reports at one point in time. To further evaluate the role of context to unlocking and hence generate ground truth for improvements of smartphone locking schemes, we conducted a longitudinal field study with 57 participants over four weeks. The design of the study was governed by three research questions: How frequently do people unlock their phone? What is the influence of context on perceived necessity of locking? And how frequently are users potentially subject to shoulder surfing or unwanted access to their device?

To increase data validity, we instrumented users' private phones to implement an experience sampling method and gather quantitative data like unlock frequencies and authentication times. The field study was grounded on the results of the online survey and a focus group. We conducted this focus group (n=7) to familiarize ourselves with participants' reasoning and views on our research questions. The results helped us to further reduce the question list to the most important aspects and keep the participants' additional effort as low as possible.

4.1 Method

To elicit a longitudinal picture of users' everyday behavior and perceptions, a subtle and low-effort data collection method was necessary. We decided to collect data from users of the Android OS, as it is both very common and

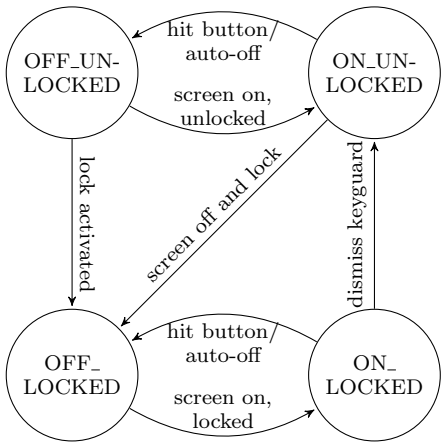

Figure 1: The states and transitions logged during data collection.

provides suitable APIs to collect the desired data. We implemented an app that would automatically log (un)locking activity on users' phones. Additionally, we displayed mini-questionnaires on random occasions to obtain a sample of users' views on their locking behavior immediately and within a given situation (cf. Section 4.1.3 below for details). The logged information was periodically backed up to our servers when the phone was connected to a WiFi network. We collected data over a period of four weeks.

Presenting questionnaires in-situ is known as the experience sampling method (ESM) and has been previously applied to investigate real-life situations [16, 6, 15]. Other longitudinal methods have been used to capture user experience on mobile phones [22], such as the Day Reconstruction Method. However, for our exploration of smartphone locking behavior and perception, we can easily use the capabilities of modern smartphones to collect the necessary data in situ and do not need to let users remember parts of their experience. Additionally, Möller et al. have previously demonstrated problems with relying on self-reporting during long-term studies [24]. We hence split our data collection efforts in two parts: Activity Logging and Mini-Questionnaires. The questionnaires only ask for immediately observable information or information from the near past and hence do not need to heavily rely on participants' memory. We present the details of our approach in the following two subsections.

4.1.1 Activity Logging

Our app monitored SCREEN_ON and SCREEN_OFF intents as well as the KeyguardManager state provided by the Android OS. This allows us to derive when a device was activated, unlocked and deactivated. Figure 1 provides a state-machine representation of the collected state information. Whenever a users presses the hardware button activating or deactivating the smartphone's screen, the state transitions between ON_* and OFF_* states. When the lock screen is dismissed, the system transitions from ON_LOCKED to ON_UNLOCKED. Finally, the transition from *_UNLOCKED to *_LOCKED occurs either immediately or after a certain delay, depending on users' configurations. We logged timestamps when entering a state. It is important to note that especially the time it takes to unlock the phone (transitioning from ON_LOCKED to ON_UNLOCKED) is a worst-case estimate, as it includes the time users spent viewing notifications or the clock on the lock screen first. Also, our app did not need any permissions to collect this data.

4.1.2 Mini-Questionnaires

As we aimed to capture participants' perceptions of threats related to their smartphone locking behavior in their daily life, we enriched the automatically logged data with participants' subjective views. We applied a method similar to what Cherubini and Oliver proposed [4]. Using two very short questionnaires, participants were asked about their surroundings and subjective perceptions. The two questionnaires were randomly displayed with a certain probability after a subset of device unlocks and contained multiple-choice questions to facilitate rapid answering. One questionnaire focussed on the unlock procedure and gathered shoulder surfing possibilities, who an attacker would be, as well as how likely and severe such an attack would be. Participants were instructed to briefly consider their environment and indicate if someone was able to see the contents of their screen in this situation. Additionally, we elicited satisfaction with the locking procedure in this situation and the sensitivity of the data to be accessed. Participants were instructed to judge sensitivity of data subjectively without giving them any further definition in order to not disrupt their own mental model. The second questionnaire focussed on the time span between the current unlock and the last use. This questionnaire elicited views on the necessity of the lock screen, if unwanted access has been possible, and how annoying the locking mechanism was in this situation. Both questionnaires asked participants to characterize the environment they are currently in as private, semi-public or public, according to the categories we obtained in the online survey as well as the pre-study focus group. The contents of both questionnaires can be found in the Appendix C.

4.1.3 Situation Sampling

To obtain a representative sample of day-to-day situations, we needed to randomly choose unlock events throughout the day after which we would display one of the two mini-questionnaires. Pre-testing showed that unlocking behavior varies widely between participants, days, and time of day. We hence dismissed the possibility to apply a fixed sampling schedule for all participants. Some participants may use their device more frequently during the day, while others may become particularly active in the evening. Additionally, we aimed to sample as many different situations as possible and therefore did not want to restrict the sampling time frame to, for instance, working hours as has been previously done in similar contexts [15]. Pre-testing also revealed that it takes about 30 to 40 seconds to complete the mini-questionnaires on the device. In order to not overwhelm participants, one of the two questionnaires would be randomly displayed with a certain probability and at most once per hour. Participants were also able to press a "Not Now" button, that would dismiss this questionnaire immediately, in order to allow quick access to the phone if necessary.

At deployment time, the probability that a questionnaire was shown for a given unlock was set to 20 % based on a one week pre-study. After one week of data collection, probabilities were adjusted to collect about 5 to 6 questionnaires per day to keep the task as unobtrusive as possible while

covering a wide range of situations. Heavy users (at least 9 unlocks per hour) were throttled to 10 % probability and medium users (between 4 and 8 unlocks per hour) to 15 %. We chose to adapt the sampling rates to put an even burden on all participants and make the study less intrusive.

4.1.4 *Briefing and Debriefing*

All participants were briefed about the study and the method during an initial meeting in person or by phone. The data collection procedure and the questions in both questionnaires were explained and participants had a chance to ask questions. The app was then installed on each participant's phone before participants tested both mini-questionnaires. After the data collection period, participants came in for a debriefing interview. We collected the data from participants' phones and removed all traces of the app. We also conducted a short interview, whose structure and results will be presented in Section 4.2.3.

N	52	
Age	19 – 32 years, median 23 years	
Gender	23	female
	29	male
Occupation	47	undergrad or grad students
	5	PhD student or staff
Highest degree	34	high school diploma or less
	18	Bachelor/Master degree
IT experience	25	work(ed) in or study(ed) IT
Smartphone history	34	months (mean)
Lock screen type	13	PIN
	22	Pattern
	17	Slide-to-unlock
Code lock for	22	months (mean)
Avg. PIN length	4.5	digits (range: 4-6)
Avg. Pattern length	5.2	cells (range: 4-8)

Table 5: Longitudinal field study participant demographics.

4.1.5 *Participants*

We recruited 57 participants at two locations in Germany, Hannover and Munich, in January 2014. At one location, 27 participants were recruited through message boards, social networks, and mailing lists, while at the other 30 students and graduates where recruited using a study participation mailing list. We advertised a four week study on Android lock screens for users that have had a smartphone with Android 2.3 or higher for at least 3 months. A 10 Euro base-salary plus 14 Euro-cent per completed mini-questionnaire were promised as compensation. Participants earned 30.79 Euros on average.

While all 57 participants completed the data collection part of the study, we removed one participant who did not show up for debriefing, three participants who repeatedly modified the time on their phone during data collection, and one participant where data collection failed for several days, as our app did not restart after rebooting this user's device. The remaining 52 participants' demographics are summarized in Table 5.

While the participants mainly comprise students of which about half also have some IT experience, we believe that this is a population worth studying as they are often very active experiencing a wide range of situations but also have phases where they sit in front of a desk for extended periods of time. As we aim to explore how different environments influence locking behavior and risk perception, our sample offers a good chance to collect a wide range of usage contexts. However, it still has to be noted that the results cannot be generalized to any particular population.

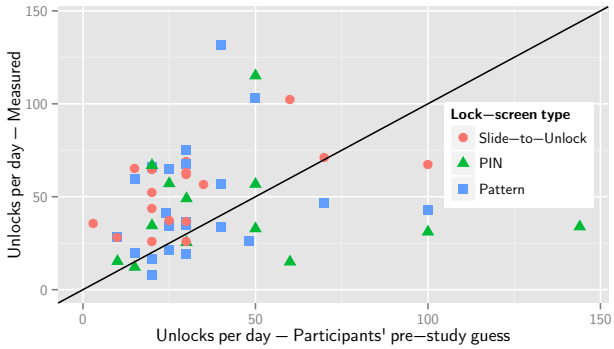

Figure 2: A comparison of participants' pre-study guess of unlocks per day versus the actually measured values.

4.2 Results

Participants contributed 29.5 days of data on average. To equalize the time we analyze per user, we pruned each participants' dataset to 27 complete days from midnight to midnight by removing the first hours and the remaining days. Due to our method, each user contributed a different amount of data. In order to not over-represent users that use their phone more frequently, we first aggregate data per user and then average across users' aggregates where appropriate.

4.2.1 *Logged Data*

Within the 27 days, we observed an average of 2242.3 activations (switching the screen of the device on) per participant (sd = 1160.2, median=2260), ranging from 651 to 5419. Correspondingly, 1286.0 unlocks (dismissing the lock screen after activating the phone) were logged on average per participant (sd = 711.8, median=1127), ranging from 215 to 3545.

Per day, participants activated their phone 83.3 times (sd = 43.0, median=83.8) and unlocked 47.8 times (sd = 26.4, median=42.1) on average. This translates to an average of 5.2 activations and 3.0 unlocks per hour, assuming that a user is awake for 16 hours per day. Participants unanimously attributed the discrepancy between activations and unlocks to activating the screen of their phone to see the current time and to check for notifications. Overall, usage was largely similar during daytime hours, ramping up in the morning and down in the evening after 9 pm (also cf. Figure 8 in the Appendix).

During recruitment, we asked participants how frequently they think they unlock their phone per day. Figure 2 compares these guesses with the measured frequency. We find that most users severely underestimated their use. However, participants who use their phone less frequently appeared to give better estimates.

Figure 3 shows that the distribution of unlocks per hour across users is bimodal. We hence group users into heavy

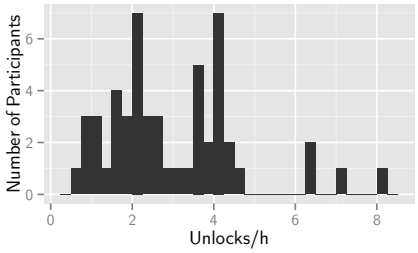

Figure 3: Histogram of users' mean combined activation and unlock times.

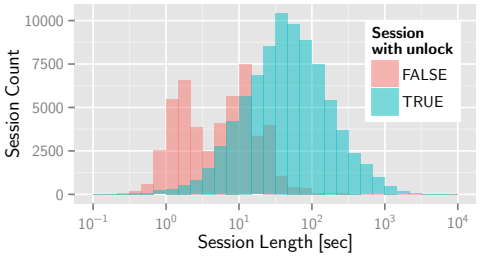

Figure 4: Histogram of session lengths on a log scale.

and "regular" users, where heavy users unlock their phone more than 3 times per hour. Please note that significance testing results based on this grouping are only of exploratory nature, as groups were formed post-hoc.

Activating and unlocking the phone took 2.67 seconds without a code lock (sd = 8.46s, median=1.26s), 3.0 seconds using a lock pattern (sd = 13.3 sec, median=1.69s), and 4.7 seconds using a numeric PIN (sd = 20.72s, median=2.85s) across all unlocks. Averaging unlock times per user, we ran a user-type by lock-type between-subjects ANOVA and found a highly significant main effect for lock-type ($F(2, 46) = 11.37$, $p < .001$) as well as a significant main effect for user-type ($F(1, 46) = 6.39$, $p = .002$). Heavy users completed their unlocks more quickly on average (2.9 vs. 3.8 seconds). Holm-corrected pairwise testing also showed that PIN (4.9 seconds on average) was significantly slower than the two other mechanisms (Slide-to-Unlock 2.6 and Pattern 3.2 seconds, $p < .001$, Cohen's d = 1.58 and 1.27 respectively). During the 27 days of the experiment, participants spent an average of 1.17 hours each (sd = .87, ranging from .2 to 5.1 hours) just unlocking their device. There also was a significant correlation between unlocking time and unlocking frequency (Spearman's $\rho = -.30$, $p = .034$).

An average session (from SCREEN_ON to SCREEN_OFF) lasted 70.3 seconds (sd = 241.5s). However, sessions where participants actually saw the home screen lasted for 104.1 seconds (sd = 193.9s, median=45.6s) on average, including the time it took to dismiss the lock screen. The remaining sessions (those when the device was not unlocked) lasted only 12.4 seconds (sd = 297.6s, median=5.2s) on average. Figure 4 gives an overview of session lengths, grouped by whether or not the session entered the home screen. It can be clearly seen that sessions last longer once the lock screen was dismissed. Also, the distribution of session lengths on a locked device is bimodal. We hypothesize that the maximum at about one second is for checking the time, while the maximum at about 10 seconds session lengths represents cases where users check notifications. Averaging per user, we did not find a significant correlation between unlock frequency and average session time.

Overall, users spent 43.0 hours on average (sd = 22.1h, median=41.2h) using their smartphone within the 27 days of our experiment, of which an average of 2.9 hours were spent on a locked device (i. e. checking time or notifications on the lock screen). 2.9 % of the overall time was related to unlocking the phone on average, ranging from .6 to 9 %.

4.2.2 *Questionnaire Data*

We collected 3410 completed unlock risk questionnaires (65.6 per user on average, range 15-110) and 3172 completed data risk questionnaires (61.0 per user on average, range 15-105). The sampled situations included a wide range of times of day and even collected samples when participants used their phone at night (cf. Figure 8 in the Appendix). Filling the questionnaires took 23.7 (sd = 35.9) and 21.3 (sd = 22.6) seconds on average for each type respectively. In the following, we present results from questionnaire parts individually.

Environments.

In both questionnaires, participants reported the environments in which they were in the moment they unlocked the phone or in which they have been since they last used the phone. Averaging environment proportions per user, these environments were mostly private (62.4 %), semi-public in 19.5 % of cases and public in 18.2 %. In line with previous findings [12], this indicates that most smartphone use takes place at home or in similarly private spaces.

Perception of Lock Screen.

In the first mini questionnaire, we asked participants how annoying the unlock (which they just completed prior to filling out the questionnaire) was. Participants reported different proportions of annoying unlocks (either "annoying" or "very annoying"). Figure 5 shows the relationship between the proportion of annoying unlocks, the number of completed questionnaires (corresponding to how heavily users use their smartphone), and the type of lock screen they use. A large amount of participants was very happy with their lock screen, as they reported no or almost no annoying unlocks across their questionnaires. Only 12 of 52 participants indicated being annoyed by their lock screen in more than 50 % of their mini-questionnaires. There also is no clear trend of users with a particular lock type being more annoyed. However, we note that only three users with Slide-to-Unlock reported annoying unlocks in more than a quarter of their questionnaires.

Additionally, in the other mini questionnaire, we asked if users with a code lock would have rather not have had a code lock in this situation and vice versa. High ratings on the 5-point numeric scale of this question indicate dissatisfaction with having a code lock or not. Figure 6 and Table 6 give an overview of the answers provided. In the figure, the y-axes additionally show how many questionnaires each user completed, approximating how frequently the phone is used.

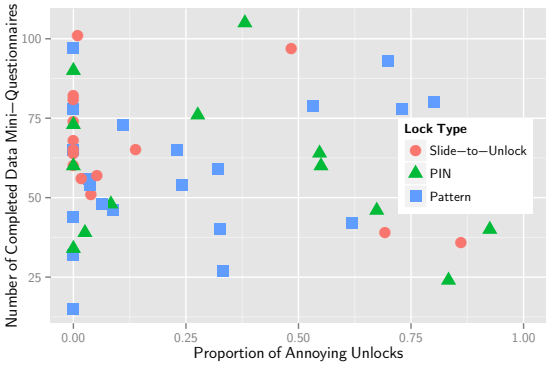

Figure 5: Proportion of annoying unlocks per user versus how many questionnaires were completed.

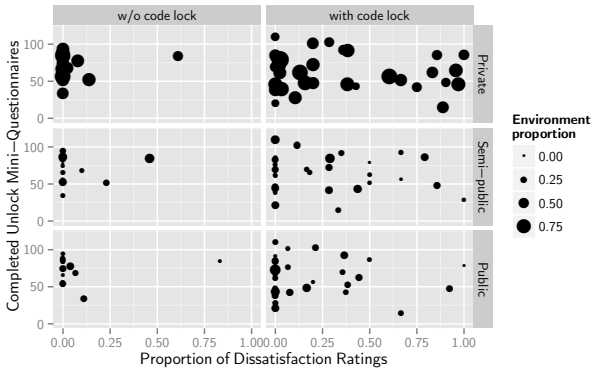

Figure 6: Proportion of dissatisfied ratings per user versus how many questionnaires they completed, grouped by whether they had a code lock screen and in which environment the rating was given.

Participants' answers are grouped by the environment they were provided in and whether or not this participant had a code-lock. The size of each point in the graph indicates how frequently this user reported being in this environment.

The data shows that participants without a code lock were generally more satisfied with their status quo. Only few of them indicated dissatisfaction in more than a quarter of their responses across all environments. Participants with code locks showed more variability and more participants indicated dissatisfaction in more than a quarter of their responses. Especially users that are frequently in private environments were very dissatisfied with their code locks. It is also noteworthy that fewer code-lock participants indicated strong dissatisfaction in public environments compared to semi-public or private situations.

A possible interpretation is that being annoyed by a lock mechanism overlays risk perception to some extent as there is only a limited trend towards more satisfaction with lock screens in potentially more dangerous public situations.

Data Sensitivity.

We asked each participant for subjective ratings on how sensitive the data that is going to be accessed in this session is. In 684 (20.1 %) of 3410 completed mini questionnaires, users indicated that they did not know what kind

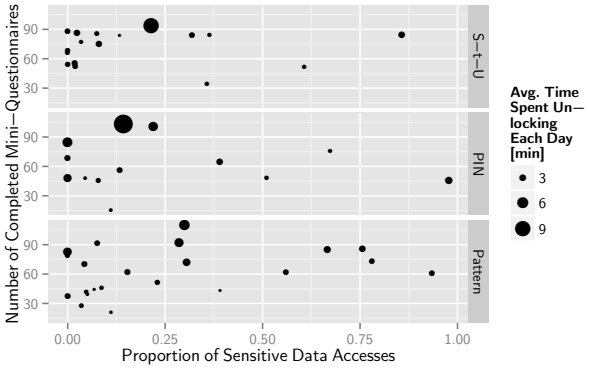

Figure 7: Proportion of sensitive data accesses per user, grouped by lock mechanism. The y-axis also shows completed questionnaires.

of data they were going to access. Aggregating proportions of unknown accesses per participant, the mean proportion amounts to 19.6 % ($sd = 25.0$ %) and participants' individual values range from 0 % to 88.2 %.

In 25.3 % (691) of the 2726 remaining reported situations, participants indicated accesses to sensitive data. For each user, this means that during the experiment only 10.6 hours ($sd = 15.0$) of the 43 hours each participant spent using their device contained accesses to sensitive data on average. All but ten users indicated that they access less sensitive data in more than half of the sampled sessions. Figure 7 visualizes the proportions of sensitivity ratings across the sampled situations per participant. It is also visible that one user spent a lot of time unlocking the phone each day even though the data that should be accessed was not sensitive in most cases. Notably, the ten participants that were accessing most sensitive data use their phone more frequently (i. e. filled more questionnaires).

Shoulder Surfing.

Table 7 gives an overview of shoulder surfing possibilities perceived by our participants. Across the 3410 unlock risk mini-questionnaires we collected, shoulder surfing was not perceived to be possible in a majority of 83.0 % of cases. When it was possible, mostly known persons were observers, except in public environments. In more than half of the situations where shoulder surfing would have been possible, participants thought it to be unlikely or very unlikely that this did actually happen. Had it happened, the threat from the potential attacker would have been low or very low in most of the possible shoulder surfing situations, especially in private environments. Overall, we found only 11 of the 3410 (.3 %) reported situations were it was likely that a shoulder surfer was looking at the screen and it would have been severe or very severe if that had actually taken place. Seven of these occurred in public situations.

We also asked those participants with a code lock whether or not they protected their code entry during the last unlock, by for example tilting their screen away from onlookers or waiting to unlock the phone. Only 18 participants reported 52 instances in which they actively protected the code input from a shoulder surfing threat within 1869 sampled situations where a code was entered (2.8 %).

Environment	# Situations	Mean Proportion of Dissatisfaction Ratings w/o code lock	with code lock	overall
private	2115 (62.0 %)	5.0 % ($sd = 14.9$ %)	32.7 % ($sd = 36.0$ %)	23.6 % ($sd = 33.2$ %)
semi-public	690 (20.2 %)	4.6 % ($sd = 12.2$ %)	23.0 % ($sd = 29.3$ %)	17.0 % ($sd = 26.3$ %)
public	605 (17.7 %)	6.2 % ($sd = 20.1$ %)	16.6 % ($sd = 26.9$ %)	13.2 % ($sd = 25.2$ %)
Overall	3410	5.3 % ($sd = 15.8$ %)	24.1 % ($sd = 31.4$ %)	17.9 % ($sd = 28.6$ %)

Table 6: Participants' dissatisfaction with their locking mechanisms by environment.

Environment	# Situations	Known Person	Unknown Person	Nobody	Unlikely	Low Severity
private	2115 (62.0 %)	8.6 % (181)	0.0 % (1)	91.4 % (1933)	56.6 % (103)	92.9 % (169)
semi-public	690 (20.2 %)	22.2 % (153)	4.6 % (32)	73.2 % (505)	65.4 % (121)	84.9 % (157)
public	605 (17.7 %)	10.4 % (63)	24.5 % (148)	65.1 % (394)	56.0 % (118)	68.3 % (144)
Overall	3410	11.6 % (397)	5.3 % (181)	83.0 % (2832)	59.2 % (342)	81.3 % (470)

Table 7: Shoulder surfing possibilities across potential "attackers" and environments. The last two columns give percentages with respect to possible shoulder surfing attempts (i. e. by known or unknown persons).

Unwanted Access.

In the data risk mini-questionnaire, participants were asked to report situations in which unwanted access to their smartphone was possible. Eleven participants did not report any of these situations and the remaining 42 participants reported a total of 245 occasions out of 3172 possibilities (7.7 %) and between one and twenty occasions each. Table 8 provides an overview of unwanted access occasions, who an attacker would have been, how many of these occasions were rated as unlikely and for how many the consequences participants saw were rated as benign. Unwanted accesses were infrequently possible, mostly by known persons except in public situations and rated as mostly unlikely and benign.

4.2.3 Debriefing Interview

During the debriefing sessions, we asked if participating in the study or seeing the questionnaires influenced participants' smartphone use. One participant reported to have increased the time interval after which the lock screen is shown again from 30 to 90 seconds, another participant stated that he sometimes did not turn his screen off immediately. Three participants stated that they may have used the device a little less frequently at the beginning of the study. Ten participants said that being part of the study made them pay more attention to why and how often they use their phone. While it made them realize their usage, they reported not to have altered their behavior. One participant said that he may remove his code-lock after the study, as participating made him realize how much effort unlocking with a PIN takes.

Participants were also asked to rate how annoying they found answering the mini-questionnaires to be. Only 5 participants selected 4 on a numeric scale from not annoying at all (1) to very annoying (5). 43 participants chose 2 or 3 and an additional 4 chose not annoying at all. On the contrary, many users reported that they found participating in the study very interesting for themselves, as it helped them assess their own behavior better. We also presented participants with a summary of the data they had shared with us, including frequencies of logged events, general usage statistics as well as overviews of mini-questionnaire answers. Most participants found these figures to be interesting and sometimes alarming, as they would not have expected to activate or unlock their phone as frequently. We also gave participants a numeric scale asking how well the collected data represents their actual behavior (logged data) and perception (questionnaire answers) from "not at all" (1) to "very much" (5). Participants felt that the data was valid: only one participant chose 3, 31 chose 4, and 20 chose 5.

To see how well the sampled situations covered participants' daily lives, we asked them if there were additional situations in which unwanted access was possible and if so of which nature those were. Several participants said that there probably were more of these situations, but they were mostly the same as the ones they reported in the sampled situations. Similarly, we asked participants if the proportion of situations where shoulder surfing was possible matched their own perception. Participants agreed that the numbers we collected and the proportion of shoulder surfing situations match their perception beyond the situations were questionnaires were shown. However, several participants mentioned that there were brief situations mostly in public environments where shoulder surfing would have been possible but no questionnaire was shown.

As in the online survey, we asked participants about previous critical incidents with their smartphone. Four participants had lost their smartphone before and two had unwanted access. In all cases, a lock screen was helpful to prevent more damage or was activated after the incident.

We also asked participants why they chose to have a lock mechanism with a code and coded results using the codes from the online survey. The 37 participants' answers contributed 115 code instances summarized in Table 9. The results are similar to the online survey with the exception that several participants also gave restricting statements, noting that they do not believe that lock screens offer perfect security (7), that they do not really need security (6), or that others know their code anyway (3).

Again, participants without code locks also justified their choice and 15 participants contributed 44 code instances. Table 10 provides an overview of the reasons. The most frequently cited reasons for not using a lock, as in the online survey, are inconvenience and not seeing a threat.

Finally, we asked how sensitive participants consider the data on their smartphones and whether or not they share their code with other people. 22 participants (42.3 %) chose sensitive or very sensitive on a 5-point scale, while 23.5 % of users without a code-lock and 48.6 % of users with such a

Environment	# Situations	Known Person	Unknown Person	Unlikely	Benign Cons.
private	131 (53.5 %)	97.7 % (128)	2.3 % (3)	92.4 % (121)	86.3 % (113)
semi-public	75 (30.6 %)	70.7 % (53)	29.3 % (22)	93.4 % (70)	64.0 % (48)
public	39 (15.9 %)	23.1 % (9)	76.9 % (30)	79.5 % (31)	18.2 % (11)
Overall	245 (7.7 %)	77.6 % (190)	22.4 % (55)	90.6 % (222)	70.2 % (172)

Table 8: Unwanted access occasions by environments and potential attackers. The last two columns give percentages of likelihood and severity of consequences with respect to reported unwanted access occasions.

Code	Count
Specific protection goal	13
Unspecific protection goal ("Security")	12
Specific attacker	13
Unspecific attacker	10
Protect from specific scenarios (e.g. lost, stolen)	20
Protecting specific information	5
Protecting unspecific information	8
Protect from accidental input	4
Custom certificate	5

Table 9: Reasons for using a code-based locking mechanism of field study participants.

Code	Count
Inconvenience	17
Absence of threat	16
Locking causes problems	6
Protect phone using another measures	4
Not secure anyway	2

Table 10: Reasons for not using a code-based locking mechanism of field study participants.

mechanism considered the data on their smartphones to be sensitive. However, this difference is only almost statistically significant (FET, $p = .076$). Unlock codes were shared with at least one person by 28 of 35 participants with a code-lock. Six participants indicated that at least 5 other people know their code. This also indicates that code-based locking mechanisms can be problematic in device sharing situations, as already noted by Karlson et al. [18].

5. DISCUSSION

In the two previous sections, we presented results from two studies, which we summarize and discuss grouped by the most important observations in the following sections.

5.1 High Number of Unlocks

36 of 52 participants underestimated the number of smartphone unlocks by 141 % on average. This indicates that unlocking is a subliminal action in many cases and unlock effort is kept low enough most of the time. However, even if a single unlock took only between 2.67 seconds (slide to unlock) and 4.7 seconds (PIN), the huge number of daily unlocks leads to a high impact of every additional second. Just over the course of our experiment, participants on average already spent about one hour unlocking their devices using traditional unlock screens. Taking into account that alternative authentication mechanisms often incur higher input times for increased security, this can easily add several hours of additional unlock time per month. This is especially critical when considering that average usage times per activation are relatively short and shows that authentication speed of feasible systems must be about as fast as PIN and patterns.

Since out data indicates that unlocks are perceived as unnecessary in private environments and sensitive data is seldom accessed, we suggest that more effort should be put into researching how to decrease the number of unlocks by deploying usable context- and content-dependent locking mechanisms. The work of Hayashi et al. [13, 12] are a first step in this direction.

5.2 Reasons for (Non-)Use of Authentication are Highly Diverse

The results of both studies suggest that reasons for using or not using protection mechanisms to access smartphones are highly diverse. Often, they are not based on objective reasons and were not valid from a technical perspective. In turn, a considerable number of participants provided reasonable justifications. Furthermore, others argue that code locking mechanisms are not perfectly secure anyway and even have drawbacks should the device be lost.[3] Participants without a code-lock in the field study were also very satisfied with their choice and indicated very few situations where they would have rather had a lock screen. In turn, dissatisfaction with a code-based lock was not as pronounced in public situations, as participants valued protection slightly more in that case. In terms of attackers, survey participants were most afraid of unknown malicious as well as known curious attackers. This is mirrored in the field study results, where known persons had the most shoulder surfing and unwanted access possibilities in private environments while unknown persons dominated in public situations.

5.3 Protection is More Than Authentication

Throughout the analysis, it became apparent that most participants who did not use authentication to protect their phone did not consider themselves to be unprotected. We were able to identify a fair number of approaches that participants applied to protect their devices in the online study. These users felt secure despite the absence of authentication. For instance, participants reported to never leave their devices unattended when in public settings and to keep them close at all times (e.g. in their pockets or bags). This is also mirrored in the low number of high impact unwanted access possibilities during the field study.

This is even more interesting when analyzing the risks related to smartphone use. Only 26 % of the perceived worst-case risks in the study could actually be avoided by authentication. These included risks like theft or loss of the device itself. In many cases, participants rated the monetary value of their devices higher than the possibility of losing their

[3]The finder is not able to access the address book to find the owner.

data or someone gaining access to the data. Similarly, absence of threat was a very frequently mentioned reason for not having a lock screen in the online and the field study.

5.4 Sensitive Data is Seldom Accessed

As mentioned before, when filling out the questionnaire, participants were asked whether the accessed data is sensitive for them. This was the case in 25.3 % of all sampled unlocks. This means that nearly 75 % of interactions with the smartphones were with non-sensitive data. Taking into account the overhead created by the authentication process, there is high potential for lowering the burden for the users. That is, the results indicate that binary authentication as we are using it today (i.e. all or nothing access to a device) should be seriously re-assessed. For instance, instead of protecting the mobile operating system in its entirety, protection might be used on a data level. We can see a current trend in the mobile phone industry, granting access to non-sensitive functionality like flashlight and camera (not photos) without the need for protection. Our results suggest that this does not go far enough and more aspects of the phone could be used without the need for authentication. Hayashi et al. [13, 12] already proposed potential solutions for this problem.

5.5 Shoulder Surfing Risks Perception

The results of the field study indicate that the perceived shoulder surfing risks are rather low. Our participants believed shoulder surfing would have been possible in 17 % of reported cases. However, it was considered a high risk in only 11 out of 3410 occurrences. Additionally, participants protected themselves against such attacks using physical measures only in 2.8 % of sampled situations. Overall, we can state that the participants were aware of possibly risky situations but that this did not influence their general opinion about protecting against this threat. While shoulder surfing can take place in any environment, unknown attackers are mostly present in public environments, which were however frequented least by our participants.

Shoulder surfing in private environments was mostly considered possible by people known to the user. This was, however, often not considered a threat or those people knew the lock codes anyway. Yet, this does not mean that shoulder surfing is not a risk worth addressing by improved technology. Just because users do not perceive a threat as serious does not mean that it is not. It does however mean that the additional effort a user is willing to invest to protect from it needs to be carefully assessed. Based on our results we also recommend that the shoulder surfing attack risk can be minimized by reducing the number of "unnecessary" code entries. Since shoulder surfing resistant authentication mechanisms often incur reduced performance, the user should be able to decide in which situation protection is actually necessary.

6. ETHICAL CONSIDERATIONS

While there is no reviewing board at the involved institutions for this type of user studies, all studies have to comply with federal law and privacy regulations. We conducted both studies in compliance with these strict rules. For example, identifying information had to be removed from the data before analysis and participants can only be identified in cases for which they gave explicit consent (for example to receive their compensation).

7. LIMITATIONS

The online study as well as the field study both have limitations. The online survey relied on self-reporting and can hence only shed limited light on real behavior. We therefore focussed this investigation on respondents' perceptions, attitudes and common practices. The field study also logged behavioral data, but uses a different sample of participants as well as a limited set of sampled situations. While a considerable number of situations was sampled across 27 days, participants also indicated that some rare occasions and situations that did not last very long have been missed. Furthermore, extreme situations caused participants to dismiss the questionnaire, as they needed to access information quickly. Showing the questionnaires also heightened participants awareness of risk and their own behavior. This may have influenced participants' responses.

Similarly, we were only able to extract certain events from the Android OS. The reported times for the duration of the unlock therefore also include occasions where participants first read their notifications and only unlocked afterwards. The reported times should therefore be treated as upper limits. However, as this behavior is likely similar across the lock mechanisms, the respective values should still be comparable.

Finally, the field study also included self-reported and subjective views. Participants may have categorized similar situations as, for example, public or semi-public environments, depending on their perception. Also, the same data may be perceived as more or less sensitive by individual participants and attack opportunities may have been missed. However, we believe it is the participants' views that count more than absolute numbers, as they are more likely to adopt improved security measures if they see a relevant threat by themselves.

8. CONCLUSION AND FUTURE WORK

We were able to provide in depth insights into users' interactions with smartphone locking mechanisms. The online survey gave a broad overview of participants' reasons for (not) using lock screens, how they protect their phones, and which critical incidents have previously happened to them. In addition, the longitudinal field study captured one month of unlocking activity and sampled 6582 situations in situ, providing reliable ground truth for further explorations.

We found that there is a massive number of unlocks that the participants themselves severely underestimated. Participants also showed very diverse reasons for locking or not locking their phone. The insights gathered from our studies can help future efforts to improve the adoption of smartphone protection mechanisms. We also demonstrated that users apply many physical measures to protect their phone, which often makes additional IT measures superfluous in the their opinion. Sensitive data was found to be seldom accessed which provides an opportunity to reduce the attack surface of shoulder surfing.

We believe that in future work, these results can be used to improve the design of unlock mechanisms for mobile devices in general and their adoption in particular. Additionally, it would be interesting to extend our study to include users with more diverse demographics to assess their needs and allow for a tailoring of mechanisms to specific audiences.

9. REFERENCES

[1] A. Beautement, M. A. Sasse, and M. Wonham. The Compliance Budget. In *Proc. New Security Paradigms Workshop (NSPW)*, 2008.

[2] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon. The Phone Lock: Audio and Haptic Shoulder-surfing Resistant PIN Entry Methods for Mobile Devices. In *Proc. TEI*, pages 197–200, 2011.

[3] R. Biddle, S. Chiasson, and P. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv.*, 44(4):19:1–19:41, Sept. 2012.

[4] M. Cherubini and N. Oliver. A Refined Experience Sampling Method to Capture Mobile User Experience. In *International Workshop of Mobile User Experience Research - Proc. CHI EA*, 2009.

[5] N. Clarke and S. Furnell. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, 6(1):1–14, 2007.

[6] S. Consolvo, B. Harrison, I. Smith, M. Y. Chen, K. Everitt, J. Froehlich, and J. A. Landay. Conducting In Situ Evaluations for and With Ubiquitous Computing Technologies. *International Journal of Human-Computer Interaction*, 12(1-2):103–118, 2007.

[7] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns. In *Proc. CHI*, 2012.

[8] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. Slawik, H. Hussmann, and M. Smith. Now You See Me, Now You Don't – Protecting Smartphone Authentication from Shoulder Surfers. In *Proc. CHI*, 2014.

[9] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich. Back-of-device Authentication on Smartphones. In *Proc. CHI*, 2013.

[10] J. S. Downs, M. B. Holbrook, S. Sheng, and L. F. Cranor. Are Your Participants Gaming the System? Screening Mechanical Turk Workers. In *Proc. CHI*, 2010.

[11] J. C. Flanagan. The Critical Incident Technique. *Psychological Bulletin*, 51(4):327, 1954.

[12] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley. CASA: Context-Aware Scalable Authentication. In *Proc. SOUPS*, 2013.

[13] E. Hayashi, O. Riva, K. Strauss, A. J. B. Brush, and S. Schechter. Goldilocks and the Two Mobile Devices: Going Beyond All-Or-Nothing Access to a Device's Applications. In *Proc. SOUPS*, 2012.

[14] C. Herley. So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proc. New Security Paradigms Workshop (NSPW)*, 2009.

[15] R. M. Hogarth, M. Portell, and A. Cuxart. What Risks Do People Perceive in Everyday Life? A Perspective Gained from the Experience Sampling Method (ESM). *Risk Analysis*, 27(6):1427–1439, 2007.

[16] S. S. Intille, J. Rondoni, C. Kukla, I. Ancona, and L. Bao. A Context-Aware Experience Sampling Tool. In *Proc. CHI-EA*, 2003.

[17] M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit Authentication for Mobile Devices. In *Proc. USENIX HotSec*, 2009.

[18] A. K. Karlson, A. J. B. Brush, and S. Schechter. Can I Borrow Your Phone?: Understanding Concerns When Sharing Mobile Phones. In *Proc. CHI*, 2009.

[19] P. G. Kelley. Conducting Usable Privacy & Security Studies with Amazon's Mechanical Turk . In *Proc. SOUPS*, 2010.

[20] R. A. Khot, P. Kumaraguru, and K. Srinathan. WYSWYE: Shoulder Surfing Defense for Recognition Based Graphical Passwords. In *Proc. OzCHI*, 2012.

[21] S.-H. Kim, J.-W. Kim, S.-Y. Kim, and H.-G. Cho. A new Shoulder-Surfing Resistant Password for Mobile Environments. In *Proc. ICUIMC*, 2011.

[22] S. Kujala and T. Miron-Shatz. Emotions, Experiences and Usability in Real-life Mobile Phone Use. In *Proc. CHI*, 2013.

[23] J. Maguire and K. Renaud. You Only Live Twice or "The Years We Wasted Caring About Shoulder-Surfing". In *Proc. Conference on People and Computers*. British Computer Society, 2012.

[24] A. Möller, M. Kranz, B. Schmid, L. Roalter, and S. Diewald. Investigating Self-Reporting Behavior in Long-Term Studies. In *Proc. CHI*, 2013.

[25] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, Dec 2003.

[26] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos. Progressive Authentication: Deciding When to Authenticate on Mobile Phones. In *Proc. USENIX Security*, 2012.

[27] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'Weakest Link' – A Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, 19(3):122–131, 2001.

[28] F. Schaub, R. Deyhle, and M. Weber. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *Proc. MUM*, 2012.

[29] M. Shahzad, A. X. Liu, and A. Samuel. Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures: You Can See It but You Can Not Do It. In *Proc. MobiCom*, pages 39–50, 2013.

[30] M. Tamviruzzaman, S. I. Ahamed, C. S. Hasan, and C. O'brien. ePet: When Cellular Phone Learns to Recognize Its Owner. In *Proc. SafeConfig Workshop*, pages 13–18, 2009.

[31] F. Tari, A. A. Ozok, and S. H. Holden. A Comparison of Perceived and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords. In *Proc. SOUPS*, pages 56–66, 2006.

[32] E. von Zezschwitz, P. Dunphy, and A. De Luca. Patterns in the Wild: A Field Study of the Usability of Pattern and Pin-based Authentication on Mobile Devices. In *Proc. MobileHCI*, pages 261–270, 2013.

[33] S. Yazji, X. Chen, R. P. Dick, and P. Scheuermann. Implicit User Re-authentication for Mobile Devices. In *Ubiquitous Intelligence and Computing*, Lecture Notes in Computer Science, 2009.

[34] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan. Shoulder Surfing Defence for Recall-based Graphical Passwords. In *Proc. SOUPS*, 2011.

APPENDIX

A. ONLINE-SURVEY QUESTIONNAIRE

Smartphone Risk Attitudes.

- **IF CODE LOCK:** Please estimate how many times you approximately unlock your phone on an average day. – *Numeric answer*
- **IF CODE LOCK:** Please briefly state why you are using a lock screen on your device. – *Open-ended answer*
- **ELSE:** Please briefly state why you chose not to use a PIN, password, or pattern lock screen on your device. – *Open-ended answer*
- **IF CODE LOCK:** Please rate the following statements concerning your lock screen. – *5-point numeric scale anchored at don't agree and fully agree.*
  - Unlocking my phone is annoying sometimes.
  - I like the idea that my phone is protected from unauthorized access.
  - It is difficult to unlock my phone.
  - I wish there was an easier way of unlocking my phone.
  - Unlocking my phone is easy.
  - I am concerned that someone might be observing my unlocking password/pattern/PIN in order to access my phone at a later time.
- What's the worst thing that could happen to your smartphone?
  - Losing the phone itself, because I would have to buy a new one.
  - Losing the data that is on my phone (e.g. photos, contacts).
  - Someone being able to access my data when I lose my phone.
  - Someone being able to abuse my accounts and apps when I lose my phone.
  - Someone being able to access my data when my phone is unattended.
  - Someone being able to abuse my accounts and apps when my phone is unattended.
  - Other: *text field*
- Please rate how the following events compare to the worst thing that could happen to your smartphone (Your answer was: <previous answer>). – *5-point numeric scale anchored at worse, similar and not as bad.*
  - Losing data on my computer
  - Losing my wallet
  - Losing the key to my home
  - Losing the key to my car
  - Getting my email account hacked
  - Someone breaking into my home
- Please rate how serious you find the following incidents. – *5-point numeric scale anchored at not serious and very serious.*
  - *same items as "What's the worst thing..."*
- How likely do you believe it is that each of the following things occurs to you personally? – *5-point numeric scale anchored at very unlikely and very likely.*
  - *same items as "What's the worst thing..."*
- How frequently do you think about each of the following things? – *5-point numeric scale anchored at very infrequently and very frequently.*
  - *same items as "What's the worst thing..."*
- How likely do you consider the following groups of people to be attempting to access your smartphone? – *5-point numeric scale anchored at very unlikely and very likely.*
  - Unknown malicious person
  - Unknown curious person
  - Known malicious person
  - Known curious person
- **IF known person considered likely:** Which of the following groups of known people did you just consider as potentially interested in accessing your phone without your permission? – *Choice from: Potentially curious person, potentially malicious person, I did not consider this group of people.*
  - Acquaintances
  - Close friends
  - Friends of friends
  - Parents
  - Children
  - Other relatives
  - Co-workers and colleagues
  - Other people

Extra Measures.

- Do you sometimes take additional measures to protect your smartphone in particular situations? – *Choose all that apply.*
  - I leave my phone in a safe place before going somewhere.
  - I conceal my smartphone in my clothes or in a bag.
  - I enable a lock screen for this situation or choose a harder PIN/password/pattern.
  - Other: *text field*
- **IF MEASURES TAKEN:** Please list up to three situations in which you sometimes take additional measures to protect your smartphone. – *Open ended answer in three text fields.*
- **IF CODE LOCK:** If you think someone is able to see the screen of your phone, do you sometimes take additional measures to protect your smartphone? – *Choose all that apply.*
  - I cover my smartphone while entering my PIN or pattern.
  - I wait a moment before entering my PIN or pattern.
  - I turn around before entering my PIN or pattern.
  - I tilt my screen away before entering my PIN or pattern.
  - I change my PIN/password/pattern after someone could have seen my screen.
  - Other: *textfield*

Critical Incidents.

You indicated that someone had unwanted access to your smartphone. If this happened more than once, please answer this and the following questions with regard to the most severe case of unwanted access.

- Who had unwanted access to your smartphone? – *Open-ended answer in text field.*
- Please briefly described what happened during this unwanted access. – *Open-ended answer in text field.*
- Please briefly describe which harmful consequences, if any, arose from this unwanted access. – *Open-ended answer in text field.*
- What good, if any, came as a result of this unwanted access? – *Open-ended answer in text field.*
- What do you think made the unwanted access possible? – *Open-ended answer in text field.*

B. ONLINE-SURVEY CODEPLAN

B.1 Reasons for Using Code Lock

1. Protect from specific attacker
   (a) Coworker
   (b) Spouse
   (c) Roommate
   (d) Own children
   (e) Other *unwanted* individual/Stranger
   (f) Unspecified people
   (g) Friends
2. Protect information
   (a) In general/entire phone
   (b) Private/personal/sensitive information
   (c) Generally *confidential* information
   (d) (Confidential) *Work* info
   (e) Emails/Messages
   (f) Photos
   (g) Contacts
   (h) Calendar
   (i) Other app-content
3. Protect from specific scenarios
   (a) Phone protected if stolen
   (b) Phone protected if lost
   (c) Phone protected if misplaced
   (d) Phone protected if left unattended
   (e) Someone casually picking up the phone
   (f) Unwanted disclosure, Pranks
   (g) "Messing up" the phone
4. Protect certain action
   (a) Calls
   (b) Internet use
   (c) Using services
   (d) Play with phone
   (e) Deletion
   (f) Accidental input
   (g) Accidental calls
   (h) Other accidental use
   (i) Stealing data
5. Lock is mandatory
   (a) Forced by employer
   (b) Forced because of custom certificate
6. Context
   (a) Work
   (b) Sleep
   (c) Death
7. Given protection goal
   (a) Increase difficulty of access
   (b) Increase time to recover/find phone
   (c) Access control
   (d) "Safety"/Security
   (e) Privacy
   (f) Encrypt data
8. Other
   (a) Set by default
   (b) Having a lock is a habit
   (c) Allows second wallpaper
   (d) Previous bad experience
   (e) Peace of mind
   (f) Don't know
   (g) Curiosity
   (h) Used to Locking
9. Off Topic/Other
10. "Protection", Unspecific/general

B.2 Reasons for Not Using Code Lock

1. Inconvenience
   (a) It's a hassle/annoying/easier without
   (b) Mental burden
   (c) Takes too much time/want instantly available
   (d) Use it too frequently
   (e) Don't feel like it/Just don't like it
   (f) Too impatient
   (g) Not eyes-free
   (h) Used to existing system
2. Dislike
   (a) Passwords
   (b) Unlocking in general
3. No threat
   (a) General: Don't need security/not concerned about security
   (b) Nothing to hide/not worried about privacy
   (c) No sensitive data on phone
   (d) Not afraid of loosing phone
   (e) Keep physically secured/never leave unattended
   (f) Trust people around me/no one who wants to access
   (g) Use only in private environment
   (h) Phone not valuable
   (i) No bad experiences so far

4. Locking may cause problems
   (a) May forget my password/PIN/pattern
   (b) Child may lock parent out of own phone
   (c) Want finder to be able to contact me
   (d) Phone accessible in emergency
   (e) Shared use
5. No specific reason/Carelessness
   (a) Didn't consider it/think about it
   (b) Haven't gotten around to set it up yet
   (c) Don't care
   (d) Don't know how to set it up
   (e) Don't know if available
   (f) Laziness
6. Technical Reasons
   (a) Phone doesn't support lock (sic)
   (b) Broken Screen
   (c) Slows down phone
7. Protect phone using another measure
   (a) Use locking only in specific situations
   (b) Rely on remote locking
   (c) Leave phone at home
   (d) App-specific lock
8. Rightful punishment
9. Off topic/other
10. No protection possible/is not secure anyway

B.3 Situations

These codes were attached to statements in which participants mentioned where they take extra measures.

1. Public spaces
   (a) "Out", General public space
   (b) Events (Sport, Concert)
   (c) Airport
   (d) Public transport (plane, train, bus)
2. Semi-Public Spaces
   (a) Gym/Sports/Workout/exercise
   (b) Party/Club/Bar
   (c) Work/School
   (d) Shopping
   (e) Restaurant
   (f) Cinema
3. Private spaces
   (a) Home
   (b) Car
4. Unknown Spaces
   (a) Travel/Vacation
   (b) Unfamiliar places
5. (Hardware-)Risky Conditions
   (a) Water (Swimming, Boat, Rain)
   (b) Sports
   (c) Dirt (Beach, Cooking, Mow the lawn)
   (d) Jail
   (e) Lifting objects
6. Crowds
   (a) General crowded places
   (b) High foot-traffic area
7. Clothing
   (a) No Pockets
   (b) Other
8. Persons
   (a) Suspicious/nosy persons
   (b) Unknown/Untrusted persons
   (c) Family, Kids
   (d) Ex-Partner
   (e) Coworkers/Other pupils
   (f) General other people
   (g) Friends
   (h) Partner (girlfriend, boyfriend, spouse)
9. Uncontrolled Situations
   (a) General less cautious situation
   (b) General unattended
   (c) Left charging
   (d) Drinking/Socializing
   (e) Sleeping
   (f) Checked bags/Airport Security
10. Discomforting Environment
   (a) Night/badly lit places
   (b) Dangerous neighborhood/somewhere sketchy
11. Device sharing
12. Data
   (a) Inappropriate
   (b) Sensitive
13. Long idle times
14. Not at home
15. Activity
   (a) Walking
   (b) Quick errand
   (c) Exercising
   (d) Lodging/overnight stay
16. Off Topic/Other

B.4 Extra Measures

These codes were attached to statements in which participants mentioned which additional measures they take.

1. Safer mobile storage
   (a) Wear close to body (e.g. in pocket)/keep out of sight
   (b) Pocket in handbag/hide in purse
   (c) Zippered pocket
   (d) Inside pocket
   (e) Backpack
   (f) Have someone else carry it
   (g) Keep in hand
   (h) Strapped to belt/hip

2. Safer static storage
   (a) At home
   (b) Leave/hide in car (e.g. glove box)
   (c) Locker/Drawer
   (d) Leave in hotel safe
   (e) Pocket instead of purse
   (f) Never leave in car
   (g) Other/general
3. Technical Measures
   (a) Turn off
   (b) Enable lock screen
   (c) Have remote wiping/find my phone enabled
   (d) Encrypt data
   (e) Remove memory card
   (f) Extra protection for specific apps
   (g) Disallow access to specific apps
   (h) Mute it
   (i) Remove battery
   (j) Have backup
   (k) Use biometrics
4. Pay extra attention
   (a) Check repeatedly if phone is still there/ Monitoring phone (alerts)
   (b) Use it less/minimize interaction
   (c) Monitoring bystanders
   (d) Don't leave unattended
5. Physical measures
   (a) Sturdy/special case
   (b) Protect from water
   (c) Leave on highest shelf (kids)
   (d) Screen protector
   (e) Micro-cloth
   (f) Don't give to others
   (g) Other physical measure
6. Data
   (a) No sensitive data
   (b) Different accounts
7. General/other safe place

C. MINI-QUESTIONNAIRES

Participants were randomly presented with one of two mini-questionnaires. One concerned risks arising during unlocking and the other concerned risks to the data on the phone in general.

C.1 Unlocking Questionnaire

1. Who has a view on the contents of your screen right now?
   (a) Unknown Person
   (b) Known Person
   (c) Nobody
2. IF NOT (1) NOBODY: Please rate how likely it is that someone is watching your screen right now.
   (a) 5-point numeric scale ("very unlikely" to "very likely")
3. IF NOT (1) NOBODY: Please rate how severe it would be if this person was watching your screen right now.
   (a) 5-point numeric scale ("not severe at all" to "very severe")
4. WITH CODE LOCK: Did you try to protect your code input?
   (a) Yes/No
5. WITH CODE LOCK: Would you rather not have had a code lock in this situation?
   WITHOUT CODE LOCK: Would you rather have had a code lock in this situation?
   (a) 5-point numeric scale ("do not agree" to "agree")
6. In what kind of environment are you right now?
   (a) Private
   (b) Semi-Public
   (c) Public
7. How sensitive is the data you are going to access now?
   (a) 5-point numeric scale ("not sensitive at all" to "very sensitive")

C.2 Data Risk Questionnaire

1. Please rate this unlock.
   (a) 5-point numeric scale ("not annoying at all" to "very annoying")
2. Did you take any additional measures to protect your phone since last using your phone?
   (a) Hidden in clothes/purse
   (b) Left in a safe place
   (c) Other: <Text>
3. Could someone have had unwanted access to your phone since you last used it?
   (a) Yes/No
4. IF YES (3): Who could have had unwanted access?
   (a) Unknown Person
   (b) Known Person
5. IF YES (3): How likely do you think it is that this person actually did access the device?
   (a) 5-point numeric scale ("very unlikely" to "very likely")
6. IF YES (3): How severe would the consequences of this access be, had it actually happened?
   (a) 5-point numeric scale ("not severe" to "very severe")
7. In what kind of environment has the phone been since you last used it?
   (a) Private
   (b) Semi-Public
   (c) Public

D. SAMPLING OVERVIEW

The histograms in Figure 8 provide an overview of all participants' aggregated use (bottom facet) by time of day during the experiment (27 days). The top facet shows the corresponding number of mini-questionnaires of both types participants completed.

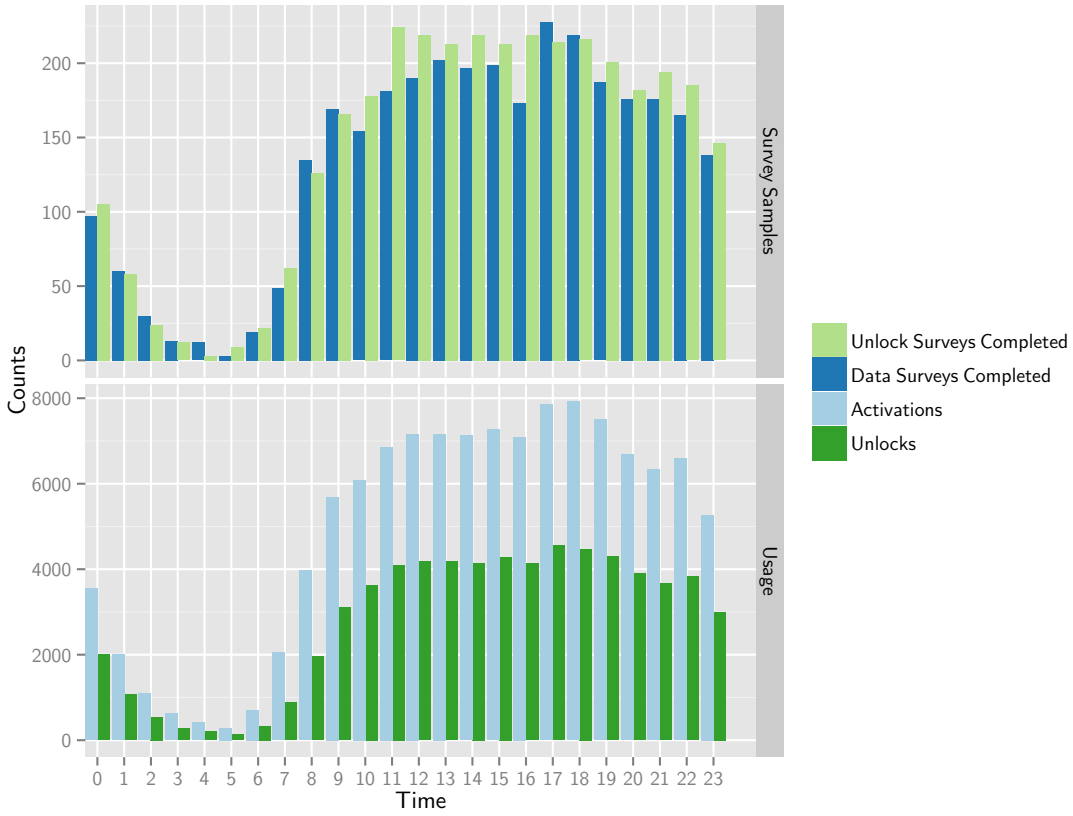

Figure 8: Overview of sampled situations per time of day, comprising number of mini-questionnaires shown as well as cumulative number of activations and unlocks.