Pervasive and Mobile Computing 32 (2016) 50–61

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Android users in the wild: Their authentication and usage behavior

Ahmed Mahfouz [a,b,*], Ildar Muslukhov [a], Konstantin Beznosov [a]

[a] Department of Electrical and Computer Engineering, The University of British Columbia, 2332 Main Mall, Vancouver, B.C., Canada V6T 1Z4
[b] Computer Science Department, Minia University, El-Minia, 61519, Egypt

ARTICLE INFO

Article history:
Available online 11 July 2016

Keywords:
Smartphone authentication
Unlocking mechanisms
Smartphone usage
Usability
Measurement

ABSTRACT

In this paper, we performed a longitudinal field study with 41 participants, who installed our monitoring framework on their Android smartphones and ran it for at least 20 days. We examined how unlocking mechanisms perform in the wild in terms of time it takes to authenticate and error-rate, and how the users' choices of the unlocking mechanisms are linked to the different patterns of smartphone usage. Based on our findings, we offer insights into improving Android unlocking mechanisms and related user experience.

1. Introduction

Smartphones have become ubiquitous personal devices, widely used by a very broad and diverse population, from teenagers, to students, to business users, to senior citizens. Due to this diversity of users as well as smartphones' inherit customizability and extensibility, the patterns of their usage vary widely. Yet, one trait is more and more common for all these users: the smartphones are becoming very personal devices that store a plethora of sensitive personal information and serve as gateways to many online services, from e-mail, to banking, to social media, to online dating. Unsurprisingly, unauthorized access to the device is the highest security risk for smartphone users [1–3].

To protect this information and their online accounts from unauthorized access, many users lock their phones (which requires entering a secret to unlock). Yet, others do not, risking the data and online services accessible through their devices [4–6]. Inconvenience, lack of motivation and awareness were the most common reasons for not-locking smartphones [7,4,8]. The research community is struggling to understand the interplay between (a) the security and usability of unlocking mechanisms, (b) the smartphone usage patterns, and (c) the willingness of users to lock their ever so personal devices. While the security and usability of smartphone standard unlocking mechanisms have been extensively studied in laboratory conditions and through surveys (e.g., [9–12]), it is largely unclear (1) how these unlocking mechanisms perform in the wild, and (2) how their choice by users is correlated with the different patterns of smartphone usage.

Empirically answering these questions is critical for informing and grounding the improvements to existing unlocking mechanisms and the evaluation of new proposals. Researchers and developers need to understand (1) the actual cost that users incur when unlocking their phones, (2) how the choice of the unlocking mechanisms is linked to the phone usage patterns, (3) how much the cost is "amortized" through the use of apps on the smartphone, and (4) once the users unlock their phones, how sensitive the apps that the users utilize are.

[*] Corresponding author at: Department of Electrical and Computer Engineering, The University of British Columbia, 2332 Main Mall, Vancouver, B.C., Canada V6T 1Z4.
E-mail addresses: ahmedmahfouz@ece.ubc.ca (A. Mahfouz), ildarm@ece.ubc.ca (I. Muslukhov), beznosov@ece.ubc.ca (K. Beznosov).

http://dx.doi.org/10.1016/j.pmcj.2016.06.017
1574-1192/© 2016 Elsevier B.V. All rights reserved.

We have conducted a field study in order to obtain empirical data on user behaviour when it comes to locking, unlocking, and using Android smartphones. Android is the most popular mobile platform worldwide, with more than one million new devices activated every day [13]. We instrumented participants' smartphones with a monitoring framework that (transparently to the user) recorded events relevant to the device unlocking and using habits. By deploying our monitoring framework on Android phones of 41 participants in a 20 day-long field study, we have collected data for understanding Android mainstream unlocking mechanisms: PIN, password, and "draw a pattern". (Pattern, for short.)

In total, we collected some 417,000 events, of these, 187,000 low-level events related to unlocking process, and 230,000 events related to apps and sessions interactions. We observed, participant interacts around 51 times on average per hour, assuming that the user use the smartphone for 10 h per day, where each event represented by one of the following actions, screen on/off, unlocking success/failure, session start/end, or app foreground/background. Among our 41 participants, 22 locked their smartphones, which is aligned with previous findings [4,3]. Out of these 22 participants, two used alphanumeric passwords, five used PINs, and the rest (15) used patterns to unlock their phones. These 22 participants interacted with their phones longer and more often than their counterparts that did not lock. One possible explanation could be that the former participants used their phones more and, as such, saw more value in the phones as well as the data and services provided through them, and therefore were willing to put an effort of securing their phones.

We found that Pattern outperformed PIN and Password methods in entry-time, while PIN had the highest success-rate. With each participant unlocking their device on average 46 times a day, rates for single unlocking errors were in the range of 0.6% (PIN) to 2.7% (Pattern) to Password (3.7%), and significantly fewer repeating errors. Yet, the error rate did not seem to be an impeding factor for adoption of unlocking methods. At the same time, Password method, which increased unlocking entry time to 4.1 s, was 9 times less likely to get adopted by the users of PIN (2.5 s) or Pattern (1.7 s). These results seem to suggest that entry-time might be a significant factor for adoption by users, and proposals for novel device unlocking methods should be carefully evaluated in that respect.

While almost half of the subjects (most of whom used Pattern) set auto-lock timeout to *immediately*, others set it to relatively large values, thus, increasing the chances for an attacker. In particular, we found that, on average, 11% of all device locks were due to auto-lock, and each device was unlocked for 65 s after the screen was turned off. This provides an opportunity window for so called *lunch-time* attacks, when someone sneaks into a smartphone if the owner left it unattended.

We discovered that short sessions are most common, with 50% being 51 s or less, with one third involving only one app, and almost two thirds involving at most three apps. The 10 most frequently used apps (out of 564) were responsible for about half of the 80,570 app sessions. Given the length of participants' sessions and the absolute times of entering unlocking secrete, the relative cost of unlocking varied from 2%–3% for 100-s sessions with PIN/Pattern method to up to 80% for short sessions with Password method.

While each of the 22 participants who locked their phones used their device for 43 min a day on average, only 100 s a day in total were spent by each Pattern or PIN participant (and 200 s by each Password participant) on unlocking their phone.

Our contributions are as follows:

- Through a longitudinal field study we collected real events on users' (un)locking behaviour and mobile device usage.
- Using the collected data, we analyzed the use of smartphones and their sessions as well as Android screen-lock methods (Pattern, PIN, and Password).
- Based on our findings, we offer insights into improving Android unlocking mechanisms and related user experience.

2. Background and related work

Smartphone unlocking methods such as Pattern, PIN and Password, protect smartphone data from unauthorized access. All of them act as protection layer that verifies the identity of the user. In this section, we provide an overview of screen-lock methods in Android. Then, we present previous work on user unlocking behaviour on smartphone followed by a literature of some alternative authentication methods.

2.1. Android screen-lock methods

Android smartphones have different screen-lock methods which help users to protect their phones from unauthorized access [14]. These methods provide different levels of security. For instance, "None" and "slide-to-lock" provide no security, while locks based on authentication methods, such as Password or PIN, provide security that depends on complexity of underlying authentication method [15,9]. In addition to a password-like authentication secrets users can also use method based on Draw-A-Secret [16,17], or simply Pattern. Such method allows users drawing a pattern in order to unlock their devices. Recent developments in Android OS by Google has introduces new type of lock, called smart lock. This feature allows unlocking the device automatically when it can connect to a trusted device (e.g., Watch).[1]

[1] This feature available only for Android 5.0 or higher.

2.2. Smartphone unlocking

Different research has been conducted to study the unlocking mechanisms in smartphones [18–20,4,9]. For instance, Uellenbeck et al. [9] studied users choice of unlock patterns and their strength. Authors found a strong bias in pattern selection process that made selected patterns more predictable. They proposed some changes on pattern layout in order to increase its strength by reducing bias in patterns selection. On the other hand, Schaub et al. [20] performed a comparative study between different graphical password schemes. They measured the efficiency of each scheme in terms of entry time, success rate and user satisfaction. The authors showed the impact of smartphone capabilities on graphical password design features. In comparison, in our study we collected daily activities of smartphones users in the wild. That is, we collected how currently deployed authentication methods are performing in real-world settings, rather than laboratory environment.

Real world studies have been conducted by others as well. For example, von Zezschwitz et al. [19] conducted a field study to evaluate performance of PIN and Pattern based authentication methods in smartphones. For that they developed an Android-like user interface that asked subjects to enter authentication secrets and random points in time. They quantitatively analyzed the input speed, error rate of both methods. They found that the input speed of PIN authentication method was faster than Pattern. Authors also highlighted that both input speed and success rate have been influenced by availability (or absence) of error recovery. In addition, they used a questionnaire to measure the usability, likability and memorability of the methods under investigation. In contrast, the scope of our study is much boarder: we quantitatively measured the performance of real screen-lock methods (Pattern, PIN and Password) in Android OS. Furthermore, we investigated the anatomy of used sessions to understand associated sensitivity and authentication costs.

Van Bruggen et al. [7] conducted a study to observe user's behaviour with different kinds of screen lock. They concentrated on the effect of intervention on user's behaviour based on incentives, morality and deterrence principals. They showed that the majority of users use a screen lock without direct intervention. Harbach et al. [8] performed two users studies in order to understand users' risks perception while unlocking smartphones. First, they conducted an online survey to elicit users' opinions in regards to screen-locking, motivation to lock and risks assessment. Second, they asked users about their perceptions of risks at a given context, i.e., environmental settings, such as risk of being shoulder-surfed. Their main finding was that users not only suffered from many unlocks of their smartphones per day, but they also underestimated risks. Similarly, Egelman et al. [4] conducted a qualitative user study in order to understand users locking behaviour. In particular, the authors focused on reasons users choose to lock or not lock their smartphones. Finally, to quantify their results, they followed up with an online survey to measure how users perceive risks. In contrast, we collected quantitative data on users activities with their smartphone related to unlocking events and application usage.

3. Methodology

We conducted a longitudinal field study with 41 participants. The participants took part in our study during different time periods, all between December 20, 2014 and March 13, 2015, for at least 20 days each. Participants installed our application through the Google Play Store. The installed application ran as a background service in the phone of each participant, collecting transparently to the user all the interesting events. In order to increase the reliability of our data collection, our app sent on a daily basis the collected data to our back-end server. The data was encrypted with the corresponding public key and we decrypted the data after downloading it from the server to our research computer. Before collecting the data, we obtained approval from our university's research ethics board. We piloted data collection and analysis with 8 participants recruited on our university campus.

3.1. Participant recruitment

We recruited participants through an advertisement campaign.[2] The recruitment notice was posted on our university's mailing lists, Craigslist, Kijiji, Facebook, Google Ads, and flyers distributed on our university campus. The recruitment notice included a brief description of the study and a hyper-link to our study app on Google Play. According to the inclusion criteria, we accepted only adult participants (19 years or older) who had Android smartphones. As an appreciation for their time spent participating in our study, those participants who downloaded and completed the study were included in a raffle of one iPadAir2.

Initially 57 participants successfully installed and activated our study app. We excluded 16 participants; 14 of them did not complete the study. We also found that one participant registered three times. As such we only kept (the longest) one of this participant's data logs. On the launch, our study app first showed a consent form, which each participant had to accept for the app to continue. Then, it presented the participant with demographics questionnaire.[3] As shown in Table 1, 28 (68%) participants were males; ages ranged from 19 to 53 years old, with mean age 26.5 and median 26. They were using different versions of Android OS, ranging from v2.3.6 to v5.0.1, where version 4.4.2 was the most popular, which is in line with the statistics of the Android market [21].

[2] Approved by our IRB under protocol # H14-02707.

[3] Our app could also show the number of days elapsed since the start of the participation in the study.

Table 1
Participants demographics, $N = 41$.

Parameter	Property	# of participants
Gender	Males	28
	Females	13
Age	19–24	18
	25–30	15
	31–40	5
	41–53	3
Education	Master or Ph.D.	15
	University (Bachelor's)	18
	High school	5
	Professional school	3
Job	Student	11
	Researcher or staff	10
	Engineer	7
	Professional worker	7
	Government employee	2
	Unemployed	4

Table 2
Android broadcast actions used during data collection.

Action	Description
ACTION_SCREEN_ON	Screen turned on and device becomes interactive.
ACTION_SCREEN_OFF	Device goes to sleep and becomes non-interactive.
ACTION_USER_PRESENT	Device waked up, unlocked and the user is present.
ACTION_PASSWORD_FAILED	User entered wrong password, PIN or pattern.
ACTION_PASSWORD_SUCCEEDED	User entered successful password or pattern.

3.2. Data collection

Our study app was collecting data on the participants' devices. The app was designed to work on Android OS v2.3.6 and up, which represent the most common versions of the Android OS (greater than 95%) [21].

Our study app consisted of background services and broadcast receivers that logged user's actions. The logged data was collected and stored on the smartphone in two comma-separated-value files, one for locking/unlocking events, another for recording the beginning and end of user sessions, as well as for application-related events.

To protect confidentiality of the user data, we used app-specific internal device storage in Android OS, which was inaccessible to any other application in the system. To support protection of the logged data during its transmission, our study app encrypted it with the corresponding public key pre-installed in the app. The study app uploaded the collected data to the back-end server on daily bases.

By using our data collection app, we collected timestamped events related to the device state changes due to the participant's actions, timeouts, and other events. All these events can be classified into (un)locking the device and interacting with the apps.

3.2.1. (Un)locking events

Events related to the device locking and unlocking can be represented in a state diagram, as shown in Fig. 1. Table 2 describes corresponding events. These are broadcast actions in Android terminology. We used ACTION_SCREEN_ON to detect when the device-state changed from non-interactive to interactive. Our app also read the *auto-lock* settings for each participating device, a parameter that defines how soon the device locks itself automatically once the user stops interacting with it. We made sure to record each failed unlocking attempt, in addition to all successful attempts. We also recorded events of the participants turning the screen off by pressing the power button (rather than letting the phone to time out and lock).

3.2.2. App and user session events

To record start of a user session, we recorded timestamp for ACTION_USER_PRESENT. Since Android has no explicit action for session-end events, our logging app, on ACTION_SCREEN_OFF event, detected the locking state of the device by checking the state of the device keyguard. If the device was locked, our app recorded a timestamp that we associated with the session-end event.

Similarly, Android does not generate any explicit events when an app is launched or closed or when it switches between background and foreground. To collect corresponding data about the life-cycle of our participants' apps, our app also included an Android "observer" process, which ran always in background and checked every 500 ms the list of all running apps to identify the foreground app. If either changed, the observer recorded the corresponding changes as events in the data logs collected on the participants' phones.

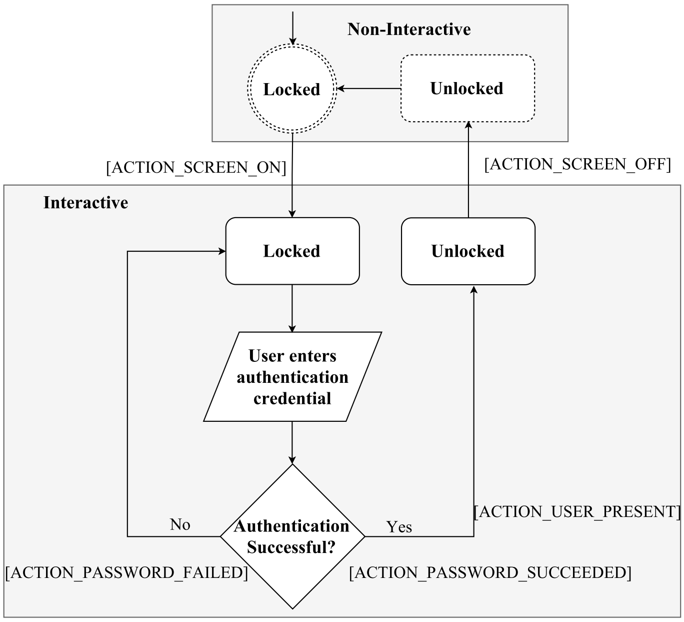


Fig. 1. States and Android OS broadcast actions related to device locking and unlocking that were logged during data collection.

For each participant, we recorded the details about applications being used within every session. In particular, we recorded timestamps of when each application was launched and closed. We identified each application by package name, e.g., *facebook.katana* for the Facebook application, which is a unique domain-like application identifier. Such data allowed us to (a) count the number of applications being used in each session, and (b) measure the frequency of application use as well as the time share of each application in overall amount of time of interaction with the given the smartphone.

3.3. Data analysis

We performed several measurements on the collected data: the number of unlocking attempts per day for each participant, the frequency and length of unlocking attempts and their outcomes, the number of applications being used within a single session, session length, etc.

For statistical difference test we used non-parametric Kruskal–Wallis as the data are not normally distributed and we used Tukey's HSD for post-hoc analysis. In addition, we used ANOVA test for normally distributed data. For counting data, we used Pearson's Chi-square test to measure association between independent variables. We analyzed data for participants who completed 20 day period and we excluded days that were recorded partially (e.g., installation and removal days were excluded). To remove outliers we used Hampel identifier [22].

4. Results

In this section, we present statistical results of our user study, based on the data from 41 participants. We split our participants into two distinct groups. **Locked** group included 22 participants that used some form of authentication method to unlock their devices. **Not-Locked** group included 19 participants that did not use any authentication methods to unlock their devices.[4] The Locked group included participants that used one of the three unlocking methods, namely (a) PIN, (b) Password, or (c) Pattern. To streamline the presentation of the results and conclusions, we sometimes refer to the participants from *Locked* group by the corresponding unlocking method, e.g., "Pattern participants". The distribution of the unlocking methods among the participants is presented in Table 3.

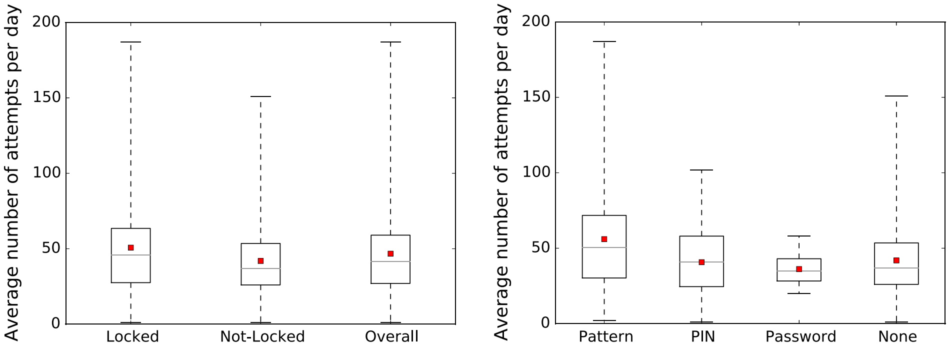
4.1. Performance of unlocking methods

For each participant, we measured several parameters related to device unlocking. First, we measured the number of unlocking attempts per day. Second, we measured the frequency of successful and unsuccessful unlocking attempts. Finally, for each unlocking attempt in *Locked* group, we measured the *entry time*, that is, the time it took a participant to enter

[4] To unlock their devices, they just swiped across the screen. We refer to this unlocking method as "None".

Table 3
Participants distributions according to screen unlock methods, $N = 41$.

Unlock type	# of users	Percentage
Pattern	15	37%
PIN	5	12%
Password	2	5%
None	19	46%



(a) Number of unlocking attempts for each group.

(b) Number of unlocking attempts for each unlocking method.

Fig. 2. Average number of unlocking attempts per day: (a) for Locked and Not-Locked groups, where the "overall" shows the results for all 41 participants; (b) for participants grouped by the used unlocking method. In both figures, the red squares and the horizontal lines in the boxes represent the mean and the median values, respectively. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

her authentication secret. The entry time parameter accounts time for a single unlocking attempt only, i.e., it does not accumulate the total time spent to unlock the device, which might include failed unlocking attempts. In what follows we discuss all these measurements in more detail.

4.1.1. Unlocking frequency

Our participants unlocked their devices 46 times a day (SD = 26), on average. Throughout the rest of the paper we refer to unlocking device's screen as to "unlock" event for all subjects, even for subjects in the Not-Locked group. Statistical analysis revealed that participants in *Locked* group unlocked their devices 22% more often than the participants in *Not-Locked* group, i.e., 51 times a day (SD = 35) versus 41 times a day, (SD = 25)respectively (Bonferroni corrected t-test, $t = 4.46, p < 0.05$). Fig. 2(a) shows the spread of daily unlocking attempts for Locked and Not-Locked groups and for all participants combined.

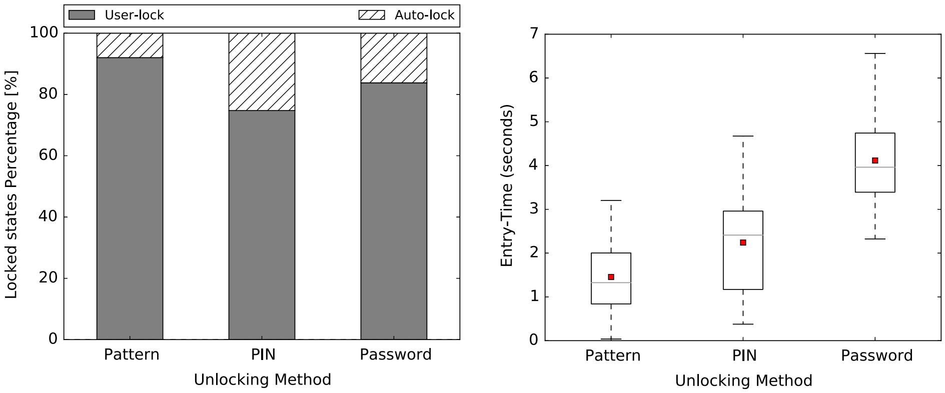
Further analysis of data showed that there was a statistically significant difference (Bonferroni-corrected Anova test, $F = 9.8, p < 0.05$) in the average number of unlocks per day between the participants grouped by the unlocking method (i.e., Pattern, PIN, Password, and None). Post-hoc pair-wise comparison revealed that Pattern participants were unlocking their devices more frequently than all other participants (Tukey HSD $p < 0.05$). In particular, every day on average, Pattern using subjects unlocked their devices 56 times (SD = 39), which was higher than by 25% and 36% in comparison with the subjects that used PIN and Passwords respectively, i.e., the subjects that used PINs unlocked their devices 42 times a day (SD = 25) and Password using subjects 36 times a day (SD = 13).

In addition, Pattern participants were unlocking their devices 27% more often than the participants from *Not-Locked* group. We did not find statistically significant difference in the remaining pair-wise comparisons. The spread of the average number of unlocks per day is shown at Fig. 2(b).

4.1.2. Auto/user locking

The value of auto-lock timeout in Android OS defines how soon a smartphone will lock itself after the device enters the sleep mode, i.e., turns off the screen as a result of a user not being active. This timeout can be chosen by the user in discrete values. The default is 5 s. Note, that if a user explicitly presses the power button, then the device locks immediately. For each participant, our app read the auto-lock timeout value from Android system's settings. This value only has a meaning for the participants from *Locked* group, because it only applies to the devices that has authentication-based unlock setup, i.e., a user has set a PIN, a Password or a Pattern for device unlock.

Our analysis revealed that only 6 participants (out of 22 in *Locked* group) kept the default value of 5 s, while the others changed it. In particular, 9 participants (41%) reduced the timeout by setting it to *immediately*, which effectively locks the phone right after it enters the sleep mode. Interestingly, 7 of them used Patterns. Another 7 increased the timeout value up to 30 min.



(a) Distribution of locking types.

(b) Distribution of entry time.

Fig. 3. The distributions of (a) locking types (auto-lock or user-lock) and (b) entry time for different screen-lock methods over locked group ($N = 22$). The red squares and the horizontal lines in the boxes in (b) represent the mean and the median values, respectively. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

On the other hand, if a user presses the power button, a smartphone locks immediately. We refer to such cases as *user-lock*. In contrast to auto-lock, user-lock does not leave any opportunity for an attacker to gain unauthorized access (by accessing the phone before it auto-locks). In order to measure how often participants used user-lock we recorded all *power button pressed* events, i.e., ACTION_SCREEN_OFF events at Fig. 1 that were triggered by the user pressing power button. These records allowed us to classify all locked states into two groups: auto-locked and user-locked. The distribution of average daily unlocks and how they split into these two groups are shown at Fig. 3(a).

Statistical analysis revealed a statistically significant difference in the distribution of locked states originating from auto-lock and user-lock between subjects that used PINs, Passwords and Patterns (Bonferroni corrected, $\chi(2) = 2328$, $p < 0.05$). Furthermore, the results of pairwise comparison suggest that there is a statistically significant difference between each pair (Bonferroni corrected χ^2-test, $p < 0.05$, Pattern vs. PIN $\chi(1) = 2216$, Pattern vs. Password $\chi(1) = 514$, PIN vs. Password $\chi(1) = 2328$).

Overall, we found that Pattern participants were three times and two times less likely to use auto-lock feature than PIN and Password participants respectively. In particular, 8%, 16% and 25% of all device lock events were attributed to auto-lock for Pattern, Password and PIN subjects respectively, or 11% of all device lock events for subjects in the Locked group. The average length of the opportunity window, a time span during which an attacker can unlock device without authentication required, for the subjects in the Locked group was 65 s.

4.1.3. *Entry time*

For each unlocking attempt, we measured *entry time*—the time it takes a user to enter her unlocking secret. In this section we discuss entry times for successful unlocking attempts only. Fig. 3(b) shows the average entry times for each unlocking method. Statistical analysis revealed a significant difference between the participants that used different unlocking methods. (Kruskal–Wallis test, $H(2) = 8.71$, $p < 0.05$.)

The results of the post-hoc analysis showed that there was a statistically significant difference in entry time between Pattern and Password participants (Tukey's HSD, $p < 0.05$). In particular, the former spent 1.7 s (SD = 0.5 s) on average to draw their patterns, while Password and PIN participants spent 4.1 s (SD = 0.3 s) and 2.5 s (SD = 0.9 s) respectively.

4.1.4. *Unlocking error rates*

Users make mistakes during authentication, and smartphone unlocking process is not exception. To assess how often our participants made mistakes during unlocking, we recorded each failed unlocking attempt, in addition to the successful ones. The likelihood of an error during unlocking attempts is shown at Fig. 4. The results of data analysis revealed a statistically significant difference in frequency of unsuccessful attempts between the participants that used Pattern, PIN, and Password methods (Bonferroni corrected, $\chi(2) = 100.37$, $p < 0.05$). Post-hoc pair-wise comparison showed that Pattern and Password participants were equally likely to make mistakes during unlocking. (Bonferroni corrected, $\chi(1) = 1.67$, $p = 0.20$.)

At the same time, PIN participants were 5.5 and 6.3 times less likely to make mistakes, in comparison to Pattern and Password participants, respectively (Bonferroni corrected χ^2-test, $p < 0.05$, Pattern vs. PIN $\chi(1) = 94.54$, PIN vs. Password $\chi(1) = 84.54$).

In addition to measuring the likelihood of an error during authentication process, we also counted how many failed authentication attempts the participants made in a row. The stacked bars in Fig. 4 show failed unlocking attempts due to single and several mistakes. Interestingly, all but one unlocking failures among PIN participants were cases with only one mistake. Whereas, Pattern and Password participants had several unlocking cases with two or more mistakes in a row.

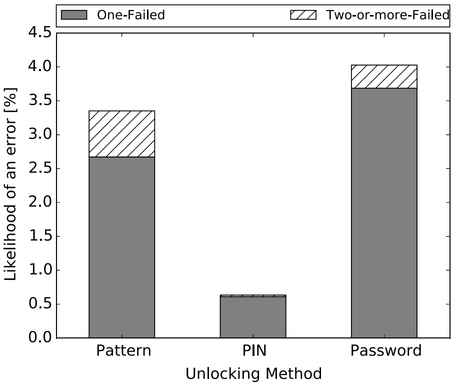


Fig. 4. Likelihood of an unlocking error. The graph shows separately the attempts with single and multiple failures.

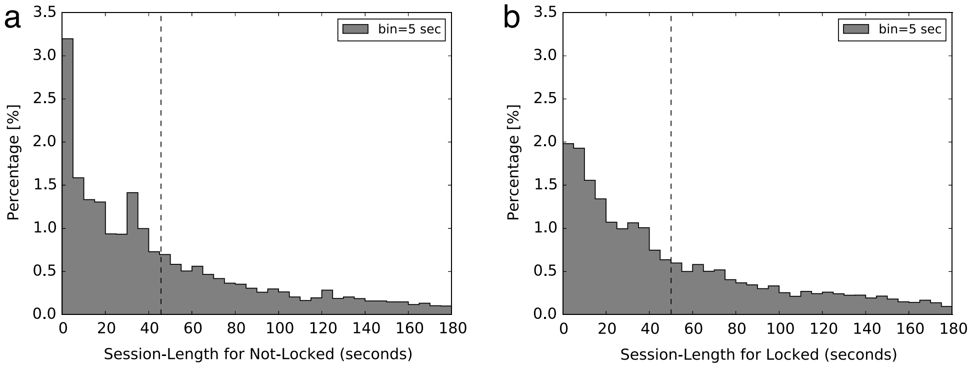


Fig. 5. Distribution of session lengths for the participants in (a) Not-Locked and (b) Locked groups. The dashed vertical lines show the average lengths.

4.2. Analysis of user sessions

The second part of our data analysis aimed at investigating the behaviour of our participants in regards to the applications they used once they unlocked their phones.

4.2.1. Session length

In total, our participants had 27,898 sessions with their phones. We used the difference between unlock and lock timestamps in order to measure the length of each session. Statistical comparison of session lengths among the participants in the Not-Locked and Locked groups revealed a significant difference (Bonferroni corrected Kolmogorov–Smirnov test, $D = 0.06, p < 0.05$). The average session of Not-Locked participants was 46 s (SD $=$ 44, median $=$ 45.5), shorter then the average session in Locked group, 50 s (SD $=$ 45, median $=$ 55.78), an 8% difference. The distributions of session lengths are presented in Fig. 5.

We also found statistically significant differences among PIN, Pattern, and Password participants (Bonferroni corrected Kolmogorov–Smirnov tests, Pattern vs. PIN $D = 0.19, p < 0.04$, Pattern vs. Password $D = 0.13, p < 0.05$, and PIN vs. Password $D = 0.06, p < 0.05$). We decided, however, not to split Locked group since the absolute differences between these groups were practically insignificant (less than one second for average session times).

4.2.2. Session characterization

Interestingly, every third session (35%) involved only a single app. Furthermore, most sessions (85%) involved at most three applications. In addition, length of the sessions where users opened two or fewer applications averaged at 25 s, while the sessions with 2 or 3 applications lasted for 100 s, on average. The distribution of the number of applications used across all sessions is shown in Fig. 6(a), while Fig. 6(b) shows average number of applications used, depending on the session length.

4.2.3. Used apps

Overall our participants used 564 unique applications. For this particular measurement, we had to exclude data of eight participants, because we were unable to obtain the name of the currently active application due to a restriction in Android 5.0 and higher, which made it impossible to obtain the name of the currently active application. On average, each participant

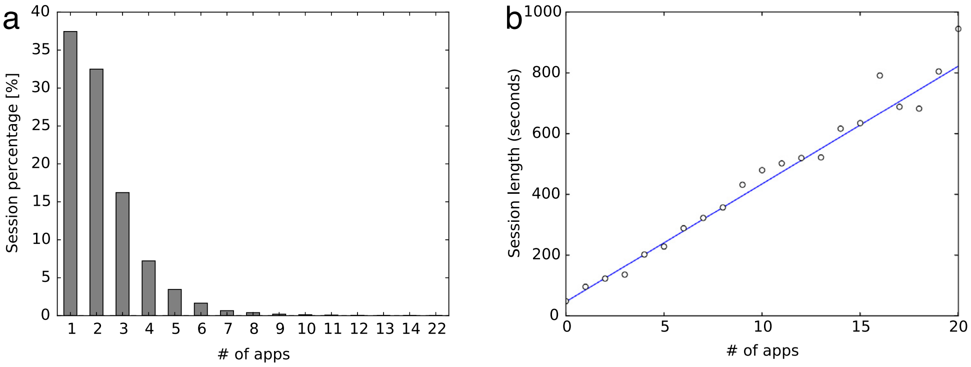


Fig. 6. Distribution of the number of applications used (a) across all sessions and (b) as a function of session length.

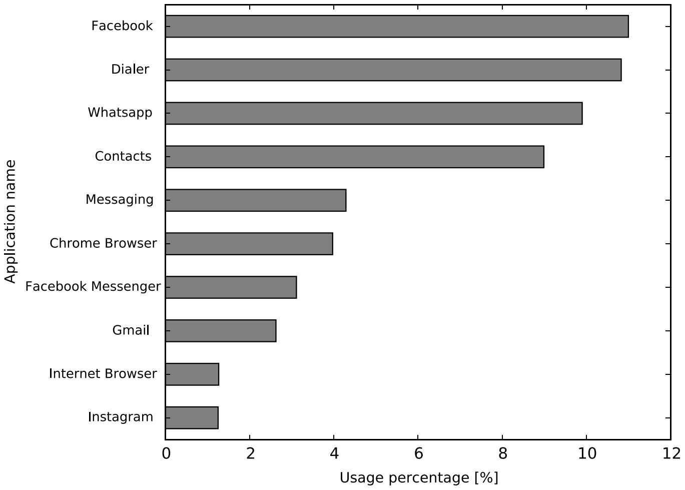


Fig. 7. Percentage of the top ten most used applications, according to the number of application sessions.

used 44 applications during our study, the actual value per participant varied from 20 to 69 ($sd = 13$, median $= 46$). Comparison of types of applications used and the average numbers of application per participant between Locked and Not-Locked groups did not reveal any statistically significant difference.

We excluded special system apps from the analysis, such as *launcher* and *systemui*, because these applications are part of Android OS, which user does not open explicitly. As shown in Fig. 7, the top ten applications comprise approximately 57% of all observed sessions. Interestingly, the majority of the most frequently used applications support short tasks, i.e., a simple task where a user unlocks the phone to open one or two applications and then locks the device. For example, a user might unlock his smartphone to just read a received message. These results are in line with a similar observation by Banovic et al. [23].

4.2.4. *Cost of unlocking*

We define the relative cost of unlocking (CU) as follows:

$$CU = \frac{UT}{ST + UT} \tag{1}$$

where UT is the time it takes to unlock the phone, and ST is the length of the session that follows the unlock. For each recorded session we calculated the corresponding cost of unlocking and then averaged these costs by grouping sessions in one-second bins, which allowed us to obtain an average cost of unlocking for sessions with increment in one second.

We found that 50% of sessions have relative cost less than 4%, as represented by the dashed line in Fig. 8. Moreover, the results show that the shorter sessions have higher cost of unlocking, up to 30%–80%, depending on the used unlocking method. For longer sessions, where the participants typically launched two applications (i.e., 25 s on average, see Section 4.2.2 and Fig. 6(b)) the cost decreased down to 5%–15%. If the session length increases even further, however, the overall cost of unlocking asymptotically decreases to a few percent. For example, for 100-s or longer sessions, in which usually three or more applications were launched, the cost of unlocking was at most 2%–3%.

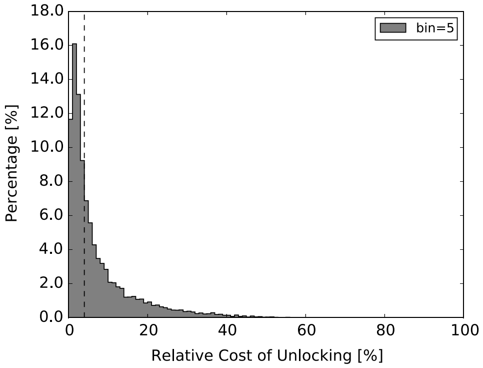


Fig. 8. The distributions of sessions according to the relative cost of unlocking. The dashed vertical line represents 50% of all sessions.

5. Discussion

First of all, our results corroborate previous reports on the proportions of smartphone users who prefer just to "swipe to unlock" rather than use any stronger protection against the threat of unauthorized physical access to their devices. Almost half of our participants (46%) did not use screen-lock method, in line with other recent findings that 52% (out of 1500) [5] and 34% (out of 500) [4] do not lock their smartphones. There are could be various explanations for the users' reluctance to keep their smartphones unprotected, which might include usability issues with current authentication methods used for locking or simple lack (or, at least, perception of it) of sensitive data on their devices [3,8,4]. While one might hypothesize that Not-Locked participants might have been using their phones more often and therefore did not want to bare the overhead of unlocking devices each time, our findings would not support such an explanation.

Instead, we discovered that those who lock their devices not only use them more frequently but also for longer sessions. In particular, Locked participants were unlocking their phones 22% more often (Section 4.1.1), and, on average, their sessions were 8% longer than among Not-Locked participants (Section 4.2.1). One possible explanation to that, *Locked* participants saw more value in the data and services provided in the smartphones.

In addition, Pattern participants were the fastest in unlocking their phones and used their devices more frequent than others in *Locked* group. This result contrasts with observation by von Zezschwitz et al. [19], where they measured the time by using a developed app rather than measuring real-world authentication time as we did. Moreover, we also found *Pattern* users often preferred to lock their phones explicitly, by pressing the power button, than other users. This might suggest that users factor in the low time (and/or cognitive) cost of unlocking with Pattern and can afford higher security, by locking the device explicitly or using shorter auto-lock timeout.

The auto-lock feature is a tradeoff between security and usability. At one extreme, when the auto-lock is set to kick in *immediately*, it provides better physical security, while sacrifices usability, by requiring users to authenticate on each device unlock. At the other extreme, setting the timeout to some extensive value, e.g., 30 min, might greatly reduce the frequency, and, as a result, the burden, of unlocking. The results of our study suggest that while almost half of the subjects set auto-lock timeout to *immediately*, most of whom used Pattern, others set it to some extensive values, thus, increasing the chances for an attacker. In particular, we found that on average 11% of all device locks are due to auto-lock, and on average the device is not locked for 65 s after the screen is turned off. This provides an opportunity window for so called *lunch-time* attacks, when someone sneaks into an unattended smartphone. We suggest that the investigation of implicit authentication is one possible option to tackle that tradeoff [24,25,12].

Another surprising finding was the low cost of unlocking, relatively to the overall smartphone usage. In particular, while each participant in Locked group used their device for 43 min a day on average, only 100 s a day in total were spent by each Pattern or PIN participant (and 200 s by each Password participant) on unlocking their phone. This corresponds to about 4% (and 8%) of participants' time spent on interacting with their smartphones. Yet, such a low overhead appears to outweigh the benefit of protection for the other 46% of the participants, who preferred not to lock their devices.

On the other hand, Password method, which increased unlocking entry time to 4.1 s, was 9 times less likely to get adopted by the users in the Locked group. These results seem to suggest that entry-time might be a significant factor for adoption by users, and proposals for novel device unlocking methods should be carefully evaluated in that respect. Even more, an addition of promising biometric sensors, such as Touch ID finger print scanner in iPhones [26], does not improve adoption of passwords by users. In particular, as we showed, increasing the time to authenticate by just a few seconds (the difference between Pattern and Password was 2.4 s) might render a method doomed.

It appears from the results that the error rate during unlocking – the probability of an error while entering unlocking secret – was not an impeding factor for adoption. In particular, we discovered that while Password and Pattern suffered from comparable error rates (4% and 3.4%), Pattern was 7 times more likely to be used than Password, as an unlocking method. Even more, PIN, which showed the lowest error rate of about 0.6%, was adopted three times less frequently than more error-prone Pattern method. These results seem to indicate that users are willing to tolerate errors (at least of this range) in unlocking their devices, provided other benefits of the unlocking method, such as speed, convenience [8,4], social acceptance [27], or cognitive cost. In other words, a novel authentication method should not be dismissed only due to the fact that it suffers from failed attempts slightly more than others.

Since the rate of repeating errors during unlocking was very low across all three unlocking methods (Section 4.1.4), few (even 3) consecutive errors could be used as an indication of a guessing attack [15].

Overall, our results suggest many users are picky when it comes to adopting methods for unlocking their smartphones. On one hand, they are willing to spend half an hour a day on social networking, web-browsing and games. On the other hand, they are unwilling to sacrifice 100 s a day on unlocking their devices. Most (about 90%) of those who locked their device, used weak authentication methods (PIN and Pattern), and faced similar dilemma, i.e., unwillingness to spend additional 100 s a day in order to use (presumably) stronger Password method. Based on these results, we recommend that all novel methods for unlocking smartphones should be compared with the most adopted methods, such as PINs and Pattern, in usability.

Given that one third of all sessions involved only one app and almost two thirds involved at most 3 apps and the unlocking cost for short sessions could be as high as 80% of the overall interaction time, there seem to be an avenue for new research towards reducing (or maybe even eliminating) the unlocking cost of one-app sessions (particularly with apps of low sensitivity). Our finding that the 10 most frequently used apps (out of 564) were responsible for about half of the sessions could be of help, as well.

6. Limitations

As with any (empirical) research, our field study had some limitations. We could only collect some certain events. We could not get details of used credentials to calculate strength of each method.

The time lapsed between ACTION_SCREEN_ON and ACTION_PASSWORD_SUCCEEDED might have included a delay due to the participant first reading the notifications on the locked screen, before starting to unlock the device. Due to the limitations of the event granularity in Android OS, we could not detect if that were the case and/or measure time the participants took to read notifications on the locked screen, before unlocking the device.

While we measured error rate and time to completion for three main unlocking methods on Android smartphones, we did not measure other important but less observable factors that might play a role in swaying users towards/away one or the other unlocking method. Some obvious factors we did not measure are convenience and cognitive overhead. For example, PIN and Pattern methods can be employed using just the thumb on the same hand that holds the phone, while Password might not, if the input has special characters, digits, or capital case. So, those participants that often run into situations that call for unlocking their phones with the holding hand, might shy away from Password method for just that reason. Compared to PIN and Password, Pattern might have lower cognitive overhead by employing visual memory for storing and recalling the corresponding secrete. All these factors might or might not have been present among our participants. Even if they were present, we do not know if they impacted our measurements or influenced participants' choices of the unlocking methods.

7. Conclusion

We performed a longitudinal field study with 41 participants, who installed our monitoring framework on their Android smartphones and ran it for at least 20 day period. With the collected data, we were able to investigate users' (un)locking behaviour and their usage of applications in the wild. The results shed the light on how in reality users use smartphones in regards authentication and usage behaviour. We showed how currently deployed authentication methods, i.e., PIN, Password and Pattern, perform in real-life settings, and highlight the importance of authentication speed on adoption by users. In addition, we show that users do not mind adopting methods with higher error rate (e.g., Pattern-based authentication method), if they are faster to type.

Acknowledgements

We would like to thank our colleagues at LERSSE lab for their feedback on the earlier version of this article. The first author would like to thank Egyptian Mission sector for the doctoral scholarship.

References

[1] E. U. A. for Network, I. Security, Top ten smartphone risks, April 2015.

[2] M.D. Giles Hogben, Smartphones: Information security risks, opportunities and recommendations for users, Tech. rep., ENISA, 2010.

[3] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, K. Beznosov, Know your enemy: the risk of unauthorized access in smartphones by insiders, in: Proceedings of the 15th International Conference on Human–computer Interaction with Mobile Devices and Services, MobileHCI'13, ACM, New York, NY, USA, 2013, pp. 271–280. http://dx.doi.org/10.1145/2493190.2493223.

[4] S. Egelman, S. Jain, R.S. Portnoff, K. Liao, S. Consolvo, D. Wagner, Are you ready to lock? in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS'14, ACM, New York, NY, USA, 2014, pp. 750–761. http://dx.doi.org/10.1145/2660267.2660273.

[5] E. Bursztein, Survey: Most people don't lock their android phones - but should, April 2015. https://www.elie.net/blog/survey-most-people-dont-lock-their-android-phones-but-should.

[6] C.R. Donna Tapellini, Smart phone thefts rose to 3.1 million last year, consumer reports finds, April 2015. http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

[7] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C.R. Crowell, J. D'Arcy, Modifying smartphone user locking behavior, in: Proceedings of the Ninth Symposium on Usable Privacy and Security, SOUPS'13, ACM, New York, NY, USA, 2013, pp. 10:1–10:14. http://dx.doi.org/10.1145/2501604.2501614.

[8] M. Harbach, E. von Zezschwitz, A. Fichtner, A.D. Luca, M. Smith, 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, 2014, pp. 213–230.

[9] S. Uellenbeck, M. Dürmuth, C. Wolf, T. Holz, Quantifying the security of graphical passwords: The case of android unlock patterns, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer &#38; Communications Security, CCS'13, ACM, New York, NY, USA, 2013, pp. 161–172. http://dx.doi.org/10.1145/2508859.2516700.

[10] A. De Luca, A. Hang, F. Brudy, C. Lindner, H. Hussmann, Touch me once and i know it's you!: implicit authentication based on touch screen patterns, in: Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems, CHI'12, ACM, New York, NY, USA, 2012, pp. 987–996. http://dx.doi.org/10.1145/2208516.2208544.

[11] A. De Luca, E. von Zezschwitz, N.D.H. Nguyen, M.-E. Maurer, E. Rubegni, M.P. Scipioni, M. Langheinrich, 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, pp. 2389–2398. http://dx.doi.org/10.1145/2470654.2481330.

[12] T. Feng, J. Yang, Z. Yan, E. Tapia, W. Shi, Tips: Context-aware implicit user identification using touch screen in uncontrolled environments, in: Proceedings of the 15th Workshop on Mobile Computing Systems and Applications, HotMobile'14, ACM, Santa Barbara, CA, USA, 2014, p. 6.

[13] G. Inc., Android, the world's most popular mobile platform, April 2014.

[14] G. Inc., Set screen lock, android users guid, February 2015.

[15] J. Bonneau, The science of guessing: Analyzing an anonymized corpus of 70 million passwords, in: Security and Privacy (SP), 2012 IEEE Symposium on, 2012, pp. 538–552. http://dx.doi.org/10.1109/SP.2012.49.

[16] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, A.D. Rubin, The design and analysis of graphical passwords, in: Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8, SSYM'99, USENIX Association, Berkeley, CA, USA, 1999, pp. 1–14.

[17] R. Biddle, S. Chiasson, P. Van Oorschot, Graphical passwords: Learning from the first twelve years, ACM Comput. Surv. 44 (4) (2012) 19:1–19:41. http://dx.doi.org/10.1145/2333112.2333114.

[18] K.N. Truong, T. Shihipar, D.J. Wigdor, Slide to x: Unlocking the potential of smartphone unlocking, in: Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, CHI'14, ACM, New York, NY, USA, 2014, pp. 3635–3644. http://dx.doi.org/10.1145/2556288.2557044.

[19] E. von Zezschwitz, P. Dunphy, A. De Luca, 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, MobileHCI'13, ACM, New York, NY, USA, 2013, pp. 261–270. http://dx.doi.org/10.1145/2493190.2493231.

[20] F. Schaub, M. Walch, B. Könings, M. Weber, 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, pp. 11:1–11:14. http://dx.doi.org/10.1145/2501604.2501615.

[21] G. Inc., Google play install stats, February 2015.

[22] F.R. Hampel, The influence curve and its role in robust estimation, J. Amer. Statist. Assoc. 69 (346) (1974) 383–393.

[23] N. Banovic, C. Brant, J. Mankoff, A. Dey, Proactivetasks: The short of mobile device use sessions, in: Proceedings of the 16th International Conference on Human–computer Interaction with Mobile Devices &#38; Services, MobileHCI'14, ACM, New York, NY, USA, 2014, pp. 243–252. http://dx.doi.org/10.1145/2628363.2628380.

[24] M. Jakobsson, E. Shi, P. Golle, R. Chow, Implicit authentication for mobile devices, in: Proceedings of the 4th USENIX Conference on Hot Topics in Security, HotSec'09, USENIX Association, Berkeley, CA, USA, 2009, p. 9.

[25] M. Frank, R. Biedert, E. Ma, I. Martinovic, D. Song, Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication, IEEE Trans. Inf. Forensics Secur. 8 (1) (2013) 136–148. http://dx.doi.org/10.1109/TIFS.2012.2225048.

[26] I. Cherapau, I. Muslukhov, N. Asanka, K. Beznosov, On the impact of touch id on iphone passcodes, in: Proceedings of the Symposium on Usable Privacy and Security, SOUPS'15, 2015, p. 20.

[27] A. De Luca, A. Hang, E. von Zezschwitz, 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, ACM, New York, NY, USA, 2015, pp. 1411–1414. http://dx.doi.org/10.1145/2702123.2702141.