Ask Me Again But Don't Annoy Me: Evaluating Re-authentication Strategies for Smartphones

Lalit Agarwal, Hassan Khan, and Urs Hengartner, ***University of Waterloo***

https://www.usenix.org/conference/soups2016/technical-sessions/presentation/agarwal

This paper is included in the Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).

June 22–24, 2016 • Denver, CO, USA

ISBN 978-1-931971-31-7

Open access to the Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) is sponsored by USENIX.

Ask me again but don't annoy me: Evaluating re-authentication strategies for smartphones

Lalit Agarwal, Hassan Khan and Urs Hengartner
Cheriton School of Computer Science
University of Waterloo
Waterloo, ON Canada
{lagarwal, h37khan, urs.hengartner}@uwaterloo.ca

ABSTRACT

Re-authenticating users may be necessary for smartphone authentication schemes that leverage user behaviour, device context, or task sensitivity. However, due to the unpredictable nature of re-authentication, users may get annoyed when they have to use the default, non-transparent authentication prompt for re-authentication. We address this concern by proposing several re-authentication configurations with varying levels of screen transparency and an optional time delay before displaying the authentication prompt. We conduct user studies with 30 participants to evaluate the usability and security perceptions of these configurations. We find that participants respond positively to our proposed changes and utilize the time delay while they are anticipating to get an authentication prompt to complete their current task. Though our findings indicate no differences in terms of task performance against these configurations, we find that the participants' preferences for the configurations are context-based. They generally prefer the re-authentication configuration with a non-transparent background for sensitive applications, such as banking and photo apps, while their preferences are inclined towards convenient, usable configurations for medium and low sensitive apps or while they are using their devices at home. We conclude with suggestions to improve the design of our proposed configurations as well as a discussion of guidelines for future implementations of re-authentication schemes.

1. INTRODUCTION

The increased usage of smartphones to access personal and corporate data requires authentication at multiple levels. A device-level authentication scheme, such as a PIN or fingerprint recognition, is required to protect access to the device while text-based passwords may be required to further establish identity for social networking, banking or enterprise apps. Existing studies have shown that the short and frequent nature of smartphone sessions creates usability issues for device-level authentication schemes [17] whereas constrained keyboards on smartphones are a bottleneck when users are authenticating using text-based passwords [29]. To mitigate these usability issues, researchers have proposed several techniques that reduce the authentication burden by leveraging user behaviour [21, 32, 37], device context [16, 24, 25] or the sensitivity of launched apps [17].

While these schemes reduce the authentication burden on the user, they may require mid-task re-authentication. Schemes that leverage user behaviour need re-authentication in case of a behaviour mismatch against the current phone user. Similarly, device context-based schemes may need to establish a user's identity in case a contextual source (e.g., ambient noise) changes. Taking the sensitivity of launched apps into account for authentication may also require mid-task re-authentication. For instance, some users have indicated that for a messenger app only opening old messages should trigger re-authentication [17].

Preliminary evaluations show that users like the convenience offered by these schemes [4, 16, 17, 19, 24]; however, a field study of behaviour-based authentication shows that re-authentications are a potential issue [19]. More specifically, the evaluated scheme used a (simulated) behaviour-based authentication scheme that focused on the user's touch input behaviour. Whenever re-authentication was required, the user's current task was interrupted and a re-authentication prompt with dark background, similar to the standard Android authentication prompt, appeared immediately. Non-surprisingly the unpredictability of a re-authentication and the context switch due to the task interruption were annoying to some users.

While re-authentication is unavoidable to preclude misuse of a device or an app, the unpredictability of re-authentication can be reduced by delaying the transition between the current task and the re-authentication prompt through a fade-in effect. During the fade-in, the user is allowed to continue interacting with their current task on the device. In addition to the fade-in effect, the re-authentication prompt can be configured to have varying levels of transparency to provide a visual of the user's current task in the background. The fade-in effect should reduce the unpredictability of the re-authentication and a visual of the current task of the user should reduce the context switch overhead due to re-authentications. Together these controls have the potential to provide increased usability at the cost of reduced security.

In this paper, we evaluate different configurations of explicit authentication schemes (such as PINs or pattern-locks) when used for re-authentication. Our focus is on the fade-in

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.

effect and the transparency of the re-authentication prompt. We choose behaviour-based authentication as a target use case to evaluate the different configurations; however, our findings can be generalized to other authentication proposals that require re-authentications. In addition to the re-authentication configuration used in the previous work [19], we select three configurations of explicit authentication schemes for re-authentication: (i) The authentication prompt appears immediately (no fade-in) and the background of the authentication prompt is transparent to provide a visual of the user's current task in the background; (ii) the authentication prompt appears immediately and the background of the authentication prompt gradually transitions from transparent to opaque for improved security; and (iii) the authentication prompt appears after a four second fade-in delay and the background of the authentication prompt gradually transitions from transparent to opaque.

We perform lab experiments using synthetic tasks to evaluate the security perception, ease of use, obstructiveness and annoyance of PIN and pattern-lock-based re-authentication based on the default configuration from the earlier study [19] (as a baseline) and the modified configurations. In addition to these qualitative usability metrics, we collect quantitative data on the task efficiency and the task error rate for a multifaceted evaluation of these configurations. Finally, we conduct interviews to gather participants' perceptions on the sensitivity of different kinds of apps and of participants' preferred configuration of the re-authentication prompt for different apps and different environments.

Our study was completed by 30 participants. Though our findings indicate no differences for the user performance (in terms of task efficiency, task error rate, and context switch overhead) against these configurations, participants found all three modified configurations to be less annoying and less obstructive as compared to the default configuration. The modified configurations were also at least as easy to use as the default configuration. As expected, the perceived security level of the modified configurations was quite low when compared to the default configuration. While the low perceived level of protection was a bottleneck in the adoption of the modified configurations in high-risk environments and for sensitive content, a significant number of participants preferred the proposed configurations over the default configuration for less sensitive content and for low-risk environments. We also communicate suggestions by the participants on how to improve the design of our proposed configurations and we discuss guidelines for future implementations of re-authentication schemes.

2. MOTIVATION

Implicit factors have been proposed to reduce authentication overhead on the web [2], personal computers [22] and smartphones [17, 25, 32]. Our focus is on smartphones. The implicit factors for authentication on smartphones leverage behavioural biometrics [32], device context [16, 24, 25] or the sensitivity of launched apps [17]. We next describe each of these three implicit factors and their potential need to re-authenticate a smartphone user.

2.1 Re-authentication Scenarios

Implicit authentication (IA): IA uses behavioural biometrics to conveniently authenticate users without requiring their explicit input. Various IA schemes have been proposed that authenticate users through their touch input behaviour [13, 21, 37], keystroke behaviour [8, 10, 14], gait behaviour [12, 27] or device usage behaviour [32, 33]. Several IA proposals have been shown to provide over 95% accuracy [13, 21, 37] and researchers have proposed to use them as a primary authentication mechanism for users who do not lock their device or as a secondary authentication mechanism to compliment the existing primary authentication schemes.

There are scenarios when an IA scheme is unsure about the identity of the user. This uncertainty may be caused by an adversary using the device or it could be the result of a false reject. False rejects occur when legitimate users are misclassified as adversaries. When an IA scheme is unsure about the identity of the user, it uses an explicit authentication mechanism to re-authenticate the user. Furthermore, if an IA scheme relies on the input behaviour of the user, the false rejects can occur mid-task and re-authentication requires interrupting the current task of the user [19].

Context-aware authentication: Several schemes have been proposed that leverage device context to reduce authentication overhead [16, 24, 25, 28]. These schemes rely on a variety of contextual sources, including location, proximity to WiFi and Bluetooth devices, and ambient light and noise. An evaluation of CASA [16] shows that it can reduce explicit authentications by 68% and a lab study of the scheme proposed by Riva et al. [28] indicates that it can reduce the number of explicit authentications by 42%.

Context-aware schemes can be deployed to sense and assist in authentication only when users begin their interaction with the device. However, to preclude attacks from informed attackers (such as friends and coworkers), a continuous authentication scenario is more suitable. For instance, a continuous proximity sensing scheme will not allow an informed malicious coworker to unlock the device at the workplace and then move to a secluded place to access personal data on the device. Since such scenarios may arise with the legitimate user of the device (e.g., the device owner moves out of the proximity range while using the device, or an ambient noise sensor may switch off), the device owner may be subjected to mid-task re-authentication.

App-specific authentication: Hayashi et al. [17] show that all-or-nothing access to smartphones does not align with user preferences. They find that while the majority of the users prefer to be authenticated for select apps only, for a subset of apps the users want some functionality to be available always and some functionality to be available after authentication. For instance, browsing existing entries (such as contacts) in an app should always be available while modifying or deleting entries should require authentication. Similarly, looking at recent messages should not require authentication while browsing old messages should require user authentication. These scenarios require mid-task re-authentication of the user.

2.2 Need for Better Re-authentication Schemes

User studies on IA show that users find IA to be more convenient and easier to use than traditional authentication schemes [4, 19]. Evaluations of the context-aware schemes show that the reduced authentication overhead is found to

be useful and the users indicated that they would use the evaluated scheme if it was available on their devices [16, 24]. A similar positive experience was reported for an app sensitivity based authentication scheme [17].

While users agree that these schemes are useful and are interested in adopting them, most of these evaluations have not investigated the effect of re-authentications with the exception of Khan et al. in their usability study of touch input-based IA [19]. Khan et al. find that for 35% of the participants, re-authentications due to false rejects were a source of annoyance. The participants found the re-authentications to be frustrating due to their unpredictable nature and the accompanying context-switch due to authentication interrupts. The context switch was also responsible for reducing the overall task completion time of the participants.

Since unavoidable re-authentications are a potential issue in the adoption of IA, we investigate whether the unpredictable nature and the context-switch due to authentication interrupts can be reduced by modifying how a user is re-authenticated. We assume that our concepts can mitigate these usability issues and thus reduce barriers to the adoption of novel authentication schemes that require re-authentication.

3. STUDY DESIGN & OBJECTIVES

In this section, we first outline different approaches that can be used for re-authentication. We then provide the rationale for our selection of a slightly modified version of the existing authentication prompts through two configuration parameters: *time delay* and *screen transparency*. Finally, we outline the security and usability trade-offs introduced by these parameters, our constructions of re-authentication prompts with different configurations of these parameters and the usability expectations from our constructions.

3.1 Re-authentication Approaches

Several re-authentication schemes are possible. During the design phase, we considered the following:

Split-screen configuration: In this configuration, the authentication prompt and the current user task equally share the screen space (screenshots are provided in Appendix B). This enables the user to authenticate within a timeout period with their task in sight. However, it is difficult to ensure that the authentication prompt is displayed at a location that the user is focusing on. In case the authentication prompt appears in the location where the user is focusing on, it results in the aforementioned usability issues. Nevertheless, this approach is worth exploring once gaze tracking solutions for smartphones have matured [23, 26].

Alternate authentication mechanisms: Alternate authentication mechanisms have been proposed to counter shoulder-surfing attacks, which reduce the size of the authentication prompt [20] or allow the user to enter the PIN using simple up and down gestures [35]. Similar to the split-screen configuration, a challenge for these approaches is the identification of the most suitable placement of the authentication prompt for re-authentication. Another option is to use mechanisms that provide security using obscurity. For instance, De Luca et al. [7] have proposed a mechanism that allows users to enter the secret discretely through the back of the device. In another proposal, the user is expected to enter an incorrect character to authenticate when the phone vibrates [6].

These approaches are promising; however, they may introduce confounding factors as they have not been adopted widely. The missing experience of the participants with these new configuration design may affect their usability perceptions. Since several usability issues can be traced to the unpredictability and context-switch effects of re-authentication [19], we perform experiments to investigate whether the unwanted effects stemming from unpredictability and context-switches can be minimized for widely deployed authentication mechanisms. Therefore, the main objective of this study is to investigate whether widely deployed authentication schemes can be modified to make them more usable for re-authentication scenarios without significantly compromising on security.

3.2 Configuration Parameters

We introduce two configuration parameters for existing authentication prompts: *time delay* and *screen transparency* and define the possible values for each of the parameter. The *time delay* represents the time it takes between the transition from the current task of the user to the appearance of the re-authentication prompt. This variable supports two possible values: immediate lock (Imm-Lock) and gradual lock (Grad-Lock). In the Imm-Lock case, the re-authentication prompt appears immediately (without any delay) whereas for the Grad-Lock case, the re-authentication prompt appears after a predefined interval with a fade-in effect. During this fade-in, the user can continue to interact with the current task. The two possible values provide different usability and security trade-offs: the secure Imm-Lock bars the user from interacting with the current task, while the less secure Grad-Lock is not abrupt and provides the user with an opportunity to interact with the current task during the fade-in effect thereby potentially allowing the user to reduce the effect of interruption. For example, the user can finish reading a sentence.

For our experiments, we chose a four second time delay. Our selection was based on the results from previous studies and our experiments with both shorter and longer delays. Ferreira et al.'s [11] study on understanding micro-usage patterns for various smartphone apps revealed that 40% of the application usage lasts less than 15 seconds and is sufficient for a user to read or reply to a message. In a study conducted by Yan et al. [38], they find that 50% of the smartphone interactions last fewer than 30 seconds. With such brief periods of interactions, it is therefore necessary to lock the device quickly to prevent any misuse. For the grace period, we considered and tested delays between two to seven seconds. During our empirical tests with four participants, we found that the four seconds delay period allowed the participants to prepare for re-authentication prompts. The shorter delay values did not provide the users with enough time to prepare for the re-authentication prompt, whereas the longer delay values made the users anxious in anticipation of the re-authentication prompt.

The *screen transparency* variable affects the visibility of the current task by configuring the background of the re-authentication prompt to be instantaneously dark (Imm-Dark, see Figure 1a), gradually fade from transparent to dark (Grad-

Dark, see Figure 1b) or remain transparent (Imm-Trans, see Figure 1c and 1d). Similar to the *time delay* variable, the three possible states of *screen transparency* provide varying degrees of security and usability. The Imm-Dark state is the most secure one because it hides sensitive data displayed in the current task; however, the context-switch overhead should be the most in this case since the user's task is not visible anymore. The Imm-Trans state covers the other extreme where sensitive data displayed in the current task remains visible behind the re-authentication prompt; however, the context-switch overhead should be the least since the user's task remains visible while the user is interacting with the re-authentication prompt. The Grad-Dark state provides a grace period during which the user can authenticate to resume the task at hand; however, if the user fails to do so in a configurable amount of time, the background of the re-authentication prompt becomes dark thereby hiding the user's current task.

3.3 Re-Authentication Prompt Configurations

The four configurations of re-authentication prompts that we construct using the different meaningful combinations of the two configuration parameters are as follows:

1. **Immediate Dark, Immediate Lock (Imm-Dark-Imm-Lock):** We evaluate the default lock scheme on most Android smartphones to establish a baseline for when it is used for re-authentication. In this configuration the re-authentication prompt appears immediately with a dark background, which completely hides the content of the current task, and the user can no longer interact with the current task. The re-authentication prompt asks the user to enter a PIN or pattern-lock and the user is able to access the current task again only after correctly answering the re-authentication prompt. This configuration was also used in the earlier work by Khan et al. [19], as discussed in § 2.2.
2. **Immediate Transparent, Immediate Lock (Imm-Trans-Imm-Lock):** The re-authentication prompt appears immediately in this configuration and the user can no longer interact with the current task. However, the background of the re-authentication prompt remains transparent, which allows users to observe the contents of their task.
3. **Gradual Dark, Immediate Lock (Grad-Dark-Imm-Lock):** In this configuration, the re-authentication prompt appears immediately and the user can no longer interact with the current task. Furthermore, the background of the re-authentication prompt is initially transparent and the contents of the current task are visible. Then, the background of the re-authentication prompt gradually fades into a dark screen and hides the contents of the current task from the user. If the user manages to authenticate before the screen has darkened completely, this configuration keeps the user's current task visible in the background.
4. **Gradual Dark, Gradual Lock (Grad-Dark-Grad-Lock):** In terms of task visibility, this configuration is similar to the Grad-Dark-Imm-Lock configuration described above. That is, the background of the re-authentication prompt is initially transparent and then turns into dark. However, this configuration also allows the user to continue interacting with the current task for a grace-period of four seconds before the re-authentication prompt appears. During the grace period, the brightness of the current task is reduced to indicate the forthcoming re-authentication prompt to the user. After the re-authentication prompt appears, the users can no longer interact with their task.

3.4 Study Aims

We expect the following properties from our re-authentication prompt configurations:

- Imm-Dark-Imm-Lock is the most obstructive therefore it should be the most annoying. Furthermore, since it provides no visual clues on the current task of the user, task efficiency should be reduced.
- Imm-Trans-Imm-Lock also immediately locks out the user but its presentation of the re-authentication prompt is less intrusive and it provides visual clues on the current task of the user. Therefore, it should be less annoying and more task efficient as compared to the Imm-Dark-Imm-Lock configuration.
- Grad-Dark-Imm-Lock has similar properties as Imm-Trans-Imm-Lock but it provides additional security by making the current task of the user invisible after a predefined time interval. Therefore, it should score similar to Imm-Trans-Imm-Lock in terms of usability with a relatively better security perception.
- Grad-Dark-Grad-Lock enables the user to interact with the current task for a grace period and this may increase the task efficiency of the users. However, the user may not take advantage of the grace period and instead wait for the re-authentication prompt to appear, which may increase the anxiety and annoyance of the user.

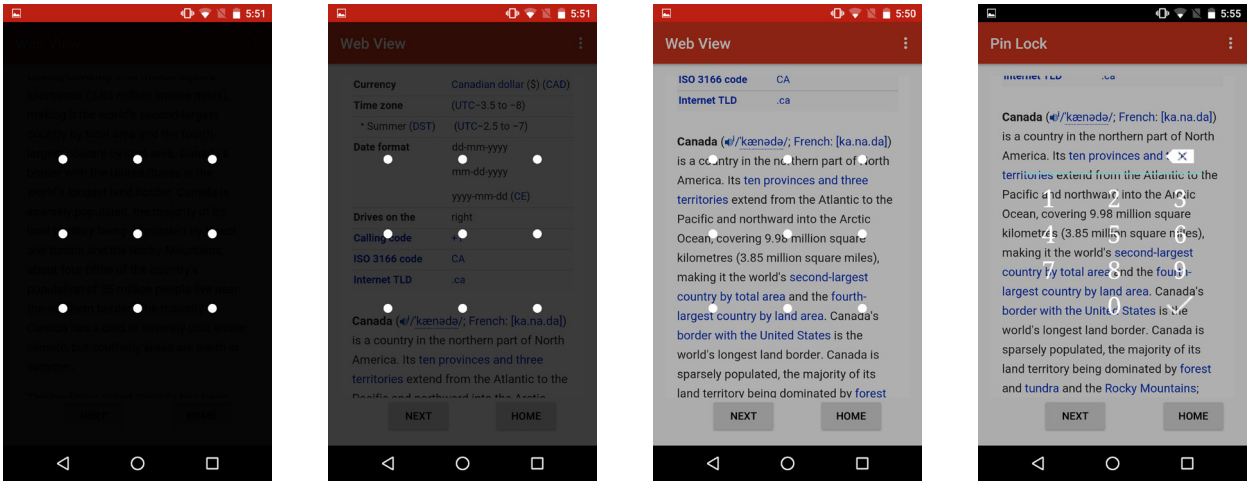
In the rest of this paper, we evaluate whether the four re-authentication prompt configurations provide the aforementioned usability properties.

4. STUDY DESIGN

In this section we outline our design of a user study to evaluate the four re-authentication prompt configurations. To measure the properties of each configuration, we perform a lab-based evaluation where participants are invited to experience each configuration by performing predefined synthetic tasks. After the users experience these configurations, they are asked to rate and provide qualitative feedback in terms of usability, security perception and their willingness to use these configurations. In addition to the user feedback, we measure the task efficiency, context switch overhead, and task error rate against each configuration. Our evaluation and feedback setup are designed to elicit the efficacy of these configurations for re-authentication in different scenarios. Our study was reviewed and received approval from the IRB of our university. We now provide details of our study design in terms of experimental setup and our methodology.

4.1 Apparatus

While several use cases exist for re-authentication (see § 2.1), we choose IA as the representative use case in this work because it was easier to explain and conduct than the other re-authentication cases outlined in the paper. Our choice of IA



(a) Imm-Dark (b) Grad-Dark (c) Imm-Trans (d) Imm-Trans

Figure 1: The proposed configurations with varying values for *screen transparency*. Figures (a), (b) and (c) show the three possible values when a pattern-lock based re-authentication prompt is used. Figure (d) shows a sample value for a PIN-based re-authentication prompt. For the Grad-Dark configuration, the background of the re-authentication prompt gradually turns from transparent into dark.

is also motivated by the prior work of Khan et al. [19] in the IA domain that highlights the issues with re-authentications in case of false rejects. To ensure that each participant experiences a certain number of false rejects, we use a simulated IA scheme, as was also done by Khan et al. In particular, our scheme simulates IA schemes based on a user's touch input or keystroke behaviour.

For our experiments, we select two widely used authentication mechanisms on Android: a 4-digit PIN and the Android pattern-lock (with the same constraints on possible patterns as in Android). The user interface of both schemes was similar to the Android lock screens (see Figure 1).

The four re-authentication prompt configurations introduced in § 3.3 are evaluated using two synthetic activities — a text entry activity and an email activity (screenshots are provided in Appendix A). We choose these activities since they represent common smartphone activities (i.e., reading and composing emails and text messages or interacting with social media apps).

- **Text entry activity:** This activity displays a 12-digit number to the participants. It also contains a text box and the users are asked to enter the displayed number in the text box using the numeric keyboard of the device.
- **Email activity:** In the email activity, users are asked to read an email in an email app. The user interface for the email app developed for this activity looks similar to the Android Gmail app. Once a participant has read the email, they are asked to answer a multiple choice question related to the email on a laptop. The emails composed for this activity contained sensitive data, which emphasized the need to protect the emails from adversaries (see Figure 10b for an example).

The design of the text entry activity ensures that the interaction of the users with the app can be measured, which enables us to compute several metrics in terms of context-switch overhead and errors made by the users. For the email activity, since the emails contain sensitive material, the users performing the email activity should consider the security implications of a re-authentication prompt configuration in addition to its usability aspects.

These activities were bundled in two separate Android apps, which allowed users to perform tasks. We define a task as completing the text entry or the email activity along with a mid-task re-authentication of the user using either the PIN or the pattern-lock in one of the four configurations. For the text entry task, the users were interrupted at predefined intervals, which were triggered based on the key presses by the users. The number of key presses required to trigger re-authentication changed across different text entry activities for each user but it stayed constant across users for those tasks for results to be comparable. Similar to the text entry task, the users were interrupted with a re-authentication prompt after a predefined number of swipes for the email task. The apps were instrumented to gather the timestamps of events, including input events by the user and the display and dismissal events of the re-authentication prompts. The apps also collected the errors made by the users for the text entry activity and during the re-authentication. We also logged the user interactions, including the keystrokes and screen touch events, during the grace period for the Grad-Dark-Grad-Lock configuration. The data collected by the apps was instrumental in computing the task completion rate, context switch overhead and the error rate against each re-authentication prompt configuration.

4.2 Evaluation Methodology

We evaluate the four re-authentication prompt configurations using the text entry and email tasks. Each scheme was evaluated in a round that consisted of four text entry tasks and two email tasks. Each user was subjected to

five rounds and in each round a different re-authentication prompt configuration was evaluated. For the first round, the participants performed the tasks without any authentication, which allowed us to establish a baseline. The participants were allowed to take a break between each task and each round. The order of the four re-authentication prompt configurations was randomly chosen for the participants.

The participants shortlisted for this study were invited for an hour long lab-based study. The participants were first asked to fill a demographic survey, which asked about their age, gender, and current occupation. They were then asked to fill a security preferences survey. In terms of security preferences, we asked the participants about their device locking habits, their preferred authentication scheme, and the adversaries that they wanted protection against. These pre-study surveys are provided in Appendix D. After the pre-study surveys, the participants were introduced to IA, the possibility of false rejects in IA, the tasks and apps used during the study, and the different re-authentication prompt configurations. The participants were also told that false rejects were simulated for the purpose of this study. We gave participants the option to select their preferred lock scheme (PIN or pattern-lock) and a corresponding secret for the study. We did not assign participants a specific scheme to avoid any bias due to their inexperience with it. This design decision prohibited us to counterbalance the authentication methods. The authentication times varied across participants. To cater for this, we report within-subject relative differences instead of absolute values. The participants experienced the different configurations in multiple rounds. After the completion of each round, they were asked to rate the usability and perceived security of the configuration that they experienced and to give an overall ranking in terms of their preferences by taking both the usability and the security of the evaluated configuration in account. Participants were also asked to indicate their preferences for the evaluated configurations under different device usage scenarios and were subjected to a semi-structured interview to gain further insight into their feedback. A researcher was present to respond to any questions the participants had.

4.3 User Feedback

The evaluated schemes trade off security for usability and since different users have different security preferences for different apps and different scenarios, we seek feedback from the users against four apps for three different scenarios. Previous studies have shown that users prefer a strict security setting for financial and email apps, which contain highly sensitive data, whereas they prefer a relatively relaxed security setting for contacts and other utility apps [17]. We sought feedback from the users for four apps: a banking app, an email app, a photos app, and a contacts app. These apps are commonly used and contain varying levels of sensitive data of the smartphone user. The participants were asked to consider the following device usage scenarios with the aforementioned apps available on the device.

- **Bus Scenario:** The participants had to consider a situation where they are traveling on a bus and they accidentally leave their smartphone behind. A stranger picks up their device and starts using it.
- **Office Scenario:** This scenario asks the participants to consider a work environment where one of their colleagues starts using their device when it is left unattended. For this scenario, the apps on the device may be used for a limited time by someone known by the smartphone owner.
- **Home Scenario:** In this scenario, we asked the participants to consider that their spouse accesses their device while it is left unattended or when they are asleep. The number of adversaries is limited in this scenario as compared to the others and the users may or may not want to protect their data from their spouse.

A researcher presented the scenarios to the participants and was available during the interview to answer any questions participants may have. Participants were given sufficient time to consider the presented scenarios. For each scenario, the participants were told that the re-authentication prompt would get activated in case the system notices any suspicious activity. We also reminded them of false rejects and the fact that they may be subjected to re-authentication while they are using the device. In order to inquire about the security perception of an evaluated re-authentication prompt configuration, the participants were told that for the purpose of these scenarios, they should consider that only IA is protecting their device. Since different users may have different security preferences for each configuration and each usage scenario, we initially asked the users to establish the sensitive nature of the apps and usage scenarios. Then the participants were asked to provide feedback in terms of security perception, usability and preferred re-authentication prompt configuration for each of the four apps under each of the three device usage scenarios. The feedback questionnaire is provided in Appendix E.

Finally, at the end of the study, we conducted a short semi-structured interview (provided in Appendix F) to gain insight into participants' overall impression of the configurations that they evaluated.

5. RESULTS

The data collected through the user studies and the interviews were recorded and analyzed. The audio responses of the participants were transcribed by one of the researchers. We report both the quantitative and the qualitative results from the study in this section. For statistical significance, we used paired t-tests when comparing continuous data for the within-subjects condition such as the inter-stroke rate for each user between grace and non-grace periods. We used one-way ANOVA when comparing continuous data for the within-subjects condition for the four authentication configurations (e.g., context-switch overhead). We used chi-squared tests when comparing participants' responses to categorical Likert-type questions.

5.1 Study Participants

We advertised the study through our university-wide mailing list and through the graduate student research portal of our university. The study was advertised with the title "Evaluating authentication schemes for smartphones" and we recruited only those users who had prior experience with using smartphones. Participants received $10 for their participation for an hour of study.

We recruited 30 participants for the study (see Table 1 for their demographics). All the participants were students from

N=30		
Gender	60%	Females
	40%	Males
Age	33%	Under 20 years
	57%	21-25 years
	7%	26-30 years
	3%	31-35 years
Lock device?	26 (87%)	Yes
	4 (13%)	No
Authentication scheme	13/26	Pattern-lock
	5/26	PIN (4 digits)
	6/26	Fingerprint
	2/26	Password
Protecting from?	25/26	Strangers
	16/26	Friends
	14/26	Room-mate
	14/26	Coworker
	3/26	Spouse, own children

Table 1: Demographic information and the device lock usage pattern of the participants.

our university. The majority of our participants (87%) reported that they locked their device. The security preferences of participants who locked their devices are provided in Table 1. We asked the four participants who did not lock their devices for their reason to do so: two indicated that they had nothing to protect, two wanted their emergency contacts to be available and one considered authentication to be inconvenient (multiple answers were possible).

5.2 Quantitative Results

Out of 30 participants, 18 participants chose to use a pattern-lock during the study, while the remaining participants chose to use a PIN. Participants were subjected to five rounds in total. During the first round, participants were not interrupted for re-authentication. This round was used to establish a baseline and we use the term BASE_ROUND to refer to it. For the remaining rounds, participants tested one of the four configurations in each round. The order of the configurations was random during the four rounds.

During each round, participants completed four text entry tasks and two email tasks. They re-authenticated once for every email and text entry task during all rounds except BASE_ROUND. The high rate of re-authentication is not representative of a real-world scenario; however, our motivation was to get participants acquainted with the configurations and to collect sufficient data to evaluate the metrics used in this section. During the study each participant re-authenticated themselves 16 times during the text entry activity (four times per configuration) and eight times during the email activity (twice per configuration). In total, 120 re-authentication events, 120 text entry tasks and 60 email tasks were logged per configuration by our apps.

5.2.1 *Effect on task completion overhead*

The task completion time is the time taken by the users to complete a text entry or an email task. It also includes the time taken by the users to re-authenticate themselves while evaluating one of the configurations. The task completion overhead is the additional time taken to complete a text entry task as compared to the BASE_ROUND in which a user is not interrupted to re-authenticate. For the task completion overhead, we only take into account the text entry activity since the emails used for the email activity were of a different nature and length during each round. Our goal is to find if there are any re-authentication prompt configurations that assist the users in completing their text entry tasks faster.

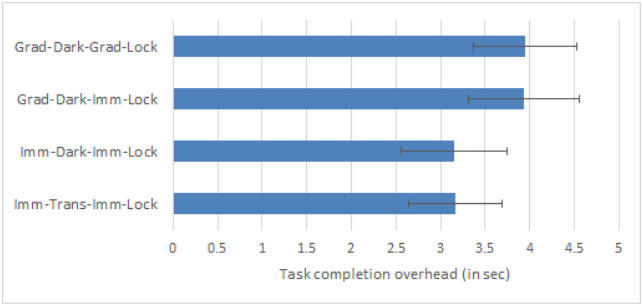


Figure 2: Task completion overhead time for the text entry activity relative to the BASE_ROUND (error bars represent 95% confidence interval).

We found that on average users took 3-4 seconds longer when they had to re-authenticate during a text entry task (see Figure 2). A one-way between subjects ANOVA was conducted to compare the effect of the four configurations on the task completion overhead, which indicated no significant differences across the four configurations *(F(3,116)=2.31, p=0.08)*.

Discussion: Our expectation that the Imm-Dark-Imm-Lock configuration is less efficient as compared to the modified re-authentication prompt configurations turns out to be incorrect. Though, we did not find any significant differences in the performance of the configurations, the participants mentioned during the study that they felt that their performance was affected during the Imm-Dark-Imm-Lock configuration:

> "It kind of freaks me out because it is too sudden, it slows down whatever I was doing." (P4)

5.2.2 *Effect on context switch overhead*

Context switch overhead for the text entry task is defined as the time taken by the users to resume their text entry task once they have re-authenticated. The context switch overhead is represented by the time interval between the dismissal of the re-authentication prompt and the first key press on the text entry task once the re-authentication prompt has disappeared. It was not possible to compute this metric for the email task because after re-authenticating a user would complete reading the email text visible on the screen before interacting with the device. Our expectation was that a visual of the user task in the background would reduce the context switch overhead. To confirm this, we conducted a one-way between subjects ANOVA to compare the effect of the four configurations on the context switch overhead. However, the results indicate no significant differences across the four configurations *(F(3,116)=1.15, p=0.33)*.

Discussion: While no statistically significant differences were observed, during the interviews, most users found the Imm-Dark-Imm-Lock configuration to be abrupt and reported that it was difficult to resume their task after re-authentication:

> "I lost my place [context] on what I was doing before [the lock appeared], so it is my least favourite. It would be too frustrating for me for everyday use, so I would rather take the risk." (P9)

> "You can't prepare for what's going to come. It takes more time to pick up after unlock" (P10)

5.2.3 *Effect of grace period*

We allowed a grace period of four seconds for the Grad-Dark-Grad-Lock configuration. During the grace period the participants could continue working on their task for four seconds before getting locked out. We observe that all participants took advantage of this grace period by continuing their work during the text entry activity. The average task completion time for the Grad-Dark-Grad-Lock configuration was 13 seconds and we found that on average users entered 38% of the text during the four second grace period with some users entering up to 60% of the total text in the grace period. A similar trend was observed for the email task where 23% of the swipe events occurred during this period (average time to complete the email task for the Grad-Dark-Grad-Lock configuration was 41 seconds).

We find that the inter-key intervals (time interval between two consecutive key presses) of the users reduced significantly for the Grad-Dark-Grad-Lock configuration during the grace period. The average inter-key interval of users reduced by almost 60% during the grace period when compared to the average inter-key interval during the task (see Figure 3). A paired t-test was conducted to compare the inter-key interval between the grace and non-grace period for the same text entry activity for each user. The results show that inter-key intervals are significantly different between the grace and non-grace period *($t(29) = 2.1$, $p = 0.04$)*.

Discussion: Our results indicate that participants took advantage of the grace period by attempting to quickly complete the text entry activity. They typed faster than their normal speeds during the grace period.

5.2.4 *Effect on task error rate*

In case the input of the users mismatched the displayed text for the text entry task, we counted it as an error (with at most one error per task). Our results indicate that users made errors in 77 out of 600 text entry tasks. However, a one-way between subjects ANOVA for the task error rate across the four configurations and BASE_ROUND indicates no significant differences *($F(4,145)=1.51$, $p=0.2$)*. Similarly, while participants made errors in 43 out of 240 email tasks, the differences were not significant across the different configurations *($F(4,28)=0.28$, $p=0.84$)*.

Discussion: The task error rate among the configurations were comparable. Though the inter-key interval of the users during the grace period reduced significantly, it did not affect the task error rate compared to the other authentication configurations.

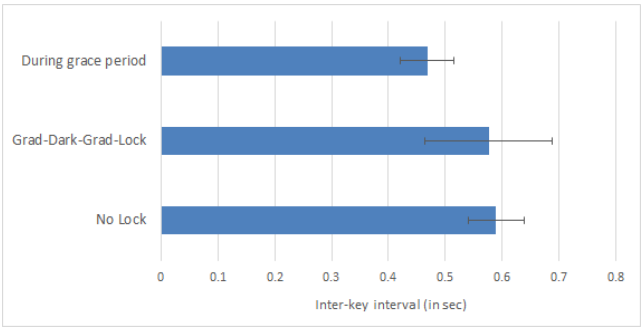


Figure 3: Inter-key interval for the text entry activity (error bars represent 95% confidence interval). The top bar represents the inter-key interval for the Grad-Dark-Grad-Lock configuration during the grace period.

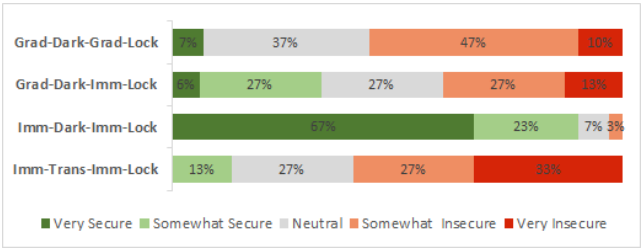


Figure 4: User perceptions of the security of the four re-authentication prompt configurations.

5.3 Qualitative Feedback

For the apps evaluated in this work, 100%, 73%, 60% and 30% of the participants considered the banking, email, photo and contacts app to be sensitive, respectively. The responses to the pre-study question regarding the adversaries that the participants (who used protection) wanted protection against indicate that different scenarios require different levels of protection. Almost all users wanted protection against strangers, which corresponds to the bus scenario. Corresponding to the office scenario, 54% of participants wanted protection against co-workers. On the other hand only 11% of participants considered that they needed protection against family members, which corresponds to the home scenario.

We now present the findings from the feedback of the participants regarding the usability and security perceptions of the configurations for each app in the different usage scenarios.

5.3.1 *Security perceptions*

Figure 4 shows the security perceptions of the participants for each re-authentication configuration. Significantly more (57% more) participants thought that the Imm-Dark-Imm-Lock configuration was more secure than the other configuration ($\chi^2(3) = 151, p < 0.001$). Imm-Dark-Imm-Lock immediately hides the content on the screen to prevent the leakage of any sensitive information. Some participants indicated that they would take advantage of this increased security at the cost of usability for some apps:

> "If I am sending an important email, I do not want anybody else to look at it even for a second. It is annoying but it would be the most beneficial." (P13)

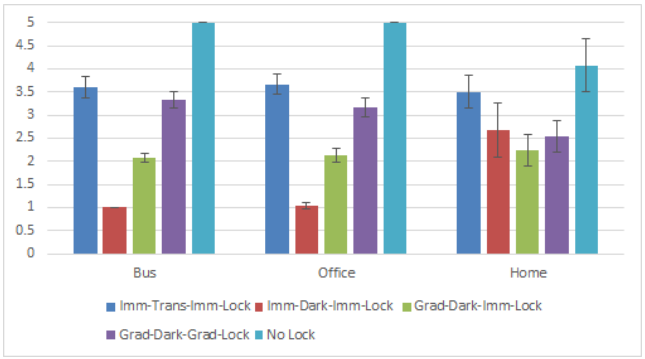


Figure 5: User preference of the configurations for the banking app in different scenarios. 1 represents the most preferred configuration while 5 represents the least preferred configuration (error bars represent 95% confidence interval).

This was followed by the Grad-Dark-Imm-Lock configuration, which was considered to be secure by 33% of the participants. We found that only 13% and 7% of the participants considered the Imm-Trans-Imm-Lock and Grad-Dark-Grad-Lock configurations to be secure. As expected, the visible task in the background is perceived negatively by most users in terms of security. The Grad-Dark-Grad-Lock configuration provides access to the device for a short period of time and participants felt that their content was vulnerable during this period. We now explore whether the configurations that were perceived to be less secure were considered appropriate for some usage scenarios.

> "I liked the idea that how the lock appears at the start [during Grad-Dark-Imm-Lock], so if it is someone else, they can't enter any text message and they can't send anything compared to the last scheme [Grad-Dark-Grad-Lock] where they can do anything if they are fast enough" (P4)

The Imm-Dark-Imm-Lock configuration was perceived most secure and all participants indicated that they would only consider using this configuration for their banking app on a bus and at the office (see Figure 5). On the other hand, for the home scenario, users had different preferences. 40% of the users indicated that they would still only consider using the Imm-Dark-Imm-Lock configuration for the banking app at home while 23% of the users indicated that they would prefer using the Grad-Dark-Imm-Lock configuration instead. Some of the user comments shed more light on the user preferences for the banking app:

> "Banking would be very sensitive, so I want it to get dark as quickly as possible." (P9)
>
> "Even with my partner, I won't feel completely secure with my banking app opened on my phone that is why I would prefer immediate dark." (P4)

The feedback from the users was inconclusive for the email app and there is no one configuration that users significantly prefer over the other for the different usage scenarios. On the other hand, for the photos app, the majority of

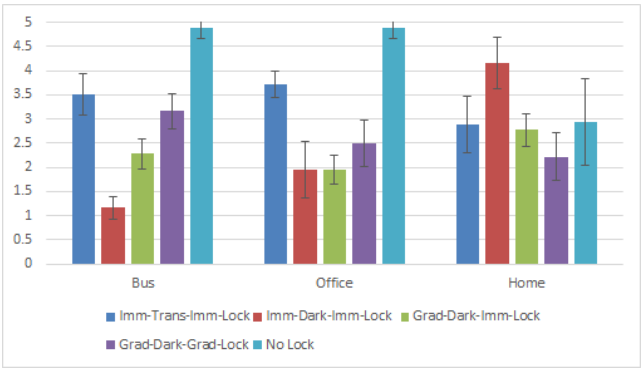


Figure 6: User preferences for the configurations for the photos app in different scenarios. Only users who consider the photos app as sensitive are included (N=18). 1 represents the most preferred configuration while 5 represents the least preferred configuration (error bars represent 95% confidence interval).

the participants who considered the photos app to be sensitive preferred the Imm-Dark-Imm-Lock configuration for the bus scenario (Figure 6). For the office scenario, the participants who were very concerned about protecting their photos preferred configurations that obscured or gradually obscured the app, preventing it from being accessed by their co-workers:

> "I won't care about my photos with respect to a stranger but in office where its more professional environment with the people I know, I would increase the security of the scheme." (P12)
>
> "I have a lot of photos that are very personal and I don't want them [strangers] to see any part of them." (P6)
>
> "I might have already shared a lot of photos with my partner, so I would prefer a comfortable lock scheme." (P6)

For the contacts app, the participants were willing to use configurations that provided device access for a period before locking them out. They wanted it so because this would allow a stranger to contact them in case they lost their device. The participants were less concerned about securing their contacts at home or office because they felt that they shared contacts with individuals at these locations.

> "If someone picked up my phone and they are looking at my contacts, they could try to return it to me through someone in my contacts, so I would choose something except the one that turns dark immediately." (P7)
>
> "For contacts, now there is an issue of privacy because these are people which they [office colleagues] might also know, so it is important that I protect their information but at the same time I don't want it to be very inconvenient for me when I look at the contacts." (P2)

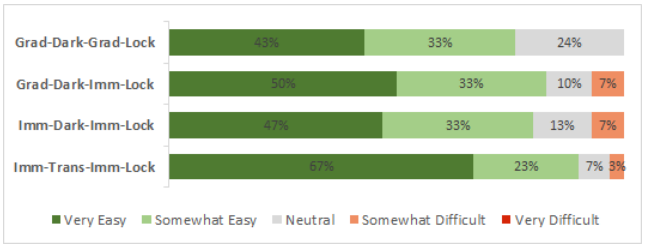


Figure 7: User perceptions on how easy it was to use the evaluated configurations.

The configuration preferences in terms of the percentage of users willing or not willing to use a particular configuration for various scenarios are presented in Appendix C.

Discussion: The participants considered the Imm-Dark-Imm-Lock configuration to be the most secure out of all four configurations. The inclination of the users while selecting the configurations are location- and app-based. While they prefer the Imm-Dark-Imm-Lock configuration to protect their banking information, they prefer to protect access to the photos app only at unknown locations. Users feel comfortable while browsing their device at home, and care less about using a more secure configuration except for the banking app.

5.3.2 Usability perceptions

Our main goal while designing these configurations was to reduce the usability issues with re-authentication reported by Khan et al. [19]. To this end, our configurations provided the users a visual of their tasks or a grace period to continue their work without disruption. We now present the perceived usability of these configurations.

We asked the users to rate the configurations in terms of ease of use. Figure 7 summarizes the responses of the users. We found that all configurations received a high rating in terms of ease of use and there were no statistically significant differences among the four configurations. In addition to a positive reception of the fade-in effect in Grad-Dark-Grad-Lock, users utilized the grace period to input data. Some of the users' comments include:

> "It helps you to continue typing and get your thoughts out. It didn't allow you to access the app though [after sometime] so it is a good balance between usability and security." (P16)

> "If I was in a rush to send an email to a client or my boss, I wouldn't want it to immediately get dark, I would want that buffer time to carry on my thoughts." (P4)

We also asked users how obstructive and annoying they thought each configuration was. Their responses (see Figure 8) indicate that significantly more participants considered the Imm-Dark-Imm-Lock configuration as more obstructive ($\chi^2(3) = 96, p < 0.01$). Similarly, Figure 8 shows that significantly more participants considered the Imm-Dark-Imm-Lock configuration was more annoying ($\chi^2(3) = 71, p < 0.01$). In terms of obstructiveness, 70% of the

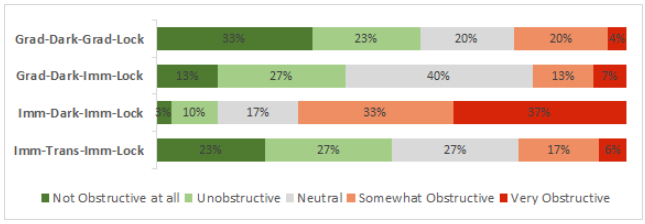


Figure 8: User perceptions regarding obstructiveness of the configurations.

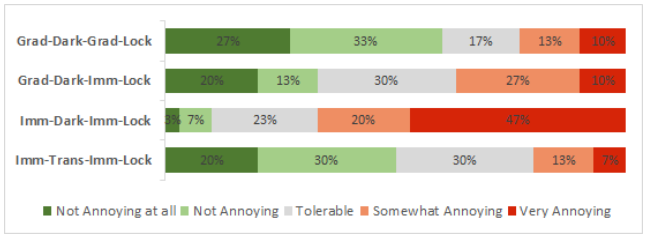


Figure 9: User perceptions regarding annoyance of the configurations.

participants rated the Imm-Dark-Imm-Lock configuration as somewhat or very obstructive and 67% of the participants rated it as somewhat or very annoying (Figure 9). This explains why Imm-Dark-Imm-Lock was the least preferred configuration for the users for email (47%), photos (52%) and contacts (47%) apps for the home scenario. On the other hand, users positively perceived the gradual fading of the screen transparency and the delay of the authentication prompt. User comments that reflect these findings are:

> "I lost my place what I was doing before [the lock appeared], so it is my least favorite. It would be too frustrating for me for everyday use, so I would rather take the risk." (P9)

> "I found it [Imm-Dark] very annoying because it was really an abrupt interruption to me, others were not abrupt." (P8)

> "When you were explaining to me, I thought it would be difficult to wait for the lock but I guess it was nice to not lock right away, so you can continue what you are doing and wait for it to come up." (P12)

Discussion: While the Imm-Dark-Imm-Lock was considered most secure and was preferred for sensitive apps and risky scenarios, it annoyed the users. On the other hand, the less secure configurations were perceived to be more usable and users preferred those for less sensitive apps and for medium- and low-risk scenarios.

5.3.3 Overall Perceptions

We found no significant difference when users were asked to rank the four configurations in the order of their preference while considering both the security and the usability of the configurations. Our results suggest that the users generally find it hard to select a particular configuration as their most preferred configuration and their choices are influenced largely by their perceived levels of the sensitivity of

the apps they are using and their perceived security of the surrounding environment.

6. DISCUSSION

In this section we discuss our findings from the semi-structured interviews and suggest future directions.

Annoyance due to the fade-in effect: While the majority of users responded positively to the modified re-authentication prompt configurations, six participants found the fade-in effect to be annoying. During the interviews, these participants indicated that the cause of this annoyance was the wait for the authentication prompt to appear:

> "I would rather deal with the lock as quickly as I can so I can get back to using the phone." (P9)

One participant suggested that the source of annoyance was its resemblance to the interruption on the web for subscription-based content:

> "I don't like it at all because it reminded of those websites, where you are scrolling and it stops letting you read the content and that kind of is obstructed and annoying." (P7)

We now outline the alternates that were suggested by these and other participants.

Participants' suggestion on how to re-authenticate: We sought suggestions from the participants during the semi-structured interview on how the re-authentication should be performed or improved. They proposed displaying a small timer at the top of the screen to indicate the time left before the users would be re-authenticated. Their comments were:

> "Maybe it can prompt you to type out a pattern on your phone without the visual obstruction, maybe like a small notification. It will warn you that it is going to lock and you can dismiss it by providing the secret." (P9)
>
> "Maybe instead of gradual fading, you can have a small timer up there on the screen near the status bar so that I should be expecting to get a lock screen." (P15)

Other comments regarding the design and display of the re-authentication prompt suggest that the delay before the appearance of the re-authentication prompt and the colour of the screen during the fade-in effect should be customizable.

Future design implications: Participants' responses show that the evaluated configurations are more usable albeit less secure than the Imm-Dark-Imm-Lock configuration. More specifically, in terms of participants' ratings, Section 5 showed that the Imm-Dark-Imm-Lock configuration favored security at the cost of usability whereas, all other configurations favored usability at the cost of security. Participants' feedback suggests that no particular configuration provides an optimum trade-off between usability and perceived security for re-authentication across all scenarios.

Furthermore, while most participants of our study had similar security preferences in terms of the three scenarios evaluated in this study, there was disagreement regarding the security preferences for the four apps. Therefore, re-authentication schemes need to provide users with a control to define these security preferences. A comment by a participant demonstrates the need for this:

> "You can have three different levels of security [depending on security preferences] and group your apps into those levels depending on the security you want for each app." (P9)

Similar to the findings of research efforts on primary authentication schemes, our findings indicate that future experiments on user re-authentication should leverage app sensitivity and location information to ease the re-authentication burden. For instance, an enterprise email client can use a more usable configuration to re-authenticate when the user is within the office building. Similarly, a banking app, which is providing additional security through an app-level IA mechanism [18], should use the Imm-Dark-Imm-Lock configuration.

7. LIMITATIONS OF THE STUDY

Similar to other human subject experiments, our participants were limited to those willing to participate. The feedback given by the participants was subjective in nature and therefore represents only the results of a limited sample of the population. Each participant had a different perception of the security level of the apps and the scenarios presented to them. For instance, for all apps (except for the banking app), the same app was rated by some participants as 'very sensitive' and by others as 'not sensitive at all'.

Another limitation is the smaller portion of participants (13%) who did not use any authentication mechanism on their smartphones. The usability and security perceptions of the configurations may have been different if more users perceived primary authentication schemes as inconvenient. Since participation in the study was voluntary, we had little control over preventing this disparity. Furthermore, the majority of our participants were students which may limit the generalization potential of our results. For instance, working professionals may have more sensitive data on their devices and they may have different security preferences.

For re-authentication purposes, the authentication prompt was presented to the participants in the center of the screen. This placement may have negatively affected the context switch overhead. An evaluation of other placement options, including a split screen configuration where the authentication prompt shares the screen with the user activity (see § 3.1) is a potential area of study in the future. We did not counterbalance the order of the configurations across the participants, which may have introduced bias.

A lab-based evaluation was performed because it was sufficient to achieve our objectives. However, we acknowledge that our participants were not subjected to real attacks and only considered hypothetical scenarios to evaluate the configurations. While performing experiments on the user device would have reduced issues due to user's unfamiliarity with the device and may have emphasized the need to protect their sensitive data, for the purpose of this study, we used synthetic tasks on a Nexus 5 device that was provided by the researchers. The synthetic tasks were used to take

measurements and a researcher provided device was used to avoid bias due to different screen sizes and type of devices.

8. RELATED WORK

Researchers have extensively investigated the usability issues with primary authentication schemes [5, 15, 34, 36] and have shown that these issues prevent users from using these schemes [9, 15]. Our research focus is to investigate different configurations of a subset of these schemes (PIN and pattern-lock) for re-authentication purposes and not to address previously uncovered usability issues issues (e.g., time consuming, considered unnecessary for some cases [15]) with these schemes.

To mitigate the usability issues, several research proposals have been put forth that reduce the authentication overhead of the users by leveraging user behaviour [21, 32, 37], device context [16, 24, 25] or the sensitivity of launched apps [17]. We provide a brief overview of these schemes in § 2.1. During the usability evaluation of a behaviour-based scheme, Khan et al. [19] observe the usability issues arising from re-authentications due to false rejects. They also list some suggestions by their participants on how the negative usability effects of re-authentications can be mitigated. One suggestion was to not interrupt the user and instead send an email alert or take a picture of the perpetrator. Another, more secure suggestion that inspired this work was to authenticate the user in a smaller portion of the screen in parallel and to offer the user a grace period before the device locks out.

Another line of research has focused on addressing the usability issues with existing primary authentication schemes by proposing alternate mechanisms, including gesture-based authentication [1, 7, 31] or graphical passwords [20, 30]. Users have reported positive experiences during preliminary evaluations of these schemes [1, 30]. We considered using different configurations of these schemes for re-authentication in our study; however, the usability perceptions of the participants would have been biased due to their missing experience with these schemes. Instead, participants evaluated different configurations of an authentication scheme that they are already familiar with in our study.

Another related work is SnapApp [3], which is a primary authentication mechanisms that provides a trade-off between security and usability. It presents a user with two unlock methods on the device screen — a PIN for secure access to all the device and a simple slide gesture for fast yet temporary access (30 seconds or less) to the device. Similar to our work, SnapApp favors usability at the cost of security; however, it is not a re-authentication scheme. To the best of our knowledge, our paper performs the first ever evaluation of modified primary authentication schemes for re-authentication scenarios.

9. CONCLUSION

We have proposed two modifications to the default authentication prompts of two primary authentication schemes (PIN and pass-lock) to make them more suitable for re-authentication scenarios: a transparent authentication prompt and a time delay before the authentication prompt appears. In terms of task performance, the proposed configurations perform as well as the default configuration however, the proposed configurations were perceived to be more convenient and less annoying by the users. We observe that user preferences of the configurations are largely context-based and there is no particular configuration that users want to use at all times. In terms of preference, while users want to use the default configuration (which obscures the app content) for highly sensitive apps, their choices for medium and less sensitive apps are influenced by their perception of the security of the surrounding environment and users preferred the proposed configurations for most of the less risky scenarios.

In terms of future work, a field study needs to be performed to understand the real-world performance of these configurations. Furthermore, since smartphone users who do not configure authentication on their devices are potential users of novel authentication strategies (such as IA), an evaluation study needs to be performed with such participants. Finally, our experiment suggests the need to design new re-authentication strategies that satisfy the unique usability and security requirements of re-authentication.

10. ACKNOWLEDGMENTS

Thanks to our shepherd, E. von Zezschwitz, and the anonymous reviewers for their valuable comments. We also thank Google, NSERC and the Ontario Research Fund for their support.

11. REFERENCES

[1] M. T. I. Aumi and S. Kratz. Airauth: evaluating in-air hand gestures for authentication. In *16th International Conference on Human-computer Interaction with Mobile Devices & Services*. ACM, 2014.

[2] J. Bonneau, E. W. Felten, P. Mittal, and A. Narayanan. Privacy concerns of implicit secondary factors for web authentication. In *SOUPS Workshop on "Who are you"*. ACM, 2014.

[3] D. Buschek, F. Hartmann, E. von Zezschwitz, A. De Luca, and F. Alt. Snapapp: Reducing authentication overhead with a time-constrained fast unlock option. In *CHI Conference on Human Factors in Computing Systems*. ACM, 2016.

[4] H. Crawford and K. Renaud. Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management*, 1(1), 2014.

[5] 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 *33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015.

[6] A. De Luca, E. Von Zezschwitz, and H. Hußmann. Vibrapass: secure authentication based on shared lies. In *SIGCHI conference on Human factors in computing systems*. ACM, 2009.

[7] A. De Luca, E. Von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich. Back-of-device authentication on smartphones. In *SIGCHI conference on Human factors in computing systems*. ACM, 2013.

[8] B. Draffin, J. Zhu, and J. Zhang. Keysens: Passive user authentication through micro-behavior modeling of soft keyboard interaction. In *Mobile Computing, Applications, and Services*. Springer, 2013.

[9] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are you ready to lock? In *ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014.

[10] T. Feng, X. Zhao, B. Carbunar, and W. Shi. Continuous mobile authentication using virtual key typing biometrics. In *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2013.

[11] D. Ferreira, J. Goncalves, V. Kostakos, L. Barkhuus, and A. K. Dey. Contextual experience sampling of mobile application micro-usage. In *16th International Conference on Human-computer Interaction with Mobile Devices & Services*. ACM, 2014.

[12] J. Frank, S. Mannor, and D. Precup. Activity and gait recognition with time-delay embeddings. In *AAAI*. Citeseer, 2010.

[13] M. Frank, R. Biedert, E.-D. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *Information Forensics and Security, IEEE Transactions*, 8(1), 2013.

[14] C. Giuffrida, K. Majdanik, M. Conti, and H. Bos. I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. In *Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2014.

[15] 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 *Symposium On Usable Privacy and Security*. ACM, 2014.

[16] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley. Casa: context-aware scalable authentication. In *Symposium on Usable Privacy and Security*. ACM, 2013.

[17] E. Hayashi, O. Riva, K. Strauss, A. Brush, and S. Schechter. Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. In *Symposium on Usable Privacy and Security*. ACM, 2012.

[18] H. Khan and U. Hengartner. Towards application-centric implicit authentication on smartphones. In *15th Workshop on Mobile Computing Systems and Applications*. ACM, 2014.

[19] H. Khan, U. Hengartner, and D. Vogel. Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In *Symposium On Usable Privacy and Security*. ACM, 2015.

[20] T. Kwon and S. Na. Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems. *Computers & security*, 42, 2014.

[21] L. Li, X. Zhao, and G. Xue. Unobservable re-authentication for smartphones. In *NDSS*, 2013.

[22] S. Mare, A. M. Markham, C. Cornelius, R. Peterson, and D. Kotz. Zebra: zero-effort bilateral recurring authentication. In *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2014.

[23] A. Mariakakis, M. Goel, M. T. I. Aumi, S. N. Patel, and J. O. Wobbrock. Switchback: Using focus and saccade tracking to guide users' attention for mobile task resumption. In *33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015.

[24] N. Micallef, M. Just, L. Baillie, M. Halvey, and H. G. Kayacik. Why aren't users using protection? investigating the usability of smartphone locking. In *17th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, 2015.

[25] M. Miettinen, S. Heuser, W. Kronz, A.-R. Sadeghi, and N. Asokan. Conxsense: automated context classification for context-aware access control. In *9th ACM Symposium on Information, Computer and Communications Security*. ACM, 2014.

[26] E. Miluzzo, T. Wang, and A. T. Campbell. Eyephone: activating mobile phones with your eyes. In *2nd ACM SIGCOMM Workshop on Networking, Systems, and Applications on Mobile Handhelds*. ACM, 2010.

[27] M. Muaaz and R. Mayrhofer. An analysis of different approaches to gait recognition using cell phone based accelerometers. In *International Conference on Advances in Mobile Computing & Multimedia*. ACM, 2013.

[28] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos. Progressive authentication: deciding when to authenticate on mobile phones. In *21st USENIX Security Symposium*, 2012.

[29] F. Schaub, R. Deyhle, and M. Weber. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *11th International Conference on Mobile and Ubiquitous Multimedia*. ACM, 2012.

[30] F. Schaub, M. Walch, B. Könings, and M. Weber. Exploring the design space of graphical passwords on smartphones. In *Symposium on Usable Privacy and Security*. ACM, 2013.

[31] M. Shahzad, A. X. Liu, and A. Samuel. Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it. In *19th Annual International Conference on Mobile Computing & Networking*. ACM, 2013.

[32] E. Shi, Y. Niu, M. Jakobsson, and R. Chow. Implicit authentication through learning user behavior. In *Information Security*. Springer, 2010.

[33] W. Shi, F. Yang, Y. Jiang, F. Yang, and Y. Xiong. Senguard: Passive user identification on smartphones using multiple sensors. In *7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2011.

[34] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In *28th Annual Computer Security Applications Conference*. ACM, 2012.

[35] E. von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann. Swipin: Fast and secure pin-entry on smartphones. In *33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015.

[36] E. Von Zezschwitz, P. Dunphy, and A. De Luca. Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In *15th International Conference on Human-computer interaction with Mobile Devices and Services*. ACM, 2013.

[37] H. Xu, Y. Zhou, and M. R. Lyu. Towards continuous and passive authentication via touch biometrics: An

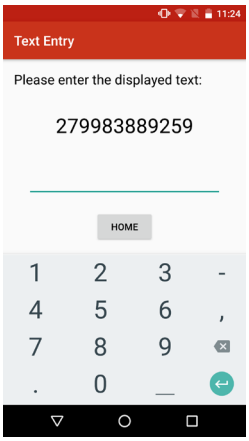
experimental study on smartphones. In *Symposium On Usable Privacy and Security*. ACM, 2014.

[38] T. Yan, D. Chu, D. Ganesan, A. Kansal, and J. Liu. Fast app launching for mobile devices using predictive user context. In *10th International Conference on Mobile systems, Applications, and Services*. ACM, 2012.

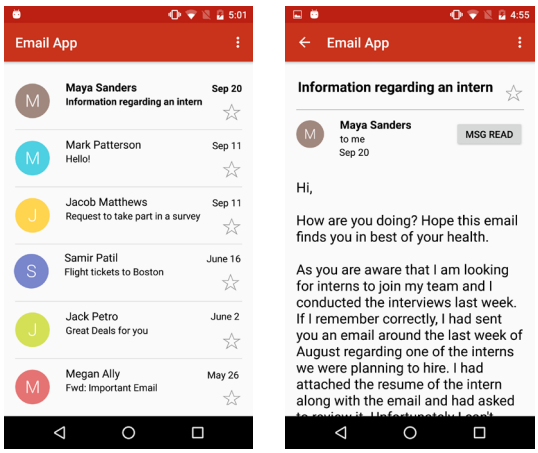
APPENDIX

A. SYNTHETIC TASK SCREENS

Figure 10 provides screen captures for the synthetic tasks performed during the user study.



(a) Text Entry Activity



(b) Email Activity

Figure 10: The activities performed by the participants during the user study. Figure (a) shows the text entry activity containing a 12-digit number, Figure (b) shows the email activity

B. SPLIT-SCREEN CONFIGUATION

Figure 11 provides screen captures for the split-screen configuration. While the *screen transparency* parameter for both Imm-Trans (Figure 11a) and Imm-Dark (Figure 11b) cases were similar to the originally proposed lock configurations, we modified the Grad-Dark configuration (Figure 11c) such that instead of gradually turning the screen dark, we used a vertical slider to gradually hide the content displayed on the top half of the screen.

C. CONFIGURATION PREFERENCES OF THE USERS

Table 2 provides an overview of the participants' re-authentication prompt preferences for the email, contacts and photos app in the bus, office and home scenarios. As mentioned in § 5.3.1, all participants preferred the Imm-Dark-Imm-Lock configuration for the banking app. For each scenario, we mention the proportion of users who are (not) willing to use a particular configuration. Users who gave a rating of 1 or 2 on a 5-point Likert scale were considered to be willing while users who gave a rating of 4 or 5 were considered unwilling to use that configuration.

D. PRE-STUDY SURVEY

Before the study, participants were asked about their security preferences. In addition, we collected demographic information from participants including their name, age group, gender, highest level of education and their current occupation.

D.1 Device Lock Usage

1. Do you currently use a lock mechanism on your phone?
   (a) Yes; (b) No
2. **If they use a lock mechanism:** Which lock mechanism do you use to lock your device?
   (a) PIN Lock (4-digit or more); (b) Password (characters and numbers); (c) Pattern-lock; (d) Fingerprint Recognition; (e) Face Recognition
3. **If they use a lock mechanism:** Who do you want to protect your smartphone access from? (choose all that apply)
   (a) Coworker; (b) Friends; (c) Spouse; (d) Own children; (e) Room-mate; (f) Other unwanted individual or stranger
4. **If they do not use a lock mechanism:** Why do you not use a lock mechanism on your phone? (choose all that apply)
   (a) It takes time to unlock the phone; (b) I don't have any data on my phone which needs to be protected; (c) No one would care what is on my phone; (d) In an emergency, others can use my phone; (e) I have never thought about it

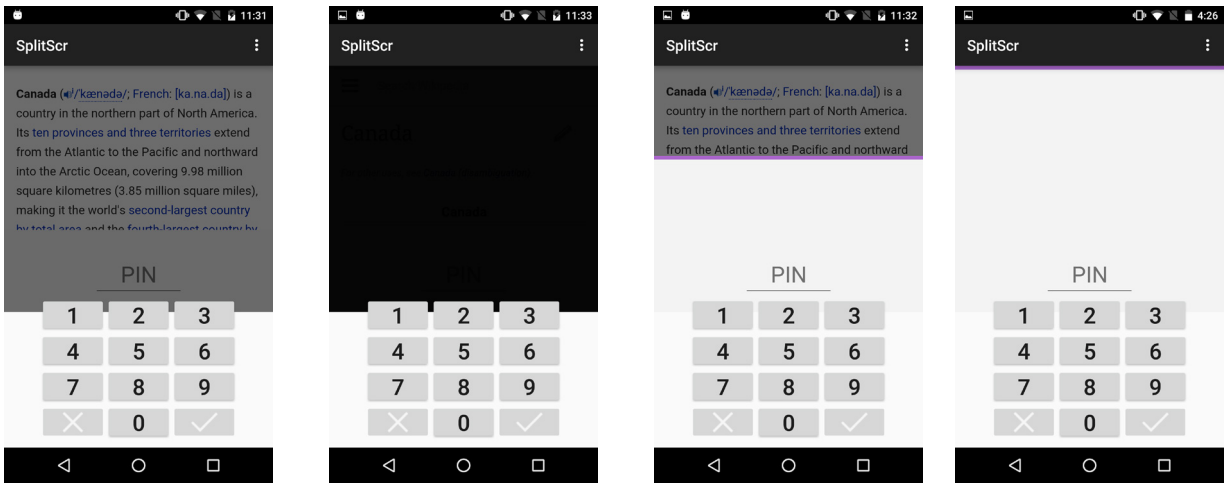
E. STUDY QUESTIONNAIRE

E.1 User perception of individual configurations

After the participants completed both activities using one of the four configurations, we asked them to give feedback on their experience with the evaluated configuration using the following questionnaire.

- Evaluate each of the following configurations that you will observe while doing the experiment. For each category, rate each configuration on a 5-point-Likert scale.

1. Immediate Dark Immediate Lock: Screen turns dark right away and PIN/Pattern appears
2. Immediate Transparent, Immediate Lock: Screen turns and stays transparent and PIN/Pattern appears right away



(a) Imm-Trans (b) Imm-Dark (c) Grad-Dark

Figure 11: The proposed split-screen configurations with varying values of the *screen transparency* parameter. For the Grad-Dark configuration, a vertical slider moves up to gradually hide the content displayed on the top half of the screen.

3. Gradual Dark, Immediate Lock: Screen slowly turns dark and PIN/Pattern appears right away
4. Gradual Dark, Gradual Lock: Screen slowly turns dark and PIN/Pattern appears after a while

(Questions to obtain users' feedback. All questions are on a 5-point Likert-type scale.)

1. Assume someone picks up your smartphone and starts reading your emails. How secure do you find the scheme to protect your data in this scenario?
   (5- Very Secure, 1- Very Insecure)
2. How easy was it to use the scheme?
   (5- Very Easy, 1- Very Difficult)
3. How obstructive was the scheme?
   (5- Not Obstructive at all, 1- Very Obstructive)
4. How annoying was the scheme?
   (5- Not Annoying at all, 1- Very Annoying)

(Once the participant evaluated and rated all four configurations, we asked them to rank them in the order of their preference.)

- Rank the schemes in your order of preference. Please take both the scheme's security and its usability into account.
  (1- Most Preferred Scheme, 4- Least Preferred Scheme)

E.2 Context-based feedback of the configurations

E.2.1 Sensitivity Ratings

Please provide a sensitivity rating of the following apps given how you use your mobile device and how sensitive you think each app is:

1. Email App
2. Contacts App
3. Photos App
4. Banking App

(5- Very sensitive, 1- Not very sensitive)

E.2.2 Scenarios

Now imagine the following scenarios and select which lock mechanism you would prefer in each case. The lock mechanism will get activated in case the system notices any suspicious activity. Please remember that since the system does not have 100% accuracy, it may assume you to be an adversary and you could encounter one of the lock mechanisms while you are using the device yourself. Assume that all of the apps below are protected only with implicit authentication and no other protection mechanism.

Bus Scenario

Imagine you riding a bus and you accidently leave your smartphone on the bus. A stranger picks your device and uses it, which gets detected by the implicit authentication protection mechanism on your device. The stranger may launch different apps on your smartphone. For each app, the implicit protection mechanism could take a different action when detecting misuse. For each of the apps listed below, rank the order of preference of the lock scheme you would prefer with 1 being your most preferred lock scheme and 5 being your least preferred lock scheme.

Please remember that even you could encounter these schemes while you are using your phone on the bus.

1. Views the emails in your inbox
2. Looks at the contacts on your smartphone
3. Views the photos stored on your smartphone
4. Accesses the banking app on your smartphone

		Bus		Office		Home	
		Would like to use?	Would not like to use?	Would like to use?	Would not like to use?	Would like to use?	Would not like to use?
Emails	Imm-Trans-Imm-Lock	27%	**53%**	27%	40%	47%	26%
	Imm-Dark-Imm-Lock	**70%**	13%	**50%**	37%	10%	**70%**
	Grad-Dark-Imm-Lock	**60%**	7%	**67%**	13%	37%	40%
	Grad-Dark-Grad-Lock	37%	33%	**50%**	23%	**63%**	13%
	No Lock	7%	**93%**	7%	**86%**	43%	**50%**
Contacts	Imm-Trans-Imm-Lock	37%	47%	37%	20%	**50%**	33%
	Imm-Dark-Imm-Lock	40%	47%	23%	**64%**	7%	**80%**
	Grad-Dark-Imm-Lock	43%	17%	**53%**	24%	27%	36%
	Grad-Dark-Grad-Lock	**57%**	20%	**70%**	10%	**57%**	13%
	No Lock	23%	**70%**	17%	**83%**	**60%**	40%
Photos	Imm-Trans-Imm-Lock	33%	**50%**	23%	**60%**	44%	33%
	Imm-Dark-Imm-Lock	**77%**	20%	**54%**	23%	17%	**80%**
	Grad-Dark-Imm-Lock	**57%**	10%	**70%**	13%	34%	23%
	Grad-Dark-Grad-Lock	23%	33%	37%	23%	**57%**	16%
	No Lock	10%	**87%**	17%	**80%**	**50%**	47%

Table 2: Configuration preferences of the participants for different apps and scenarios. Values above 50% are in bold.

Office Scenario

Imagine you are in your office and your boss calls you for a meeting. You leave your phone on your desk and one of your office colleagues starts using your phone, which gets detected by the implicit authentication protection mechanism. Your colleague may launch different apps on your device. For each app, the protection mechanism could take a different action when detecting misuse. For each of the apps listed below, rank the order of preference of the lock scheme you would prefer with 1 being your most preferred scheme and 5 being your least preferred scheme.

Please remember that even you could encounter these schemes while you are using your phone in your office.

1. Views the emails in your inbox
2. Looks at the contacts on your smartphone
3. Views the photos stored on your smartphone
4. Accesses the banking app on your smartphone

Home Scenario

Imagine you are watching television at home with your partner and you unknowingly doze off to sleep. Your partner realizes that you are asleep and starts using your smartphone, which gets detected by the implicit authentication protection mechanism. Your partner may launch different apps on your smartphone. For each app, the implicit protection mechanism could take a different action when detecting misuse. For each of the apps listed below, rank the order of preference of the lock scheme you would prefer with 1 being your most preferred scheme and 5 being your least preferred scheme.

Please remember that even you could encounter these schemes while you are using your phone at home.

1. Views the emails in your inbox
2. Looks at the contacts on your smartphone
3. Views the photos stored on your smartphone
4. Accesses the banking app on your smartphone

F. SEMI-STRUCTURED INTERVIEWS

We asked the following questions during the semi-structured interviews:

1. What was your overall impression of the configurations?
2. Would you change anything about these configurations to improve their usability or security?
3. Did you like a particular configuration more than the other?
4. Did you dislike a particular configuration more than the other?
5. Would you be willing to use any configuration on your device for daily use? Why or why not?
6. Any particular scenarios where you think that these configurations will be useful to you?