

Are You Ready to Lock?

Understanding User Motivations for Smartphone Locking Behaviors

Serge Egelman^{1,2}, Sakshi Jain¹, Rebecca S. Portnoff¹, Kerwell Liao³,
Sunny Consolvo³, and David Wagner¹

¹University of California, Berkeley
Berkeley, CA

{egelman,sakshi.jain,rpotteng,daw}@eecs.berkeley.edu

²International Computer Science Institute
Berkeley, CA

egelman@icsi.berkeley.edu

³Google, Inc.
Mountain View, CA

{kerwell,sconsolvo}@google.com

ABSTRACT

In addition to storing a plethora of sensitive personal and work information, smartphones also store sensor data about users and their daily activities. In order to understand users' behaviors and attitudes towards the security of their smartphone data, we conducted 28 qualitative interviews. We examined why users choose (or choose not) to employ locking mechanisms (e.g., PINs) and their perceptions and awareness about the sensitivity of the data stored on their devices. We performed two additional online experiments to quantify our interview results and the extent to which sensitive data could be found in a user's smartphone-accessible email archive. We observed a strong correlation between use of security features and risk perceptions, which indicates rational behavior. However, we also observed that most users likely underestimate the extent to which data stored on their smartphones pervades their identities, online and offline.

Keywords

Smartphone security; risk perceptions; human behavior

Categories and Subject Descriptors

D.4.6. [Operating Systems]: Security and Protection—*Access Controls, Authentication*; K.6.5. [Management of Computing and Information Systems]: Security and protection—*Authentication*

1. INTRODUCTION

As of 2013, over 90% of Americans claimed to own mobile phones, the majority of whom use their devices to access the Internet, check email, or use third party applications [15]. This means that they trust their devices to store and access large amounts of sensitive data, ranging from contacts to financial details (indeed 35% use their devices for online banking [17]). At the same time,

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.

Copyright is held by the owner/author(s). Publication rights licensed to ACM.

ACM 978-1-4503-2957-6/14/11 ...\$15.00.

<http://dx.doi.org/10.1145/2660267.2660273>.

these devices are prone to loss: a 2012 report by the Pew Internet Project estimated that nearly a third of cell phone users have had a device lost or stolen [8]. Lookout estimates that this comes at a cost of \$30 billion per year [26].

The cost of losing a smartphone is more than simply the replacement cost of the hardware, as the data that can be found on the device is likely to be sensitive. Symantec performed an experiment by intentionally “losing” 50 smartphones in five major cities and observed that while 96% of the devices had their data examined by those who found them, only 50% of the finders attempted to return the devices [39]. Yet, despite these risks, previous research suggests that 35% of smartphone users do not lock their devices to prevent unauthorized persons from using them [36].

We performed qualitative interviews to understand users' motivations for choosing whether or not to lock their devices. Of our 28 participants, we observed that 29% (8 of 28) did not lock their devices. Their top reasons included concerns about emergency personnel not being able to identify them, not having their devices returned if lost, and not believing they had any data worth protecting. An online survey of 2,518 smartphone users corroborated our findings. We suggest that many concerns that prevent users from locking their phones can be alleviated by simple design changes.

Finally, we performed an online experiment to evaluate whether participants' beliefs about the lack of sensitive data on their devices were well-founded. We noted that all of our interview participants used their devices to access their email accounts, without requiring additional authentication. In our online experiment, we found that of our 995 participants, many reported finding their social security numbers (20%), credit/debit card numbers (16 and 17%, respectively), bank account numbers (26%), birth dates (46%), email passwords (30%), and/or home addresses (76%) stored in their email accounts. Yet, the presence of this data correlated with locking behaviors, suggests that some users may be making rational decisions to not lock their devices.

We contribute the following:

- We qualitatively show why users choose or choose not to lock their smartphones and quantify the prevalence of these rationales among the smartphone-owning U.S. population.
- We discuss how these findings can be used to improve mobile security and the user experience.
- Our studies suggest that access to email is a seriously underestimated threat to personal information. We attempt to quantify the likelihood of finding different types of sensitive information in an email account.

2. RELATED WORK

In this section we discuss previous work on smartphone locking methods, alternatives to the existing mechanisms, and users' mobile security perceptions.

2.1 Current Methods and Attacks

Despite a majority of users taking proactive steps to protect their smartphone data, many mobile authentication mechanisms can be defeated through relatively simple attacks. For instance, the unlock codes chosen by users are often relatively predictable and can therefore be determined by simple guessing [7, 1, 35, 40]. Other threats investigated in the literature include shoulder-surfing [14, 13], inference based on smudge patterns left on the screen [3, 38], or malicious applications that abuse access to the device's sensors to infer the user's unlock code [4, 32]. While these attacks could pose a threat in certain specific situations, we suspect they have limited relevance to most users' everyday use of their phones.

Regarding common smartphone security behaviors, van Bruggen *et al.* studied the adoption of smartphone locking methods among Android users [36]. They observed that while 35% of their participants did not lock their devices, those who did were split three-to-one in favor of Android's pattern unlock feature over entering a numeric PIN. von Zezschwitz *et al.* found that users perceive the pattern unlock as being quicker and less error-prone than PINs, though their quantitative data showed that reality is just the opposite: PIN entry is both less error prone and quicker [37].

The most relevant work to our study was performed by Harbach *et al.* [21]. They surveyed online participants about locking behaviors and risk perceptions. They followed this up with a month-long experience sampling experiment in which field participants were periodically asked to report on the likelihood of someone shoulder surfing when they unlocked their phones. Our work differs from theirs in that they performed an in-depth quantitative study of the likelihood of a particular threat model, whereas we examine the magnitude of harm stemming from a broad range of threat models by comparing participants' perceptions with the sensitivity of the data actually stored on their mobile devices. Thus, we believe our studies are complementary as together they provide a detailed assessment of smartphone risks stemming from unauthorized access; "a complete assessment of risk requires that the potential effects of [a risk] be combined with the probability of occurrence" [33].

2.2 Alternative Mechanisms

Today's mobile phones use a locked/unlocked security model that was designed when the data stored on phones was limited to call histories and the names and phone numbers of contacts. Currently, smartphone locking mechanisms prevent access to almost all device functionality (with some exceptions, such as answering calls, making emergency calls, or taking photos) when the device is locked. Hayashi *et al.* investigated how well this two-state access control model meets users' needs and preferences, as well as how receptive users would be to alternate fine-grained access control policies and authentication mechanisms [22]. Most of their participants wanted at least half of their applications to be accessible without requiring an unlock code, which suggests opportunities for improving current locking mechanisms. Interestingly, participants wanted apps that contained personal data to be unavailable when the device is locked, even though this included their most frequently used applications (e.g., email).

As an alternative to the standard all-or-nothing smartphone access control approach, Riva *et al.* proposed progressive authentication [27]. Using a variety of heuristics, their system determines a level of confidence in a user's authenticity. It then determines

whether to require authentication based on the confidence level and the degree of protection the user had specified for each application. Their system reduced the frequency with which users needed to authenticate by 42% while still maintaining acceptable security.

Other researchers have proposed alternative authentication mechanisms that aim to increase usability so that more users will choose to lock their devices. Takada and Kokubun suggested minor modifications to the PIN entry mechanisms that could result in significant security gains at little usability cost [34]. Many researchers have compared different types of graphical authentication mechanisms to show that there are many viable alternatives to the standard PIN or pattern approach [6, 10, 29]. Dunphy *et al.* showed that many of the concerns preventing these graphical authentication systems from being adopted are unfounded [16]. Others have proposed increasing the security of gesture-based authentication mechanisms on mobile devices by linking them to biometrics [28, 12]. For instance, Frank *et al.* showed that an individual's gesture style could be used as a secondary authentication heuristic [18]. However, Serwadda and Phoha showed that gesture styles could be observed and replicated automatically [31].

2.3 User Perceptions and Behaviors

Chin *et al.* showed that many users are apprehensive about performing private and/or financially-sensitive tasks on their phones, primarily because of fear of theft, mistrust of smartphone applications, and unfamiliarity with security features like remote wipe [11]. Chin *et al.* also showed that users are more concerned about privacy on their phones than on their laptops. Becher *et al.* provide an overview of how security actually differs between mobile and desktop devices [5].

Many smartphone users balance privacy concerns with the desire to share their devices with others [22, 20]. Karlson *et al.* showed that it is common for users to share their phones with up to 11 different people, despite these concerns [25]. They found that many users are uncomfortable with guests having access to personal information such as voicemail, notes, files, email, SMS, and calendars. However, some users may forgo locking their devices in order to be able to easily share their devices with those close to them.

Despite research on the security, usability (i.e., false rejection rate and time to authenticate), and vulnerabilities of smartphone authentication mechanisms, we are unaware of prior work that has qualitatively explored *why* people lock their smartphones. We are also unaware of work that has examined users' perceptions about the sensitivity of the data stored on their phones *vis à vis* reality. This research is necessary because it helps us to better understand why some users may abstain from locking their phones, whether they are rational in doing so, and how system designs can encourage better security behaviors.

3. METHODOLOGY

We performed structured interviews of 28 participants to gain qualitative insights into the locking behaviors of smartphone users. We used a grounded theory approach to understand why people choose (or choose not) to lock their smartphones [19], and then we quantified these results by performing a follow-up survey using 2,518 Google Consumer Survey (GCS) participants. Finally, to compare participants' risk perceptions with actual risks, we performed a third online experiment with 995 Amazon Mechanical Turk workers to measure the frequency with which different types of sensitive information are stored in email (and therefore could be accessed on an unlocked smartphone). In this section we describe our recruiting method and procedure for the initial interviews.

3.1 Recruitment

We placed an online recruitment advertisement on Craigslist in January of 2014, under the Bay Area “et cetera jobs” section. The title of the advertisement was, “smartphone owners - participate in a study,” and it stated that the study was about how people use their smartphones (the exact wording is presented in Appendix A). We intentionally made no mention of locking or security, in order to not prime them. Those interested in participating filled out an online screening survey in which they provided information about their age, gender, smartphone make and model, amount of time using a smartphone, contact information, and availability. We screened out those who were under 18 years of age or who had been using a smartphone for under six months.

We contacted participants who met our screening qualifications by email to schedule a time for them to visit our “laboratory” (i.e., a nearby coffee shop). We recruited 28 participants in this manner and instructed them to bring their smartphones with them, as they would be answering questions about how they use them. Participants showed up for individual sessions that lasted between 30 and 60 minutes. At the end of each session, we provided each participant with a \$35 debit card.

Of our 28 participants, exactly half were male, and ages ranged from 20 to 53 years old ($\mu = 31$, $\sigma = 9.6$). Eleven were Android users (39%), whereas the rest were iPhone users. While all participants had owned a smartphone for over six months, the length of ownership for their current devices ranged from 2 months to 3.5 years ($\mu = 16$ months, $\sigma = 9.1$). Thus, the vast majority of our participants had owned a previous smartphone (68% of 28).

3.2 Procedure

Each interview session took place in our “laboratory” with one participant and two researchers. One researcher, the interviewer, asked questions from a pre-determined list (i.e., structured interviews), while the other researcher took detailed notes. Both researchers were able to ask follow-up questions or clarifications if a participant’s responses were unclear. After arriving, the participant read and signed a consent form. Next, the interviewer explained that the purpose of the interview was to better understand how participants interacted with their smartphones. Again, to avoid priming, the security focus of the interview was not revealed until towards the end, and even then, it was never made explicit. Our questions fell into the following categories:

1. **Background and General Usage:** In the first part of the interviews, we asked participants to describe their smartphones and the other computing devices that they regularly used. For example, “*What is the make and model of your current smartphone?*,” “*For how long have you been using this smartphone?*,” and “*Do you use a tablet, laptop, or desktop computer?*” We also asked about the primary purpose of each device (i.e., whether it is for personal or professional use).
2. **Smartphone Apps and Accounts:** Participants listed all third-party applications installed on their smartphones. Next, we asked them to describe the ones that they used most frequently, specifically whether any of these applications have user accounts associated with them, and whether those account credentials are saved on the phone or need to be entered with each use. We prompted participants to describe their use of applications in a few special categories: financial accounts, applications used for purchasing items, email accounts, social networking, and file sharing/backup. The purpose of these questions was to understand the sensitive data that might be stored on each participant’s device.

3. **Backup and Syncing Behaviors:** We asked whether participants backup or sync their smartphones, their motivations for doing so, and their methods. For comparison, we also asked them whether they back up other devices they own (e.g., laptops). The purpose of these questions was to estimate the data loss impact of a lost or stolen device.
4. **Locking Behaviors:** We asked participants whether or not they locked their smartphones, and if so, the method they used to do so (e.g., PIN, drawing a pattern, etc.). We verified their responses (i.e., we observed participants unlocking their smartphones during the interview). We then asked participants why they chose or chose not to lock their devices, as well as whether they performed other types of security behaviors, both on their current and previous smartphones, as well as on their other computing devices. For example, “*Did you use a security lock on your old smartphone?*,” “*When did you first start using a security lock on that phone?*,” “*Have you ever forgotten your security lock?*,” “*Have you ever told anyone else your security lock?*,” and “*Do you know the security lock of anyone else’s device?*”
5. **Sharing Behaviors:** Finally, we asked participants whether anyone else ever uses their devices and whether they ever use others’ devices. This included specific scenarios about the types of data that they would be concerned with other people seeing, the personal and professional ramifications of a lost or stolen device, and whether they had previously thought about any of these issues.

Grounded theory is a well-established method for performing qualitative research [19], in which hypotheses are only established after a thorough examination of the data. Multiple researchers perform thematic analysis of interview data by independently reading over participants’ responses to create lists of themes that each researcher observed in the responses to each question. These themes are known as “codes,” and this process is performed independently to maximize the breadth of initial codes by preventing any one researcher from dominating the process. Next, the researchers discuss their codes in order to merge their findings into a single “codebook.” Using this codebook, each researcher independently codes the data by reading through participants’ responses again. Finally, the researchers discuss their codings, measure inter-rater agreement, and then resolve any disagreements so that the resulting codings are unanimously agreed upon.

We digitally recorded each interview and transcribed the recordings. The transcriptions were used for all of the analysis in this paper, with the second researcher’s notes available as backups. Next, three researchers coded all 1,257 responses; the number of responses per interview varied due to omissions and branching (e.g., participants who did not use PINs to lock their smartphones did not receive questions about how they chose those PINs). Prior to meeting to achieve consensus, the three independent coders disagreed on the coding of 48 responses, achieving inter-rater agreement of 96%.¹

4. RESULTS

Our primary goal was to better understand why smartphone users choose to employ security locks on their devices. We observed our 28 participants interacting with their devices and found that 8 chose not to lock them (29%). Of those who did, 18 used numerical PINs (64%), one used Android’s pattern lock (4%), and one used a fin-

¹We coded over 70 questions, many of which had different possible codes; we therefore found it infeasible to calculate Cohen’s kappa separately for every coded question.

gerprint (his was the only device with this capability). In the remainder of this section, we provide details about how participants use the locking mechanisms on their devices. We present explanations for why participants chose to lock their devices, how those decisions correlate with other security behaviors, and how these behaviors are influenced by various risk perceptions.

4.1 How Locks Are Used

Of the 20 participants who locked their smartphones, fourteen (70%) reported enabling this feature as soon as they purchased their devices, whereas the remaining six enabled it after they had already owned their smartphones for several months. Eighteen of our participants used numerical PINs, and of these, half admitted to choosing their PINs based on PINs they used elsewhere, such as at an ATM or on a bicycle lock. One participant said that he initially chose a unique PIN for his smartphone as a good security practice, but after repeatedly forgetting it, he ultimately reverted to using a PIN that he used elsewhere. Seven participants (37% of 19)² said they had previously changed their unlock codes; four of whom did so to make them more memorable, whereas three participants changed them to make them harder for others to guess. We asked participants whether they ever felt that unlocking their devices was a nuisance, and while eight said yes (40%), we observed no significant correlation with whether or not their smartphone PINs were used elsewhere. This suggests that the burden of remembering an additional PIN is minimal, and that the nuisance associated with unlocking a device may not be due to the memory aspect.

Another potential nuisance is having to enter an unlock code too frequently (i.e., due to a device automatically locking after sitting idly for too long). We asked participants to navigate to the settings screen on their devices so that we could see the screen timeout interval that was set. By default (at the time of this writing), Android devices lock after 30 seconds of inactivity, whereas iOS devices lock after 60 seconds. A total of eleven participants had changed the default values (55% of 20), ten of whom made it longer so that they would not have to enter their unlock codes so frequently (increased to a median of 5 minutes), whereas one participant made it shorter (decreased to 15 seconds). In each case, the participants who extended the time cited the inconvenience of having to enter unlock codes repeatedly, whereas the participant who decreased it cited privacy reasons. This suggests that platform developers may want to increase these default timeout intervals, lest some users become annoyed and disable the locking mechanism altogether. For example, P2 used a fingerprint and said that he would not lock his device if he was required to enter a PIN every time.

We were curious if security lock usage on a previous smartphone would be a predictor of current security lock usage. Of our 28 total participants, seventeen reported owning a previous smartphone. However, we observed no correlation between previously and currently using a security lock ($r = -0.054$, $p < 0.840$). Twelve participants locked their previous smartphones, and of those, nine continued to do so on their current phones. Four participants who did not previously lock their phones started doing so.

Three participants reported locking previous smartphones, but for various reasons decided not to lock their current smartphones. One participant, P10, disabled it because he was concerned about others being able to contact his girlfriend in the case of an emergency: *“I was worried that if I got into an accident and somebody needed to call, like, my girlfriend, that they wouldn’t be able to get into my phone.”*

Another participant, P15, reevaluated his decision, and decided that the PIN was more trouble than he believed his information was worth: *“it wasn’t useful for me to have to unlock it every time I wanted to use my phone. I wasn’t in any worry that my phone was going to be taken or anything like that.”*

A third participant, P23, had locked his previous smartphone, but simply forgot to set it up on this one: *“It said choose a password. I think this time I was eager to maybe do something else so I said, like, remind me later.”*

4.2 Reasons for Locking

Before priming participants with questions about security and privacy, we asked why they chose to lock their smartphones. Six themes emerged, which we classified into two different categories. First, about two-thirds of our participants who locked their devices (14 of 20) mentioned very specific scenarios that they were trying to avoid. Second, the remaining third of participants (6 of 20) indicated that they locked their devices out of a more general sense of “good security behavior,” rather than to counter any particular perceived threat.

4.2.1 Specific Privacy and Security Concerns

The most frequently cited reason for locking one’s phone was privacy: eight participants (40% of the 20 using security locks) indicated that they chose to lock their devices to prevent people they knew from snooping or using their phones without permission. Six of these participants specifically mentioned protection from friends and family. Responses included:

“I don’t want, like, when people go through my pictures without me knowing...not all of my pictures I want other people to see” (P8)

“I had to pay, like, per minute...so I didn’t want anybody including friends to use it, or anybody who was at home or family. You know you might use my phone without me knowing, so I had a PIN on there” (P9)

“I got really really tired of my friends picking up my phone and checking my emails...like I don’t have anything to hide, but it’s like...privacy” (P14)

“Privacy from [my] mom and [my] sister” (P20)

Two participants worked with children and were concerned about snooping in their workplace environments. Specifically, P12, a teacher, mentioned problems with thefts in her school: *“so students couldn’t get into it if they stole it.”*

P17, who worked in a municipal recreation department, mentioned a similar rationale:

“I was coaching a little girls’ soccer team and they were wanting to get on my phone and play with it and stuff...I was like, I’m going to put this [lock] on there...not that I have anything to hide from them, but who knows what little 10 year olds are going to do...I never bothered changing it so now I just have it.”

We asked participants if they had ever told anyone their unlock codes: only three of these eight participants had done so (38%), whereas of the other 13 participants who locked their devices, twelve had acknowledged sharing unlock codes with others (92%). This correlation was statistically significant ($\phi = -0.589$, $p < 0.007$). That is, those who were concerned about specific individuals were

²We do not consider the participant who used a fingerprint.

less likely to share their unlock codes than those only concerned with strangers. Yet despite concerns about specific individuals, most of these eight participants indicated that they were still comfortable allowing close friends and family to use their devices. In fact, seven reported that someone else had used their phone in the past four weeks (88% of 8). Thus, these participants were concerned about *regulating* access to their devices, rather than locking others out completely.

Similar to regulating when known individuals use the device, the second most common rationale was preventing strangers from accessing devices. Specifically, six participants (30% of 20) mentioned the lock as either a theft deterrent or to prevent strangers from accessing their personal information:

“I don’t do that [lock my phone] so that someone I know can’t get in...” (P1)

“It at least prevents someone...from being able to pick it up and messing around with it” (P4)

“Because otherwise my phone would just be able to be accessed by anyone and I don’t want that. Also, I’m automatically logged in to my email, my Facebook, a lot of different things without having to put [in] a password” (P16)

“...[a thief] is not going to be able to use it” (P20)

P3, who used to work at an Apple Store, said he started using a PIN because he was worried that he might leave his iPhone out and customers would confuse it with a demo unit:

“I had more sensitive information on there, all my credit card information, my bank information on there...I was just more aware of what people would have access to.”

Three participants (15% of 20) mentioned that they enabled security locks on their smartphones after they personally had bad experiences on a previous phone when they did not use a security lock. For instance, P5 mentioned that a friend played a joke on him by changing the default language to Russian: *“my old phone, someone took it and changed the settings...it was pretty hard to go back to my original settings.”*

Another, P6, mentioned a stranger making expensive calls:

“I accidentally left my phone—not the smartphone, but my Razr—a long time ago in a park...somebody actually used it to make calls, so now...with a smartphone you have a lot more [personal data], compared to the Razr cellphone, I’m a little paranoid about that.”

4.2.2 General Concerns

Contrasting with the majority of lock-using participants who identified specific threat models, six participants (30% of the 20 lock-using participants) mentioned motivations that were more general. These explanations amounted to enabling it simply because the option to do so was presented as part of their smartphone’s setup process, social pressure from friends and/or family, or simply not seeing a downside to doing so.

Two of these participants (10% of 20) indicated that they began locking their smartphones because they were prompted at setup and otherwise would not have thought about it:

“I didn’t have that originally, but on one of the last updates it like demanded it” (P11)

“I actually think that the gentleman just set it up when he sold me the phone” (P28)

Given that these participants could not name a specific privacy or security concern, one might expect that they would eventually disable the security locks, if they believed that they otherwise had no practical value. We asked participants about this and found that P11 had been using a PIN for 12 months, the entire length of time that she had owned a smartphone. P28, whose device was only 6 months old, indicated that he initially set it up on a previous phone because the setup program prompted him, he then went out of his way to set it up on his current phone out of habit.

Two other participants (10% of 20) said that they were persuaded to use a locking mechanism by a friend or significant other, and otherwise would not have done so. That is, for some users, social influence or adherence to social norms is the prime motivator, rather than specific privacy or security concerns:

“I guess just that was suggested to be a good idea, my girlfriend uses one” (P25)

“My friend reminded me that this was a smartphone...there was access to lots of my accounts” (P27)

Finally, another two participants (10% of 20) indicated that they set it up simply because they did not see a reason not to, though could not mention any specific concerns:

“I figured since it had the feature anyway, it’s pretty quick I guess, I might as well use it...” (P2)

“Just like, why not? I mean it was probably, I read something about like easy tips to safeguard your phone or something” (P7)

Our results indicate that most users actively enable locking mechanisms on their devices due to specific privacy and security concerns, whereas a minority will do so when prompted and will continue to do so, even if they see it as a nuisance. That is, most users see locking as a valuable feature.

4.3 Reasons for Not Locking

Eight participants chose not to lock their smartphones (29% of 28). Based on their responses to the initial question on why they chose not to lock their devices, three non-mutually-exclusive themes emerged: lack of motivation, convenience, and lack of concern.

The most common explanation was lack of motivation: they simply had not gotten around to setting it up, but were not averse to it. Three participants (38% of 8) fell into this category. Though they indicated that they would like to lock their phones, they had not bothered to look into how to do so:

“Yeah, I thought about it. I just never bothered. I mean, it’s probably something I should do, but...” (P19)

“It [current phone] said choose a password...I said, like, remind me later.” (P23)

One participant was prompted during setup to enable locking (P23), but postponed it and forgot. He said that he previously drew a pattern to unlock his Android phone, but in the last month received a warranty replacement reset to the factory settings. He

indicated that he plans to re-enable it, and that our prompting reminded him. Similarly, the two other participants indicated that they were still planning to enable locking. Thus, for over a third of our participants who did not lock their devices, it was not a willful decision, but an oversight. In total, twenty-three (82% of 28; 95% CI:[0.63, 0.94]) were unopposed to locking their devices.

However, the remaining five participants who did not lock their smartphones made deliberate decisions. These five participants all stated that locking their devices would not be worth the effort. Specifically, three participants (38% of 8) mentioned that the inconvenience was too great. Two participants, P10 and P24, specifically mentioned the ability for strangers to use their phones in the case of an emergency:

“I was worried that if I got into an accident and somebody needed to call like my girlfriend that they wouldn’t be able to get into my phone...” (P10)

“...like if I’ve got into an accident and I couldn’t tell them what [the lock] was or something like that” (P24)

The third participant mentioned personal experiences finding lost phones and returning them to the owners because she was able to browse through their contact lists. Thus, she was worried that if she locked her own phone, it would decrease the likelihood of getting it back if she ever lost it:

“...if I lost my phone, I trust in people enough that they would open it up and try and get hold of someone instead of stealing it. I just, I have best hopes for people so...I just, I found a few phones, and I wouldn’t have been able to help the person if it was locked...I’m totally 50/50 split on this” (P18)

P18 was unaware that both Android and iOS include features to help the finder of a lost phone locate the owner. Android allows the owner to display contact information on the lock screen [9], whereas Apple’s Find My iPhone application allows the owner to put her device into “lost mode” from a website, which displays her contact information on the lock screen [2]. Of course, this does not address the issue of being able to display information during emergencies. Some people have resorted to adding address book contacts under the heading “ICE,” which stands for In Case of Emergency [24]; several different applications have also been developed to place this information on the lock screen. However, none of the major smartphone platforms provide this feature by default.

Finally, two participants (25% of 8) did not believe they had any information worth protecting:

“I’m not worried about losing my phone, or having somebody pick up my phone and use it” (P15)

“I don’t feel like I keep anything valuable on here...there’s nothing in here I feel like I need to protect. Yeah, if I started having financial information or if there was a reason that people could get to my passwords...that would be a reason to lock it up.” (P21)

Both of these participants claimed to regularly backup their data and therefore were not at risk of data loss. The most sensitive data on their devices appeared to be email, as neither had any applications that stored sensitive data (e.g., banking). Likewise, these participants had installed a median of 14 applications, whereas the re-

maining 26 participants had installed a median of 31 applications.³ Thus, it is possible that these participants’ decisions to not lock their devices was rational, however, it is not possible to say with certainty without knowing whether any potentially sensitive information is contained in their email accounts (and therefore accessible through their unlocked smartphones).

4.4 Comparison with Online Sample

To quantify why smartphone users choose or choose not to lock their devices, we conducted a separate online survey.

4.4.1 Methodology

We commissioned a survey using Google Consumer Surveys (GCS) that featured two multiple-choice questions. The first question, “What secret unlock method do you use on your smartphone?” featured the following options:

- I don’t have a smartphone
- None (I just slide to unlock)
- PIN / Passcode / Password / Pattern
- Fingerprint
- Other

We asked participants who reported using a security lock (i.e., PIN, passcode, password, pattern, or fingerprint), “Why did you decide to use a locking method on your smartphone?” We provided the following options, with instructions to select all that applied:

- Prevent strangers from using my phone
- Control when friends/family use my phone
- I’ve never thought about why I use one
- It’s easy to do
- Other people I know use a security lock
- None of the above

For participants who indicated that they did not use a security lock, we asked, “Why did you decide not to use a locking method on your smartphone?” We provided the following options, with instructions to select all that applied:

- In an emergency, others can use my phone
- It’s too much of a hassle
- I’ve never thought about it
- No one would care about what’s on my phone
- None of the above

The possible answers to each question were based on the most popular reasons for using or not using a security lock, as determined by our in-person interviews, and were not mutually-exclusive (with the exception of “none of the above”). Overall, we received a total of 2,518 responses from smartphone users to the first question (i.e., the locking method used). These responses were split roughly 60-40 in favor of locking: 1,470 respondents claimed to lock their smartphones (58% of 2,518), whereas 1,048 respondents claimed to not lock their smartphones (42% of 2,518).

We received 500 responses for why security locks were used and 500 responses for why security locks were not used. Thus, our analysis only focuses on these 1,000 participants. Our data included demographic inferences (rather than relying on self-reporting). Gender was reported for 797 of these participants (56% male), age

³The sample size of two is insufficient to compare whether this difference in medians is statistically significant.

| Why did you decide to use a locking method? | | |
|---|-----|---------|
| Prevent strangers from using my phone | 273 | (54.6%) |
| Control when friends/family use my phone | 116 | (23.2%) |
| It's easy to do | 102 | (20.4%) |
| I've never thought about why I use one | 43 | (8.6%) |
| Other people I know use a security lock | 41 | (8.2%) |
| None of the above | 61 | (12.2%) |
| Why did you decide not to use a locking method? | | |
| It's too much of a hassle | 168 | (33.6%) |
| No one would care about what's on my phone | 131 | (26.2%) |
| I've never thought about it | 97 | (19.4%) |
| In an emergency, others can use my phone | 47 | (9.4%) |
| None of the above | 101 | (20.2%) |

Table 1: Responses from 500 participants to why they lock their smartphones, as well as another 500 participants who explained why they chose not to lock their smartphones.

ranges were reported for 776 respondents (median of 35-44 years), and income ranges were reported for 995 participants (median income range of \$25,000-\$49,999). Finally, the vast majority of our participants resided in urban or suburban areas (86%), while 12% resided in rural areas. Based on these demographics, we believe that our sample is reasonably representative of the U.S. smartphone-using population.

4.4.2 Results

Overall, we observed that a majority of participants (55% of 500) claimed to lock their devices to prevent unauthorized access by strangers, whereas only 23% indicated that it was to regulate usage by friends and family (Table 1). Of those opting not to lock their devices, a plurality believed it was too much of a hassle (34% of 500) and 26% did not believe their devices could be used to access sensitive data.

Our initial in-person interviews followed a grounded theory approach to uncover the different explanations for why participants chose or chose not to lock their devices [19], whereas the goal of our online survey was to measure how prevalent these explanations were among the population at large. For this reason, and because the two experiments were performed at different times, using different methods, and on different samples, direct statistical comparison of the two experiments would not be meaningful.

We believe these results validate the findings from our in-person interviews, because the possible reasons that we uncovered for locking or not locking one's smartphone were applicable to 84% of our 1,000 online survey respondents. Only 12% of those locking their smartphones (61 of 500) and 20% of those not locking their smartphones (101 of 500) indicated that they did so for a reason other than any of the ones that we provided to them.

4.5 Perceived Threats

To understand interview participants' motivations for locking their devices, we presented them with several scenarios involving data compromise on their smartphones. In one scenario, we asked them what the worst personal consequences would be if strangers gained access to their phones and whether they thought someone could then impersonate them. In another, we asked about professional consequences. Finally, we asked whether they had any concerns about the data stored on their significant others' smartphones.

Only one participant believed that he would not face any personal consequences if a stranger gained access to his smartphone. The remaining participants fell into a handful of non-mutually-exclusive categories, the most common of which related to online identity theft (61% of 28). These seventeen participants cited concerns

about online account compromise, rather than someone impersonating them offline. Despite us priming participants to think about identity theft (i.e., we directly asked them about an attacker's ability to impersonate them), only one participant made the connection between offline and online identity. This participant mentioned that he had a scan of his passport in his Dropbox account and was concerned it could be used to steal his offline identity.

Similar to identity theft, the second most common theme related to strangers using participants' smartphones to impersonate them online. Seven participants (25% of 28) specifically mentioned social networking accounts, such as a stranger being able to post to Facebook or read previous posts. Participants were also likely primed to this concern because they previously had gone through their installed applications and indicated whether or not each one required authentication. Seven participants (25% of 28) mentioned general privacy concerns, such as knowing someone might be looking through their personal photos or contacts.

We were surprised that beyond the loss of the hardware itself, only six participants (21% of 28) raised concerns relating to financial loss. Five (18% of 28) were concerned with a stranger accessing their banking information, such as their account details via an installed banking application, while three participants (11% of 28) were concerned that their lost phones would be used to make purchases via applications that they had installed (e.g., Amazon, Groupon, Starbucks, Uber, etc.).

During the beginning of each interview, we asked participants to state their occupations. While two were unemployed and two others were full-time students, the remaining 24 participants held a wide variety of different occupations, which are listed in Appendix B. Eighteen participants (64% of 28) did not believe there would be any professional consequences, and none of our participants indicated that they would be required to report the loss to their employers or that they risked being fired. Of those concerned about professional consequences, the most common concern was having one's reputation damaged by inappropriate communication with work contacts, which was voiced by five participants (18% of 28). Three (11% of 28) were concerned about strangers seeing sensitive work-related information, and another two (7%) were concerned that strangers would have access to data inappropriate for the work place, which could then be disseminated to coworkers.

Eighteen of our participants had smartphone-owning significant others. Of these participants, only five (28% of 18) voiced concerns over the security of the data stored on their partner's phone. Without prompting them to describe that data, three outright volunteered that their partners stored intimate photos:

"Not my phone number so much as naked pictures...yeah that probably wouldn't be a good thing." (P1)

"Besides the naked girlfriend pictures?" (P7)

"Maybe sexy pictures or something, but I don't know where he keeps those." (P16)

The remaining two participants voiced concerns over sensitive personal emails and a partner potentially jeopardizing his security clearance. For the participants who were unconcerned, two primary reasons emerged. Ten (77% of 13) did not believe their significant other stored any sensitive information and three (23% of 13) believed their significant other was taking adequate precautions.

Overall, our interview and survey data suggest that many smartphone users choose not to protect their devices because they do not believe any sensitive information is stored on them. While many of the interview participants who did not lock their devices had fewer

applications installed, and therefore potentially less sensitive information, every participant’s smartphone still had access to email, which did not require additional authentication. Thus, it is possible that these email accounts might be a fruitful target for an attacker.

5. ACTUAL RISKS

In this section, we attempt to quantify the risks that participants might face if their smartphones are accessed by unauthorized individuals, and how those risks compare with the risk perceptions of our interview participants. Based on our hypothesis that some participants undervalued the risk posed by access to email, we performed an online experiment to quantify the types of sensitive information that might be found in an individual’s email account.

5.1 Email Risks

All 28 interview participants had the passwords for their primary email addresses saved on their phones, such that an attacker with access to the device in an unlocked state could control the owner’s email account. Because many online services use email for password recovery, email accounts can be an overlooked attack vector for an attacker trying to gain access to other applications and accounts. Beyond actively using a stolen email account to gain access to other services by using it to reset their passwords, we were curious about the types of sensitive information a motivated attacker could find about a victim in that victim’s email archive, which would be searchable from a stolen device.

5.1.1 Methodology

We conducted an online survey of email users to understand the types of sensitive information that could be found in their email accounts. We recruited 1,000 participants via Amazon’s Mechanical Turk to search through their email archives for different types of personal information, to report how many hits their searches turned up, to describe the contexts of the found emails, and to indicate how surprised they were by the results. We restricted participation to those over 18 years old residing in the U.S. Our only other screening requirement was that they needed to have successfully completed at least 95% of their previous tasks. We used participants’ open-ended descriptions of the found emails as a screening mechanism to detect cheating. After removing five participants who provided gibberish or nonsensical responses to this question, we were left with 995 legitimate responses. Because this method could only screen out participants who reported finding sensitive information (i.e., those claiming to be unsuccessful did not answer this question), our results likely represent lower bounds; it is possible that some participants did not correctly perform the task and therefore inflated the denominator.

We randomly assigned participants to one of nine conditions that varied based on the data type to be searched. We asked participants to perform most of the searches using multiple formats that we provided them. The data types and formats were as follows:

1. **Social Security Number (SSN)**
Format: “XXX-XX-XXXX” and “XXXXXXXXXX”
2. **Last 4 digits of the Social Security Number (SSN)**
Format: “XXXX”
3. **Bank account number**
4. **Last 4 digits of a bank account number**
Format: “XXXX”
5. **Credit card number**
Format: “XXXXXXXXXXXXXXXXXX” and “XXXX-XXXX-XXXX-XXXX”

| Condition | total | % |
|--|-------------------|--------------|
| 1. SSN (full) | 22 of 113 | (20%) |
| 2. SSN (last 4 digits) | 44 of 124 | (36%) |
| 3. Bank Account Number (full) | 27 of 105 | (26%) |
| 4. Bank Account Number (last 4 digits) | 45 of 108 | (42%) |
| 5. Credit Card Number (full) | 14 of 90 | (16%) |
| 6. Debit Card Number (full) | 19 of 111 | (17%) |
| 7. Date of Birth | 57 of 123 | (46%) |
| 8. Email Password | 35 of 115 | (30%) |
| 9. Home Address | 80 of 106 | (76%) |
| Total (i.e., any sensitive information) | 343 of 995 | (35%) |

Table 2: Participants able to find various types of information in their email accounts. We randomly assigned each participant to one of nine between-subjects conditions.

6. Debit card number

Format: “XXXXXXXXXXXXXXXXXX” and “XXXX-XXXX-XXXX-XXXX”

7. Date of birth

Format: “MM/DD/YYYY” and “MM-DD-YYYY”

8. Email password

9. Home address

We compensated all participants \$1, regardless of whether or not their searches were successful, so as to not incentivize over-reporting. Based on the clarity of participants’ open-ended descriptions of the emails found, we saw no indication that they over-reported results. It seems likely that this experiment may underestimate the amount of sensitive information in email archives, because it is likely that some participants may have felt uncomfortable reporting this information to us, despite the fact that our instructions made clear that we did not want them to share the specific search results with us. Thus, this is another reason why we suspect that our results represent lower bounds on the prevalence of sensitive information.

To assess whether locking behaviors correlated with the amount of sensitive data found in an email account, we prefaced the survey with a question on whether or not participants lock their smartphones. We used the same question and options from the Google Consumer Survey that we discussed earlier (i.e., *What secret unlock method do you use on your smartphone?*). Unfortunately, we did not think to add this question until after we had already received 495 responses, and thus we only collected responses to this question for the last 500 respondents.

5.1.2 Results

We observed that 343 participants (35% of 995) reported finding at least one email containing the requested information (Table 2). As would be expected, the frequency with which certain data types were found appeared to vary inversely with the perceived sensitivity of that data: at the low end, “only” 16% of participants found their full credit card numbers, whereas 76% reported finding their home addresses.

We performed Fisher’s exact test to examine whether participants with unlocked smartphones were more or less at risk than those with locked smartphones. We observed a statistically significant difference: 38% of those using locks found sensitive information in their email accounts, whereas 27% of those not locking their smartphones found sensitive information ($p < 0.010$; two-tailed). While significant, the effect size is small (Cramer’s $V = 0.123$). In addition to more lock-using participants finding sensitive information, a Mann-Whitney U test indicated they also found significantly more of it ($U = 23,340.5, p < 0.009$).

Many participants reported being surprised by their findings. We performed a Pearson correlation between participants' self-reported surprise assessment (reported using a 5-point Likert scale, from *expected many more* to *expected many fewer*) and the number of hits their searches yielded and found a positive correlation ($r = 0.14$, $p < 0.0005$). Likewise, a Mann-Whitney U test of the surprise assessments between those who found any hits and those who did not was also statistically significant ($U = 98,735.5$, $p < 0.001$).

Thus, over a third of our participants found sensitive data in their email accounts, which was surprising to them, and those locking their smartphones were more likely to find sensitive data. Of course, these results say nothing about causality; we do not know if participants choose to lock their phones because they know that more sensitive data can be found in their email accounts (accessible from their phones), or if participants are more willing to send sensitive data via email because they lock their phones. It is also possible that some or all of this effect could be simply due to priming: participants who acknowledged not locking their phones may have felt a need to under-report. Regardless of the reason, it is still disconcerting that of those who do not lock their devices, 19% found full bank account numbers, 33% found email passwords, and 46% found dates of birth.

This is particularly troubling when considering the authentication requirements of many smartphone applications that store sensitive data, such as the payment, shopping and banking applications that many of our interview participants had installed. While these applications require additional authentication, which participants cited as a reason for their lack of concern, in many cases the authentication can be circumvented when an attacker has access to email. Passwords to Groupon, Amazon, and Uber accounts, which protect a user's financial information and physical address, can be reset via email. PayPal and eBay require a full credit/debit card number and the answers to two security questions in order to change a password: our online survey suggests that an attacker would be able to locate a credit/debit card number in a victim's email account around 17% of the time, while Schechter *et al.* showed that guessing the answers to security questions is often quite easy [30]. Similarly, with knowledge of the username (often saved on the applications' home screens), the passwords for Bank of America and Fidelity can be reset via email. Without knowing the username, the passwords for Wells Fargo, Chase and Fidelity can be reset with two of the following four pieces of information: account number (found in 26% of email accounts),⁴ birthdate (found in 46% of email accounts), credit/debit card number (found in 16-17% of email accounts), or Social Security Number (found in 20% of email accounts).

6. DISCUSSION

In this section, we discuss how our experiment compares with related work, ways in which more users could be motivated to lock their smartphones, whether it is rational to expect all users to lock their phones, the limitations of our experiments, and we conclude with future work.

6.1 Comparison with Related Work

As discussed in Section 2, Harbach *et al.* also performed an experiment to examine users' motivations for locking (or not locking) their smartphones [21]. Because our experiments were performed at different times, using different samples, and used different survey instruments and interview guides, we cannot make a direct statistical comparison. However, at a high level, we believe our

⁴For users with multiple bank accounts, the probability of finding the one being reset is obviously lower.

experiments are complementary. Harbach *et al.* performed an in-depth field study on the likelihood of one particular threat model occurring—shoulder surfing. They also noted that “no participant mentioned protecting login credentials or logged-in accounts directly.” We expanded upon this by asking participants about the types of sensitive data that could be found in their email accounts (Section 5). We observed that indeed this is a serious threat, as many participants were able to find data ranging from passwords to bank account numbers. Thus, while Harbach *et al.* observed that there are situations in which users have sensitive data displayed on their devices upon which others may eavesdrop, we show that a device falling into the wrong hands may yield even greater violations of privacy and other security-related consequences.

Our studies also corroborate each other. For instance, we found that despite being viewed as a nuisance, many users continue to lock their devices because they believe that the benefits outweigh the costs. Harbach *et al.* observed that 47% of their online participants stated that unlocking their phones was annoying, yet continued to use an locking mechanism, whereas 40% of our lock-using interview participants also said that it was a nuisance (despite continuing to use it). Supplementing the answers to this question with open-ended followup during the in-person interviews helped to shed additional light on participants' motivations. For instance, we observed that almost every participant had some experience with the theft or loss of a device, either first or secondhand. As we will discuss in the next section, the opportunity to ask open-ended followup questions during interviews allowed us to propose new strategies to encourage more people to enable locking mechanisms on their mobile devices.

Where our studies diverge is with regard to conclusions. Harbach *et al.* concluded that because “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” [21]. Through our qualitative interviews and our online quantitative survey, we observed that roughly a quarter of our participants chose to lock their devices in order to regulate when friends and family accessed them. For these participants, the primary threat model stemmed from these private environments. Thus, the decision of whether or not a device should be locked at any given moment is likely to extend beyond context and the content to be displayed on the device's screen, but also needs to consider the user's personal privacy preferences and the data stored on—or accessible through—the device.

6.2 Improving Uptake

Assuming that locking one's smartphone is a “good” security behavior, how can we motivate more people to do so? Given the millions of people in the U.S. using smartphones, the 29% of interview participants (and 42% of GCS respondents) not locking their smartphones represent a large number of users who may be exposing themselves to threats unnecessarily. Based on the GCS data, a large minority of users do not lock their devices because they do not believe it is worth the effort (34% of 500). We believe that the majority can be motivated through simple design changes to mobile platforms and education.

Our GCS data indicated that 26% of users do not lock their devices because they do not believe that they have any data worth protecting. Our email experiment rebuts this: 35% of our participants were able to find sensitive data stored in their email accounts, which an attacker could easily access on an unlocked smartphone. None of our interview participants—regardless of locking behavior—made a connection between the sensitive data that might

be stored in an email account and the ability to access that data through their smartphone, and therefore it is likely that those claiming to not have any sensitive data stored on their smartphones were not making this connection either. We believe that some awareness could be achieved by better messaging. For instance, several participants indicated that a customer service representative initially helped them setup their smartphones; during this process, the representative could point out that any information contained in their email archives could be viewed by anyone who possesses their smartphone. Likewise, due to network effects, email providers have a strong incentive for mobile users to prevent unauthorized access to email accounts. The providers could enforce this by using existing technologies: for instance, Microsoft's Exchange allows an administrator to specify a minimum security policy (e.g., using a PIN of a certain length, a finite number of failed unlocks, etc.) with which mobile devices must comply in order to access email.

One in five of our GCS respondents claimed to not lock their smartphones simply because the idea had not occurred to them. These are not users who are opposed to locking. As we observed during our interviews, several participants locked their devices not because of specific concerns, but because they were asked about it during device setup. These participants continued to lock their devices long after. This suggests that inertia plays a role in the use of locking mechanisms: those who use them tend to continue to do so, even if they cannot cite a specific reason why, while many who do not simply do so because they were never asked. Platform designers could likely get more users to lock their devices by simply asking them if they would like to do so as part of the setup process. This could work on an opt-out basis (e.g., the setup process could require them to set it up, but allow them to visit a settings panel to disable it at a later time), or it could allow them to skip setting it up, but may ask them again in the future.

Finally, we observed that almost 10% of users do not lock their devices because they are worried that emergency personnel might not be able to use their smartphones to notify loved ones. As we noted earlier, applications exist to address this concern by displaying this information on a device's lock screen. Platform designers could directly address this concern by building this feature into the platform, and make it configurable during device setup, so as to make its existence clear to users.

6.3 Rational Rejection?

Our email experiment showed that those who did not lock their phones were able to find significantly less sensitive information in their email accounts; only 27% reported locating sensitive information, as compared to the 38% who locked their smartphones. We also observed that 34% of our GCS respondents did not believe that their devices contained data that would be interesting to others, and therefore opted to not lock them. We do not know where the union of these two sets lies: for instance, it is possible that the 34% who do not believe their devices store sensitive data are entirely correct. If this is the case, the rejection of locking mechanisms may be a rational decision for them. For instance, Herley observed that some security advice that experts give to users is irrational once one compares the value of the resources being protected against the cost of users' time to protect it [23]. In this case, it is possible that many users are correct to not lock their devices because the effort to do so would far exceed the value of the data being protected. Taken as a whole, the time spent unlocking a smartphone is likely non-trivial. For instance, Harbach *et al.* empirically showed that in 27 days, their participants spent an average of over an hour each just unlocking their devices [21].

Locking one's device may not be a one-size-fits-all security practice. That is, while many users are likely to benefit from the practice, this may not be universal. Instead, systems need to be designed to accommodate some amount of nuance with regard to security policies, weighing user needs with risks.

6.4 Limitations

Like all human subjects experiments, our participants were limited to those willing to participate. While the demographics from our online samples were representative of the U.S. Internet-using population, we did notice that our interview sample had a deficit of highly skilled professionals. None of our interview participants reported storing sensitive work-related documents on their smartphones. We suspect that this may have had an effect on the generalizability of our results. For instance, doctors, lawyers, and tech workers might have more sensitive information stored on their smartphones and email accounts (and may or may not take additional precautions to protect that information). However, we believe that any bias here is limited, as highly skilled professionals make up a small proportion of the total population.

Likewise, we also observed that few of our interview participants were parents. We suspect that parents would be likely to have photographs or other sensitive information about their children on their devices, and might therefore have greater concerns about a stranger accessing such photographs or information on a stolen smartphone.

Our interviews and online survey relied on self-reported data. The email search task was self-reported because we could not ethically inspect the email accounts of others in order to measure the prevalence of sensitive information. We designed this experiment so that the same incentive was provided regardless of outcome, and therefore we believe that if there was a bias, it was in favor of under-reporting. Thus, we believe that the numbers we report on risks are likely lower bounds.

6.5 Conclusions

We examined why smartphone users choose or choose not to use a security lock on their phones. We followed this study up with an online survey to examine how our results generalize to the larger U.S. population. We observed that all of our participants use their devices to check their email accounts, regardless of whether or not they choose to lock their devices, and so we performed another online experiment to quantify the frequency with which sensitive information could be obtained via an email account. Based on these experiments, we offered design suggestions to help platforms increase the number of users who use a security lock on their smartphones and to better communicate some of these risks to end users. However, we believe that future work is still needed to validate these suggestions.

7. ACKNOWLEDGMENTS

This work was made possible by Intel through the ISTC for Secure Computing and NSF award number CNS-1318680. We thank Cormac Herley for his feedback, as well as Refjohürs Lykkewe.

8. REFERENCES

- [1] Andriotis, P., Tryfonas, T., Oikonomou, G., and Yildiz, C. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13*, ACM (New York, NY, USA, 2013), 1–6.
- [2] Apple, Inc. Find My iPhone, 2014. <http://www.apple.com/icloud/find-my-iphone.html>.

- [3] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., and Smith, J. M. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies*, WOOT'10, USENIX Association (Berkeley, CA, USA, 2010), 1–7.
- [4] Aviv, A. J., Sapp, B., Blaze, M., and Smith, J. M. Practicality of accelerometer side channels on smartphones. In *Proceedings of the 28th Annual Computer Security Applications Conference*, ACSAC '12, ACM (New York, NY, USA, 2012), 41–50.
- [5] Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., and Wolf, C. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, SP '11, IEEE Computer Society (Washington, DC, USA, 2011), 96–111.
- [6] Bonneau, J., Herley, C., Oorschot, P. C. v., and Stajano, F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, SP '12, IEEE Computer Society (Washington, DC, USA, 2012), 553–567.
- [7] Bonneau, J., Preibusch, S., and Anderson, R. A birthday present every eleven wallets? The security of customer-chosen banking PINs. In *FC '12: Proceedings of the the Sixteenth International Conference on Financial Cryptography* (March 2012).
- [8] Boyles, J. L., Smith, A., and Madden, M. Privacy and data management on mobile devices, September 5 2012. <http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/>.
- [9] Broida, R. How to improve your chances of recovering a lost android phone, February 20 2013. <http://www.pcworld.com/article/2028782/>.
- [10] Chiang, H.-Y., and Chiasson, S. Improving user authentication on mobile devices: A touchscreen graphical password. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '13, ACM (New York, NY, USA, 2013), 251–260.
- [11] Chin, E., Felt, A. P., Sekar, V., and Wagner, D. Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM (2012), 1.
- [12] De Luca, A., Hang, A., Brudy, F., Lindner, C., and Hussmann, H. Touch me once and i know it's you!: Implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, ACM (New York, NY, USA, 2012), 987–996.
- [13] De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M.-E., Slawik, B. E., Hussmann, H., and Smith, M. Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, ACM (New York, NY, USA, 2014), 2937–2946.
- [14] De Luca, A., von Zezschwitz, E., Nguyen, N. D. H., Maurer, M.-E., Rubegni, E., Scipioni, M. P., and Langheinrich, M. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, ACM (New York, NY, USA, 2013), 2389–2398.
- [15] Duggan, M. Cell phone activities 2013, September 19 2013. <http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/>.
- [16] Dunphy, P., Heiner, A. P., and Asokan, N. A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, ACM (New York, NY, USA, 2010), 3:1–3:12.
- [17] Fox, S. 51% of u.s. adults bank online, August 7 2013. <http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/>.
- [18] Frank, M., Biedert, R., Ma, E., Martinovic, I., and Song, D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *Information Forensics and Security, IEEE Transactions on* 8, 1 (Jan 2013), 136–148.
- [19] Glaser, B. G., and Strauss, A. L. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Publishing Company, Chicago, 1967.
- [20] Hang, A., von Zezschwitz, E., De Luca, A., and Hussmann, H. Too much information!: User attitudes towards smartphone sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*, NordiCHI '12, ACM (New York, NY, USA, 2012), 284–287.
- [21] Harbach, M., von Zezschwitz, E., Fichtner, A., Luca, A. D., and Smith, M. 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 2014)*, USENIX Association (Menlo Park, CA, July 2014), 213–230.
- [22] Hayashi, E., Riva, O., Strauss, K., Brush, A., and Schechter, S. 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 (2012), 2.
- [23] Herley, C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *New Security Paradigms Workshop* (2009), 133–144.
- [24] Hitti, M. Put 'ice' on your cell phone. WebMD Health News, October 16 2006. <http://www.webmd.com/news/20061016/put-ice-on-your-cell-phone>.
- [25] Karlson, A. K., Brush, A., and Schechter, S. Can i borrow your phone?: understanding concerns when sharing mobile phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2009), 1647–1650.
- [26] Lookout. Mobile lost & found: Your phone's favorite hiding places, March 22 2012. <https://blog.lookout.com/blog/2012/03/22/>.
- [27] Riva, O., Qin, C., Strauss, K., and Lymberopoulos, D. Progressive authentication: deciding when to authenticate on mobile phones. In *Proceedings of the 21st USENIX Security Symposium* (2012).
- [28] Sae-Bae, N., Ahmed, K., Isbister, K., and Memon, N. Biometric-rich gestures: A novel approach to authentication on multi-touch devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, ACM (New York, NY, USA, 2012), 977–986.
- [29] Schaub, F., Walch, M., Könings, B., and Weber, M. Exploring the design space of graphical passwords on smartphones. In *Proceedings of the Ninth Symposium on*

Usable Privacy and Security, SOUPS '13, ACM (New York, NY, USA, 2013), 11:1–11:14.

- [30] Schechter, S., Brush, A. B., and Egelman, S. It's no secret. measuring the security and reliability of authentication via. In *Proceedings of the 2009 IEEE Symposium on Security and Privacy*, IEEE Computer Society (Los Alamitos, CA, USA, 2009), 375–390.
- [31] Serwadda, A., and Phoha, V. V. When kids' toys breach mobile phone security. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, ACM (New York, NY, USA, 2013), 599–610.
- [32] Simon, L., and Anderson, R. Pin skimmer: Inferring pins through the camera and microphone. In *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, SPSM '13, ACM (New York, NY, USA, 2013), 67–78.
- [33] Starr, C., Rudman, R., and Whipple, C. Philosophical basis for risk analysis. *Annual Review of Energy I* (November 1976), 629–662.
- [34] Takada, T., and Kokubun, Y. Extended pin authentication scheme allowing multi-touch key input. In *Proceedings of International Conference on Advances in Mobile Computing & Multimedia*, MoMM '13, ACM (New York, NY, USA, 2013), 307:307–307:310.
- [35] Uellenbeck, S., Dürmuth, M., Wolf, C., and Holz, T. Quantifying the security of graphical passwords: The case of android unlock patterns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, ACM (New York, NY, USA, 2013), 161–172.
- [36] Van Bruggen, D., Liu, S., Kajzer, M., Striegel, A., Crowell, C. R., and D'Arcy, J. Modifying smartphone user locking behavior. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, ACM (New York, NY, USA, 2013), 10:1–10:14.
- [37] Von Zezschwitz, E., Dunphy, P., and De Luca, A. Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, ACM (2013), 261–270.
- [38] von Zezschwitz, E., Koslow, A., De Luca, A., and Hussmann, H. Making graphic-based authentication secure against smudge attacks. In *Proceedings of the 2013 International Conference on Intelligent User Interfaces*, IUI '13, ACM (New York, NY, USA, 2013), 277–286.
- [39] Wright, S. The symantec smartphone honey stick project. Tech. rep., Symantec, 2012.
- [40] Zhao, Z., Ahn, G.-J., Seo, J.-J., and Hu, H. On the security of picture gesture authentication. In *Proceedings of the 22Nd USENIX Conference on Security*, SEC'13, USENIX Association (Berkeley, CA, USA, 2013), 383–398.

APPENDIX

A. RECRUITMENT ADVERTISEMENT

To recruit our 28 interview participants, we posted the following advertisement to the Craigslist Bay Area “et cetera jobs” forum:

Subject: **Smartphone owners - participate in a study!**

Do you own a smartphone?

Have you been using it for at least 6 months?

If you answered “yes” to both questions, then you may be eligible to participate in a study that looks at how people use smartphones!

The study involves meeting a UC Berkeley researcher for an interview in a public place (i.e., a Starbucks near the Berkeley BART). During the interview, you'll answer questions about the apps you have installed on your phone, the activities you typically use your phone for, and how you use various features on your phone.

The interview will take less than an hour. Participants will receive a \$35 Visa gift card for participating in the study.

To be eligible for this study, you must:

-Be over 18

-Have owned a smartphone for at least 6 months

Please fill out the following survey and we will contact you if you qualify: [URL to the screening survey on SurveyGizmo]

B. PARTICIPANTS' OCCUPATIONS

Our 28 interview participants reported holding the following occupations or working in the following industries:

- Audio engineer
- Student (x2)
- Customer service (x3)
- Healthcare (x3)
- Vendor management
- Publishing
- Financial analyst
- Program coordinator
- Unemployed (x2)
- Teacher
- Journalist (x2)
- Librarian and research assistant
- Retail manager
- City government
- Assistant to stage manager at theater
- Writer (x2)
- Volunteer at hospital
- Startup
- Proof reader
- Professional organizing