# Mobile Device Security: Hopes and Fears

Elizabeth Stobert[1], Irwin Reyes[2], Carrie Gates[3], and Robert Biddle[3]

[1] ETH Zürich
Zürich, Switzerland
estobert@inf.ethz.ch
[2] Irwin's affiliation
USA
[3] Carleton University
Ottawa, Canada

**Abstract.** Users must make a variety of decisions about how to secure their mobile devices. We surveyed users about the types of threats that concern them, and how they configure their smartphones and tablets to protect against these threats. We found that users customize their security approaches on a per-device basis, making different decisions when protecting their smartphones and tablets. This suggests that future security mechanisms for smartphones need to be designed to allow users to take advantage of their security assessments. However, this needs to be balanced with not overcomplicating security for users.

## 1 Introduction

Smartphones and tablets are increasingly ubiquitous in everyday life. Smartphone sales continue to grow every year [23], as more people around the world rely on their mobile devices to be their gateway to the Internet. Because these mobile devices are being used for sensitive tasks such as online banking, social media, and email, there is frequently personal and sensitive information stored on those devices.

The security of mobile devices is thus of utmost importance. From a systems perspective, manufacturers and designers have integrated a variety of security features into mobile devices, ranging from application isolation [2] to device encryption [12]. The significance of these decisions was recently highlighted in a high-profile case involving the FBI's inability to bypass the encryption on an iPhone [6]. These security features address many important aspects of security for mobile devices, but other aspects of security remain in the user's hands. Users must choose whether to lock their device, what type of lock to use, and what password to use.

Extensive research has focused on understanding what kinds of PINs and passwords users choose for their devices [9, 20, 5], or in helping them to select better credentials [22]. However, in this work we are interested more broadly in the spectrum of measures that users take to secure their devices and what threats they are hoping to protect against. Understanding what decisions users make around the security of mobile devices is important to the design of security mechanisms. How do people secure their devices? What kind of protections do their devices need? What motivates their security decisions, and what are the threats that concern them? Particularly, how do they use authentication for their mobile devices?

In this work, we surveyed users about how they protect their mobile devices (both smartphones and tablets), and the types of threats that concern them. We also investigated how users felt about proposed future authentication strategies such as continuous authentication. We conducted a survey with a total of 334 participants. We also asked participants to download an application that collected information about their device configuration, and allowed us to evaluate how users actually behave when asked to download potentially insecure applications to their phone.

Our studies find that people protect their smartphones and tablets differently. They appear to make decisions and reckon about threats on a per-device basis as opposed to a per-user basis. When assessing how to secure their devices they take into account the tasks for which the device is used, the other users of the device, the contexts in which the device is used, and the possibilities for device misuse. We found that people liked the idea of automatic security mechanisms, but were less enthused about the idea of security mechanisms that would require additional decision-making. Based on these results, we suggest that template security mechanisms could be pre-configured for different types of devices, and that recommender systems could be designed to help users customize their security settings to match their specific context and needs.

## 2 Background

The primary mechanism for securing mobile devices is a screen lock. Screen locks are not mandatory on most mobile platforms, and not all users choose to configure this security option for their devices. Studies have found results ranging from around 40% [18, 1, 14, 4] of users locking their phones to around 70 or 80% [13, 10]. A 2013 study by van Bruggen et al. [21] found 65% of their student participants had a screen lock enabled. Harbach et al. [18] conducted a longitudinal field study to investigate threats to smartphones. They asked users to install an application to monitor screen locking and unlocking, and the application also asked users about relevant threats through mini-questionnaires. They found that the average user activated their phone almost 84 times per day, and (fully) unlocked it almost 50 times per day. However, only 43% of surveyed users locked their phones. Egelman et al. [13] conducted a smaller qualitative study and found that 70% of their interview participants locked their phones. In a larger online survey, they found that about 60% of participants locked their phones [13]. In an interview study about handling lockout situations, Hang et al. [15] found that 66% of participants reported locking their phone. A 2016 study of Android locking behaviours in eight different countries found differences in how users of different nationalities perceived the sensitivity of the data on their devices, but the percentage of users who locked their phones was fairly similar across the countries surveyed (ranging from 50% in Italy to 76% in the UK, with a median of 68%).

Variation is also seen in the distribution of types of screen lock used. One study of a student-based population found that 78% of those locking their phones were using pattern locks, while the remainder used PIN or password screen locks [21]. In Harbach et al. [18]'s study, the majority of users who locked their phones used PINs (78%). 20% of participants used a pattern lock, and about 1% used a password. Although they studied users of both Android and iOS, their study was conducted before the introduction of TouchID. A 2015 study of iPhone users by Cherapeau et al. [10] found that 96% of their participants locked their phone, and 46% of participants were using TouchID to lock their phones.

Studies investigating why users do or do not lock their phones have found that users generally discuss privacy issues as reasons for locking their phones, and inconvenience when explaining why they do not lock their phones [13, 18, 10, 17]. Harbach et al. [18] found that users locked their phones for a variety of reasons relating to protection: protecting information, protecting from attackers, and protection in specific scenarios. Users in their study who did not lock their phones mostly cited inconvenience and a perceived lack of threat. Egelman et al.'s qualitative interviews [13] uncovered more nuanced reasons for locking or not locking. Users who locked their phones often had specific scenarios or threats (mainly curious friends and family) that they were trying to avoid. Other users locked their phones because of a generic sense that they *should* lock their phones, motivated by social pressure or by the design of the smartphone user interface.

For users who did not lock their devices, the reasons related to a lack of motivation, concern, and convenience. Users said that having to enter an unlock code frequently was a nuisance [18], and that locking their phone would deny access to someone who needed it in an emergency [13, 10]. Cherapeau et al. [10] found that users who did not use a lock were likely to bring up usability problems with device locking.

### 2.1 Lock Usability

A major usability concern relating to smartphone locking is how long it takes to unlock the phone. Harbach et al. [18] found that unlocking a phone took an average of 2.7s without a passcode, 3.0s with the Android pattern lock, and 4.7s with a PIN. A followup study [16] that collected data about instrumented phones over a one month period was able to tease apart the time spent on different parts of the unlocking process. They found that while the time for users to actually interact with locks was very low ($<$ 1s for all schemes), the preparation time varied between different schemes. The median preparation times were 2.2s for slide to unlock (*i.e.* no lock), 4.3s for pattern unlock, and 9.8s for PIN.

People use their smartphones for substantial periods of time each day. A large scale study of mobile application usage in 2011 [8] found that users spent almost exactly an hour each day on their phone, but that the average length of a session in a single app was only 71 seconds, and that in the majority of sessions, users use only one or two applications.

Al Abdulwahid et al. [3] surveyed users about the comparative usability of various authentication schemes. Respondents in their study were positive about the usability of Android Pattern Unlock, rating it slightly more positively than Apple TouchID, though it was unclear whether users had experience with all systems that they were asked to rate.

Users unlock their phones in a variety of situations. A study by Bhagavatula et al. [7] compared the usability of Apple Touch ID and the Android Face Unlock with traditional PINs. They investigated a variety of usage scenarios and found that when seated, participants rated the biometric unlocks as easier to use. Touch ID and PINs were easy to use in the dark, but the Android Face Unlock was not. All schemes were fairly easy to use while walking, even while carrying another bag, though Touch ID was made more difficult by this. Touch ID was rendered unusable with wet or moisturized hands, while the Android Face unlock performed well in this scenario.

Bhagavatula et al. [7] conducted a survey study of biometric unlocking techniques, and were specifically interested in the Android Face Unlock. They reported having difficulty recruiting users of Face Unlock, and in their survey, only 16% of respondents reported using it. Another survey of biometric authentication on smartphones [11] noted that Face Unlock is not made obvious to users in the Android user interface; for 30% of respondents using Android but not Face Unlock, it was because they were unaware of the Face Unlock option.

Face Unlock users liked the convenience of Face Unlock [7], and considered it to be more secure than a PIN (particularly surprising since Android explicitly warns the user otherwise during the Face Unlock enrollment process) [7, 11]. Other respondents who reported having previously used Face Unlock said that it was unreliable, especially in low-light situations. De Luca et al. [11] also found that some participants had stopped using Face Unlock because of the social undesirability of holding the phone in front of their face to authenticate.

## 3 Method

To investigate the security habits of users with regard to their mobile devices, and to better understand how these behaviours differ across device types, we conducted a study on Mechanical Turk. The goal of the study was to better understand the security habits of Android users, regarding smartphones and tablets. The study had two parts: a survey about security behaviour on mobile devices, and an installation of our `Device Surveyor` application on a phone. The study was approved by our university's ethics review board.

The main part of the study was a survey about how users secure their devices, both smartphones and tablets. We asked questions about whether users lock their devices, what they are concerned about protecting on the device, and what they perceive as the major threats. We also asked about participants' level of interest in future authentication mechanisms (such as continuous authentication) available on their devices. The survey also asked a few questions about respondents' demographics. The survey questions were designed to investigate our subjects of interest, and we consulted studies in the literature to ensure that available responses encompassed known possibilities [13, 18]. To avoid pushing participants to make exclusive responses that did not encompass the breadth of their experience, we structured the majority of questions as multiple choice questions where the participant was able to choose as many options as they wished. This also allowed us to look at the co-occurrences of multiple answers. To avoid response bias, we randomized the order of presentation for question responses.

`Device Surveyor` was developed by us, and was designed to extract and assemble a report with technical details about the device on which it is installed. These details included the model and manufacturer, the version of Android running on the device, the screen size and resolution, the keyboard and language, the type of lock enabled, and whether the device had root access enabled (i.e. "was rooted"). None of the details were personally identifying, and the participant was asked to review the generated report and and anonymously submit it to our web server before proceeding to the second part of the study. We chose to distribute `Device Surveyor` as a sideloaded app rather than through the app store so that we could examine potential differences between participants who were or were not willing to take the risk of installing it.

## 4 Results

### 4.1 Demographics

334 participants completed the survey, and of these, 40% were women. The majority of respondents were aged between 25 and 34. Approximately 78% of participants lived in North America (almost all from the USA), and the 20% were from Asia (primarily India). Only three participants did not live in either Asia or North America.

In general, our sample was highly educated. 152 participants (84%) said that they had at least some university or college education, and 90 respondents reported having completed a university degree, either undergraduate or graduate. We coded respondents' occupations according to a national occupation classification, and classified participants who listed themselves as students, homemakers, retired, unemployed, or those who listed their primary occupation as working on Mechanical Turk as not part of the labour force. Respondents reported working in a large range of fields, and the three largest occupation areas were natural and applied sciences (primarily information technology), sales and service, and business and finance (many in the context of small business ownership).

Almost all of our survey respondents (327 of 334) reported having a smartphone, and 199 of them reported having a tablet (192 reported having both). Our survey asked questions about security behaviour separately for smartphones and tablets. In the next sections, we present the findings from the `Device Surveyor` reports, then the survey findings for each device type.

### 4.2 Device Reports

While not prohibited by the Mechanical Turk Terms of Service, downloading applications from outside the Google Play store has security risks, and we were unsure whether study participants would be willing to take this risk to install `Device Surveyor`. Because we developed and distributed the application ourselves, we were able to assure participants that it was secure, but participants had no particular reason to trust us. The application was written for the Android operating system, meaning that only users with Android devices were eligible to participate in our study. We conducted our total data from two samples, one where the `device surveyor` step was mandatory and one where it was not (otherwise, the studies were identical).

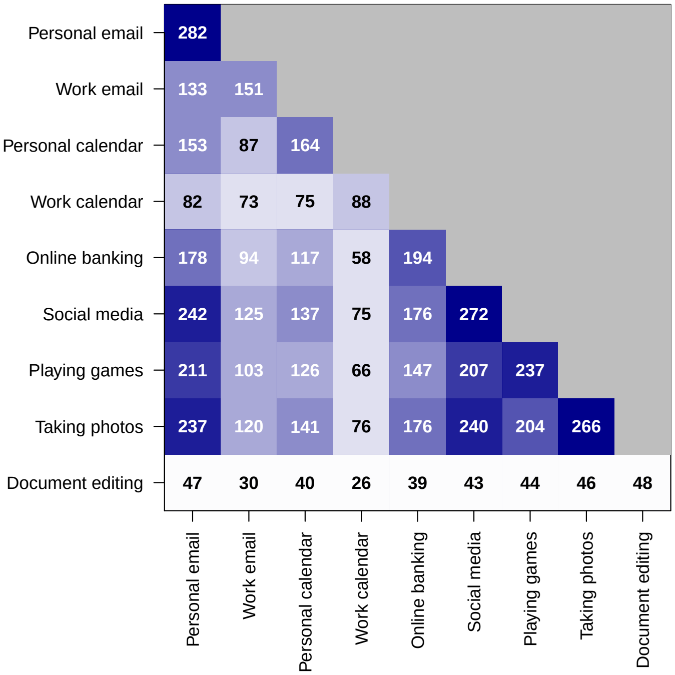
In total, 187 people completed the device report (180 in the first part, and only 7 in the second). Only 10% of participants that completed the device report had root access enabled on their phones. The majority of these were men (14 participants), and came primarily from North America. They listed a variety of occupations and it was not clear that users with rooted devices had primarily IT backgrounds.

The first sample was set up so that only participants who were willing to download and install the Android application were permitted to complete the survey. This meant that the survey sample was composed of people who had demonstrated their willingness to install applications from outside the Google Play store. Android notifies users doing this at the time of installation that there are associated risks to installing these applications, so we assume that our survey respondents were all reasonably cavalier about security risks (or perhaps influenced by the clearance of our research ethics board). In the second sample, the download step was optional and only a few participants participated in that part of the study. While we cannot conclusively say that the participants in the second sample were unwilling to download the application for security reasons (it also saved them time and effort), we do know it was easier and faster to find participants for the second sample.

Demographically, the two samples were very similar: breakdowns of gender, age, education, occupation and location appeared alike. Reported security behaviour was also very similar: about the same percentage of each sample locked their mobile devices, and they were interested in the same kinds of security mechanisms. To avoid repetition, we chose to combine the two samples when discussing the results.

### 4.3 Smartphone Security Behaviour

The majority of the 327 smartphone users who completed our survey were experienced users. 83% of participants had owned a smartphone for at least 3 years and when asked to rate their level of smartphone expertise, the median response was 6 on a scale from 1:Novice to 7:Expert. 41% of respondents reported checking their phone at least once every 15 minutes. Participants were overwhelmingly likely to say that they carried their device with them “often”



| | Personal email | Work email | Personal calendar | Work calendar | Online banking | Social media | Playing games | Taking photos | Document editing |
|---|---|---|---|---|---|---|---|---|---|
| Personal email | 282 | | | | | | | | |
| Work email | 133 | 151 | | | | | | | |
| Personal calendar | 153 | 87 | 164 | | | | | | |
| Work calendar | 82 | 73 | 75 | 88 | | | | | |
| Online banking | 178 | 94 | 117 | 58 | 194 | | | | |
| Social media | 242 | 125 | 137 | 75 | 176 | 272 | | | |
| Playing games | 211 | 103 | 126 | 66 | 147 | 207 | 237 | | |
| Taking photos | 237 | 120 | 141 | 76 | 176 | 240 | 204 | 266 | |
| Document editing | 47 | 30 | 40 | 26 | 39 | 43 | 44 | 46 | 48 |

**Fig. 1.** Activities frequently conducted on smartphones. Frequencies shown out of 327 smartphone users. Participants were allowed to choose more than one response, so frequencies do not sum to 327.

or "always" (95%). 79% carried only one smartphone. Of the participants with more than one smartphone, almost all had two phones.

When asked about the activities they conduct on their smartphone, participants were most likely to say that they used their phones for personal email, social media, taking photos and playing games. Figure 1 shows a co-occurrence matrix where all activities are shown along the x- and y-axes. The diagonal shows how many participants reported doing that activity, and the darker colours show higher frequencies. The other entries show how many participants reported doing both activities). In general, respondents were less likely to say that they use their phones for work purposes.

Almost two thirds of participants (205 participants, 63%) said that they lock their phone. Of those who did lock their phones, 48% reported using a pattern lock and 30% reported using a PIN. The remaining participants used fingerprint scanners (12%) or passwords (9%). Participants who locked their phones were most likely to say that they locked their phone to protect specific information on the phone, to protect it in the case of a specific situation (such as loss or theft), or both (Figure 2). Participants were most likely to say that they

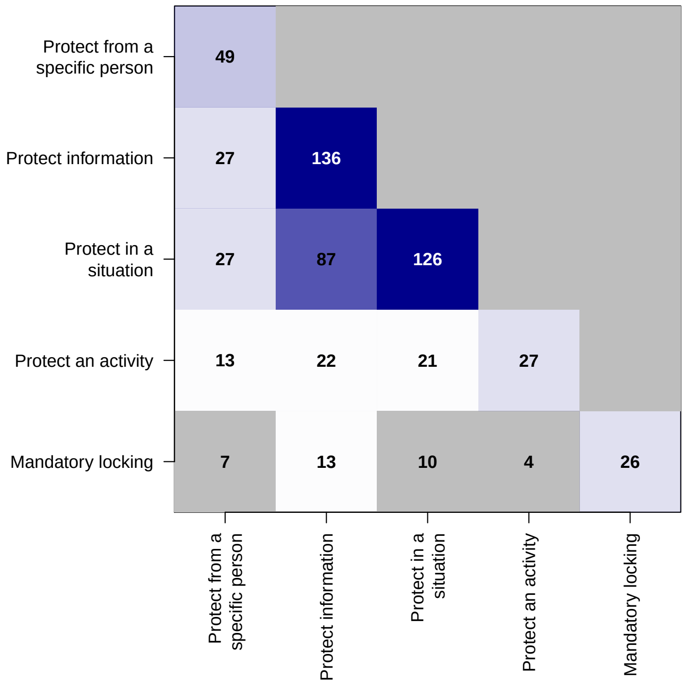


**Fig. 2.** Reasons why users lock their smartphones. Frequencies shown out of 205 smartphone users who lock their phone. Participants were allowed to choose more than one response, so frequencies do not sum to 205.

were protecting emails/messages, photos, and personal information (or some combination thereof). Activities that specifically concerned participants were most likely to be data and internet use on the phone. Among the 122 participants who said that they did not lock their phone, the most common explanations were inconvenience (42%) and being unconcerned about security (30%).

When asked about who else uses their smartphones (Figure 3), respondents' primary response was spouses. Children and friends occurred, but were less common. 72% of respondents said that their phone was used by some kind of family member, making this the predominant phone-sharing scenario. Almost 75% of the 327 respondents said they were not concerned about these other users accessing their personal data. Of these, 62% said that they had nothing to hide (presumably from these family members). For those who were concerned about others using their device, common protection strategies included locking the phone, and making sure to keep the phone nearby.

We were also interested in how users feel about about the proposed future authentication technologies such as continuous authentication mechanisms. Most respondents (78%) liked the idea that their phone could automatically detect

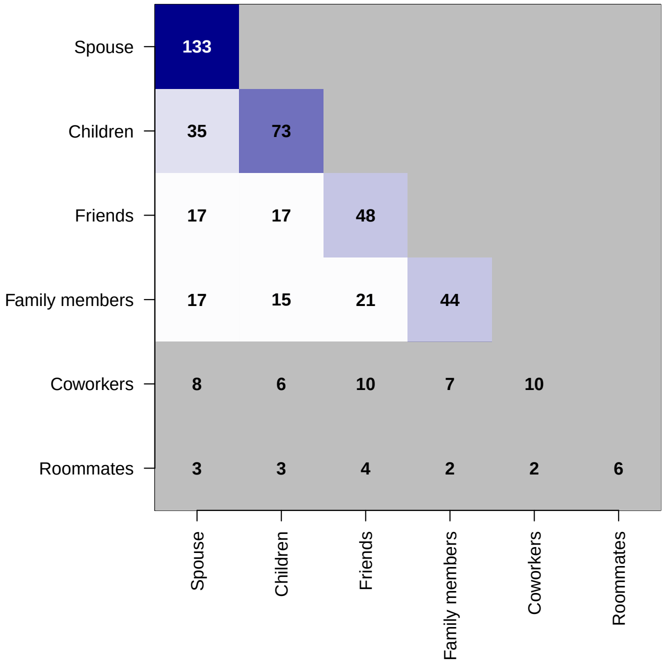


**Fig. 3.** Additional users of smartphones. Frequencies shown out of 327 smartphone users. Participants were allowed to choose more than one response, so frequencies do not sum to 327.

unauthorized users and lock them out, but respondents were warier of the idea of application-specific restrictions (58% disapproval).

In a write-in question where respondents were asked how they protect their data on their smartphones, participants described a variety of non-technical approaches to securing their data, including physical security (keeping the phone in close proximity to them), installing additional security applications (anti-virus applications or “app-lockers”), or enabling guest mode for additional users. The type of data specifically mentioned by respondents was mainly financial, with a few references to photos, personal information, and work files.

### 4.4 Tablet Security Behaviour

For participants who reported owning a tablet, we asked the same set of questions separately about how they use and protect their tablets. Fewer users in our survey had tablets as well as smartphones: only 199 people had tablets compared to 327 with smartphones (however, almost all owners of tablets also owned a smartphone).

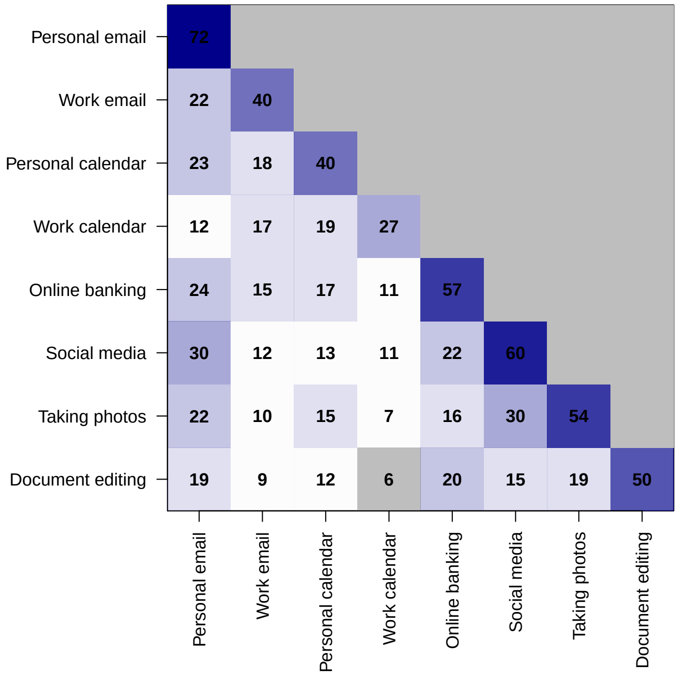


**Fig. 4.** Activities occasionally conducted on tablets. Frequencies shown out of 199 tablet users. Participants were allowed to choose more than one response, so frequencies do not sum to 199.

The pattern of use appeared quite different for tablets and smartphones. 83% of participants who owned tablets (165 participants) used only one tablet regularly, and the majority (77%) reported looking at their tablets less than once per hour. Correspondingly, participants were much less likely to say that they regularly carried their tablets with them than phones. 68% said that they only carried their tablets "sometimes" or "seldom", and 13% said that they never carried their tablets with them.

Playing games, personal email, and social media were the most common activities for which participants frequently used their tablets. The range of activities frequently performed on tablets was much narrower than those on smartphones, where frequent activities were more numerous and more diverse. However, the range of activities that participants reported doing "sometimes" on their tablets was wider (Figure 4). This pattern was opposite to what was seen with smartphones, and fits into a wider pattern that people use their smartphones "frequently" and their tablets "sometimes".

63% of tablet users (124 participants) did not lock their tablets. This was a reversal of the smartphone statistics, where 63% of users locked their devices. Of

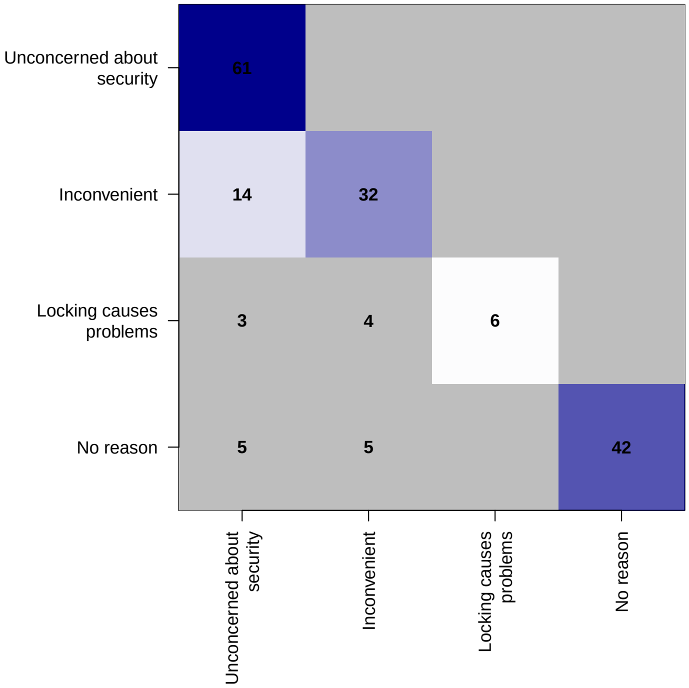


**Fig. 5.** Reasons why users do not lock their tablets. Frequencies shown out of 124 tablet users who did not lock their tablets. Participants were allowed to choose more than one response, so frequencies do not sum to 124.

participants who said they had both a smartphone and a tablet (192 users), this proportional reversal was still true, meaning that locking seems to be related to device considerations, not personal preferences. For the 37% of tablet owners (75 participants) who locked their tablets, the most common type of lock used was a PIN (61%). When asked why they locked their tablets, participants were most likely to say that it was to protect the tablet in a certain situation (loss (47%) or theft (48%)). To a lesser extent, users also said it was to protect a specific activity (activity of concern was primarily internet use (9%)), or to protect it from a specific person (a child (12%), or a coworker (8%)).

For the 124 tablet users who did not lock their tablets (Figure 5), the primary reason was a lack of concern about security. Others cited inconvenience, or said that there was no reason that they did not lock their tablet. When asked why they were unconcerned about security, people said that they kept no sensitive data on the device (46%) or had nothing to hide (61%). To a lesser extent and in conjunction with these reasons, users also indicated that they trusted the people who had access to the device.

Tablets were also likely to be used by family members, primarily spouses (44%) and children (33%). Users were overwhelmingly unconcerned about these additional users accessing their personal data (87% said they were unconcerned), and most (59%) said it was because they had nothing to hide.

Users were not especially enthusiastic about the idea of having users automatically detected and locked out of their tablets (53% agreement), and they were overwhelmingly uninterested in being able to restrict access to certain applications on the phone (80% disagreement). It appears that the different use case for tablets significantly impacts the way that users think about and conceptualize security for these devices.

When asked about how they protect their data from other users of their tablets, multiple respondents said they kept no personal data on the tablet, and the responses seemed to indicate that many tablets were freely shared among family members.

## 5 Discussion

We found distinctions in users' security concerns and behaviours on smartphones and tablets. Users were more obviously concerned about the security of their smartphones, and presumably for sensible reasons: it appeared that smartphones were used more frequently, and for applications of all types (including sensitive applications), were taken more places, and were more exposed to more users.

Tablets appeared to be primarily used for entertainment purposes in the context of the home, and by a circumscribed set of users. Although participants were concerned about theft or loss, the monetary value of the device itself seemed to be of more concern than the information on it. In write-in responses, several participants mentioned that their device was shared for entertainment by other family members (mainly children). Correspondingly, participants seemed less concerned about the security of these devices.

The differences between how people secure smartphones and tablets shows that people do consider the likelihood of threats to the device and tailor their security behaviour to those assessments. People do not have a "personality type" for security – they are not "security aware" or unaware, but rather they are judging their behaviour by an assessment of value for each device. This includes a complex evaluation of what they use the device for, what data is stored on it, who uses the device, and what might plausibly happen to the device.

Although this is an encouraging result, one problem is that users might not be aware of the true threats to the device. Issues like application spoofing and mobile malware are not protected by the kinds of measures explored in our survey. Previous work [19] has found that users show a poor understanding of the differences between appropriate authentication for mobile devices and those for online applications, such as email. We suspect that the users in our survey may also have been making incorrect assumptions or evaluations of risks and defences.

The set of technical means by which users can protect their devices is fairly limited: devices can have locks enabled (with a variety of types of password), can be encrypted, can make use of a guest account, or be remotely wiped. Other protection mechanisms are non-technical: the user can protect the physical security of the device by hiding it, or limiting who has access to the device. The user might also decide to limit information stored on the device, and might try to protect the device security by installing fewer applications. However, these are imperfect defences and it can be hard for anyone to know to what extent these behaviours actually protect security. Regardless of concerns, there are simply not that many options for how to secure a device.

This suggests that a higher level of granularity is needed: users can and do reason about different threats and attack vectors, but cannot protect against them in a targeted way. Of course, the usability challenges of granular security also need to be addressed. Users do not have extra time to spend on configuration, and the configuration mechanisms need to be carefully designed so that users can understand them, and avoid making dangerous errors.

As we see further integration between mobile and desktop operating systems, an issue that will need to be addressed is security for different devices. Should the same security features be made available on different types of devices? The results of our survey show that many users are less concerned about security for their tablets than for their smartphone. One possible approach could be to configure default security options differently for different device-types. For example, in a recent release, Apple iOS began requiring 6-digit PINs (rather than the previously required 4 digits) for all new devices. While this is likely justifiable for smartphones, it appears less necessary for tablets. Perhaps tablets could have been left with 4-digit PINs as the default, accounting for their use contexts. Users who store sensitive data on their tablets, or frequently take them outside the house could be given the choice to increase the length of the PIN. Another idea might be that depending on the likelihood of shoulder surfing, a system might make the masking of passwords a configurable option. The risks of shoulder surfing could be higher for a smartphone used frequently on the street than for a tablet used mainly in private.

As part of our survey exploration, we asked users about their interest in future authentication mechanisms. Because we anticipated that most respondents would be unfamiliar with what was meant by continuous authentication, we described the system as one where unauthorized users would be “automatically” locked out of the system, and did not mention the technical means by which this would be evaluated. We speculate that one possible reason that respondents were enthusiastic about this is that they liked the idea of security mechanisms that required little effort for them. This points to another way in which pre-evaluating the needs of the situation could benefit users by taking some of the burden of configuration away from them. A wizard or recommender system could guide users through the set-up process for device security, asking a few quick questions about the device’s context of use, and could then recommend a security configuration based on the user's responses. Users could still tweak the settings, but would have a plausible starting point.

### 5.1 Limitations

The results presented here are preliminary, and we intend them as a jumping-off point for future study and design. Although our results are in line with the findings of related work [18, 16, 13], it is possible that our results were affected by the demographics of our sample. Our participants were primarily young, male, and educated, and it is not completely clear whether their habits and behaviours generalize to the rest of the population. It is also possible that people choosing to work on Mechanical Turk have higher awareness of computer security issues than the general population. In particular, participants who were willing to download and install an application outside the app store may have more lax security standards.

## 6 Conclusion

Based on the results of our studies, users are making considered decisions about security for their mobile devices. They are taking different measures to protect different devices, and assessing environmental and contextual factors along with the information stored on the device when deciding what security measures to implement on each device.

This creates a design opportunity to tailor protection mechanisms to different threats, and to let users layer those protections to address their specific situations. Security mechanisms for mobile devices are limited: the choice is whether or not to enable a lock screen, and what password might be chosen. This means that regardless of what they perceive as the threat, users are currently unable to customize the defence to match that threat, and take advantage of their own evaluations of risk and defence.

We suggest that pre-configuring security settings on a per-device basis could be a useful way of guiding users toward appropriate security decisions for their mobile devices. Existing and additional research on how users secure their devices and assess threats to those devices could be used to create "template" security settings or a recommender system to help people sensibly secure their mobile devices.

However, designing customizable options could be a double-edged sword – users are unlikely to want to invest more work into securing their devices, and like the idea of automatic security mechanisms. The design of a system such as this would need to carefully consider issues such as error avoidance and user comprehension.

This is exploratory work. Further work is needed to better understand the nuance of how users protect their devices and what kind of rationales they develop. We suspect that users are not always reasoning accurately about threats to their devices and may base their security decisions on false evidence, incorrect assumptions, or missing knowledge. The nature of survey-based studies means that we did not have a method for investigating these issues.

The results of our studies are promising: users do care about security, and do consider it. They are reasoning about threats and adjusting their expectations to their threat assessments. Users do not need to be convinced that they should care about security, but they do need guidance in accurately assessing risks and understanding effective ways to protect against those risks.

## 7 Acknowledgements

We would like to thank our shepherd, Markus Dürmuth for his help in preparing the paper. We acknowledge support from Dell Research and from a Natural Sciences and Engineering Research Council of Canada Discovery Grant.

## References

1. Cell Phone Security — Wireless Threats. *Consumer Reports*, June 2013.
2. Y. Acar, M. Backes, S. Bugiel, S. Fahl, P. McDaniel, and M. Smith. SoK: Lessons Learned From Android Security Research For Appified Software Platforms. In *IEEE Symposium on Security and Privacy (SP '16)*. IEEE, 2016.
3. A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich. Security, Privacy and Usability – A Survey of Users' Perceptions and Attitudes. In *link.springer.com*, pages 153–168. Springer, 2015.
4. P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz. 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, 2013.
5. A. J. Aviv, D. Budzitowski, and R. Kuber. Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. In *The 31st Annual Computer Security Applications Conference*, pages 301–310. ACM, 2015.
6. BBC News. FBI 'May be able to unlock San Bernardino iPhone'. `http://www.bbc.com/news/world-us-canada-35868322`, Mar. 2016.
7. C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides. Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. In *USEC '15*, pages 1–10, San Diego, CA, 2015.
8. M. Böhmer, B. Hecht, J. Schöning, A. Krüger, and G. Bauer. Falling asleep with Angry Birds, Facebook and Kindle: a large scale study on mobile application usage. *Mobile HCI*, pages 47–56, 2011.
9. J. Bonneau, C. Herley, P. van Oorschot, and F. Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *IEEE Security and Privacy*. IEEE, 2012.
10. I. Cherapeau, I. Muslukhov, N. Asanka, and K. Beznosov. On the Impact of Touch ID on iPhone Passcodes. In *SOUPS 2015*. USENIX, 2015.
11. A. de Luca, A. Hang, E. von Zezschwitz, and H. Hussmann. I Feel Like I'm Taking Selfies All Day! Towards Understanding Biometric Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*, pages 1411–1414. ACM, 2015.

12. M. Egele, C. Kruegel, E. Kirda, and G. Vigna. Pios: Detecting privacy leaks in ios applications. In *Network and Distributed Security Symposium (NDSS '11)*. Internet Society, 2011.
13. S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors. In *Proceedings of the SIGSAC Conference on Computer and Communications Security (CCS '14)*, pages 750–761. ACM, 2014.
14. A. Goode. Bring your own finger – how mobile is bringing biometrics to consumers. *Biometric Technology Today*, (5):5–9, 2014.
15. A. Hang, A. de Luca, E. von Zezschwitz, M. Demmler, and H. Hussmann. Locked Your Phone? Buy a New One? From Tales of Fallback Authentication on Smartphones to Actual Concepts. In *MobileHCI '15*, pages 295–305. ACM, 2015.
16. M. Harbach, A. De Luca, and S. Egelman. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI '16)*. ACM, 2016.
17. M. Harbach, A. De Luca, N. Malkin, and S. Egelman. Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI '16)*. ACM, 2016.
18. M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2014.
19. E. Stobert and R. Biddle. The Password Life Cycle: User Behaviour in Managing Passwords. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2014.
20. S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. *Proceedings of the SIGSAC conference on Computer & Communications security (CCS '13)*, pages 161–172, 2013.
21. D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy. Modifying Smartphone User Locking Behavior. In *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, 2013.
22. R. Weiss and A. de Luca. PassShapes – Utilizing Stroke Based Authentication to Increase Password Memorability. In *NordiCHI*, pages 383–392. ACM, Oct. 2008.
23. V. Woods and R. van der Meulen. Gartner says worldwide smartphone sales grew 9.7 percent in fourth quarter of 2015. `http://www.gartner.com/newsroom/id/3215217`, Feb. 2016.