Slide-to-Unlock Revisited: Two New User Authentication Techniques for Touchscreen-Based Smartphones

Ahmed Sabbir Arif, Ali Mazalek
Synaesthetic Media Laboratory
Ryerson University
Toronto, Ontario, Canada
{asarif, mazalek}@ryerson.ca

ABSTRACT

We present two new user authentication techniques that look and feel like slide-to-unlock. The intention is to encourage users, who do not use a user authentication technique on their devices, to start using one. Results of a user study showed that the new techniques perform relatively well compared to slide-to-unlock and digit-lock, and users find at least one of the techniques easy to use.

Categories and Subject Descriptors

K.6.5 [**Security and Protection**]: Authentication.

General Terms

Performance, Design, Experimentation, Security, Human Factors.

Keywords

User authentication; slide-to-unlock; mobile security; password.

1. INTRODUCTION

Smartphones are becoming an integral part of our everyday life. They are built with more advanced computing capability and connectivity than regular mobile phones. This allows users to perform a variety of tasks on these devices. As a result, smartphones usually accrue sensitive information over time and often gain access to wireless services and organizational intranets. This makes it vital to secure the data stored in these devices. Yet, recent surveys revealed that 34% mobile users in the U. S. and 65% in the U. K. do not take any security measure to protect their smartphone data, because they either find it too much of a hassle or worry that they will forget the password and lose access to their smartphone [3, 4]. Most smartphones (without user authentication) allow users access to the device by performing a slide-to-unlock gesture that requires dragging an icon across the touchscreen, either horizontally from left to right (iOS, Android) or vertically from bottom to top (Android, Windows Phone). Presently, the two most popular user authentication techniques for mobile phones are digit-lock and pattern-lock. A recent survey showed that about 87% U. S. mobile users, who use a user authentication technique on their devices, use one of these two methods [4]. The digit-lock method requires users to select and memorize a four-digit personal identification number (PIN) and later input it to unlock the device. It offers 10,000 unique password combinations. Pattern-lock, a graphical method, requires user to select a pattern by connecting four or more dots from a 3×3 grid. All connecting dots need to be unique. Users are allowed to connect a dot that requires going through other dots, only when those dots have already been used. Under these conditions, this method offers 389,112 unique password patterns. Many alternatives are also available, such as image selection, multi-word/phrase selection, and biometrics [2].

2. THE NEW TECHNIQUES

We present two new mobile user authentication techniques. Our inspiration for developing these techniques was the saying, “Some security is better than no security.” Our intention was not to develop techniques that are more secure than the existing ones, but that are simple and resemble the slide-to-unlock gesture, so that users who do not use an authentication technique will be encouraged to start using one and might eventually move to a more secure technique once they have grown into the habit of using one.

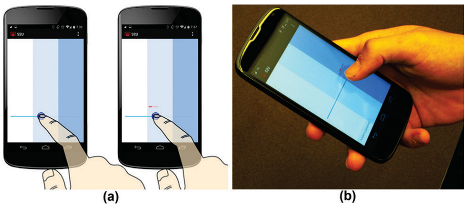

Figure 1. The custom application and the device used during the study: (a) the *sequential* and *timed* methods, respectively, (b) a user inputting a *timed* password during the study.

The **sequential-slide-to-unlock** technique allows users to select a custom slide pattern as their password. It divides the touchscreen vertically into three different zones (i.e. A, B, and C) and considers each as a distinct touch area. See Figure 1. Thus, it considers a stroke initiated from a particular zone distinct from the one initiated from a different zone. Unlike most slide-to-unlock gestures, it allows users to swipe horizontally from any zone (even from the centre), to any direction, and travel between the zones. Thus, the user can select a password that travels from zone B to C, and then to zone A (password length = 4). They can select any pattern as their password, as long as it goes through at least two different zones (password length = 2). Although, there is no upper limit on this, we noticed that users usually select passwords that requires going through the zones for less than eight times (password length < 8), for which this technique offers 70 unique password patterns.

The **timed-sequential-slide-to-unlock** technique is a variation of the *sequential* technique. In addition to selecting swipe patterns, it allows users to pick one of the three available timeframes for each zone. To select a timeframe for a zone, users have to hold their finger still on that zone for 200 ms to see a progress bar above their finger (see Figure 1). The progress bar is divided into three equal segments, each representing a different timeframe. It progresses forward in every 200 ms. If users want to select the 2^{nd} timeframe for zone A, for example, they have to hold their finger

MOBIQUITOUS 2014, December 02-05, London, Great Britain
Copyright © 2014 ICST 978-1-63190-039-6
DOI 10.4108/icst.mobiquitous.2014.257921

still on the zone for 200 ms, then continue swiping when the progress bar displays the 2nd timeframe. The progress bar iterates itself, thus, users can wait for the next iteration if they miss a queue. They could also slightly move their finger within the zone to restart the progress bar. This technique offers in total 473,536 unique password combinations (when password length < 8).

3. USER STUDY

The study to explored the new techniques' performance.

3.1 Apparatus and Participants

We used a custom application, developed with the Android SDK, on a Google Nexus 4, 133.9×68.7×9.1 mm, 139 g, for the study. It ran on Android 4.4.2 KitKat at 1280×768 pixel resolution and 320ppi. See Figure 1. It logged all interactions with timestamps and recorded user performance to the device's internal storage.

Eight participants, aged from 22 to 34 years, average 28 (SD= 4), participated in the study. They were all frequent users of mobile devices. Two of them did not use any user authentication method, while others used either digit-lock or pattern-lock. Two of them were female and one was left-handed.

3.2 Procedure and Design

In the study, users used the three techniques: *conventional* slide-to-unlock, *sequential*, and *timed*. They all started with *conventional*, then we counterbalanced the new techniques to eliminate the effect of learning. With each technique, users attempted to unlock the device 15 times. We deliberately limited the number of attempts, as a prior study showed that users easily get tired when performing gestures on mobile touchscreens [1]. A short practice block preceded each condition, where users tried the corresponding technique. Similar to conventional slide-to-unlock, the device provided users with feedback on each unlocking attempt. That is, it made a sound when users successfully unlocked the device, but vibrated for 250 ms when they failed to do so. The system did not allow users to correct their errors. It recorded a gesture from the moment users touched the screen to the moment they lifted their finger. In summary, the design was: 8 participants × 3 techniques (within-subjects, counterbalanced) × 15 attempts = 360 attempts.

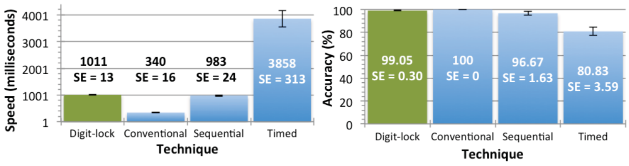

Figure 2. Average speed and accuracy with ±1 standard error.

3.3 Results

We used repeated-measures ANOVA for all analysis. For better comparison, we reported the results in comparison with digit-lock, by using data from a prior user study [1].

3.3.1 Speed and Accuracy

An ANOVA identified a significant effect of technique on entry speed ($F_{2,7} = 8.42$, $p < .005$). A Tukey-Kramer test revealed that *conventional* was the fastest of all techniques, while *timed* was the slowest. Figure 2 illustrates average entry speed for all techniques, including digit-lock.

An ANOVA identified a significant effect of technique on accuracy rate ($F_{2,7} = 2.52$, $p < .005$). A Tukey-Kramer test revealed that *timed* was significantly more error-prone than *conventional*, but failed to find a significant difference between *sequential* and *conventional*. Figure 2 illustrates average accuracy rate for all techniques, including digit-lock. Further investigation revealed that about 29% of the errors in *timed* were caused by incorrect zone selection, while the remaining 71% were caused by incorrect time selection.

3.3.2 User Feedback

Upon completion of the study users were asked to complete a short questionnaire where they could rate the examined techniques on seven-point Likert scales. Later, we converted the scales to three-point scales using linear transformation to calculate ratios.

Table 1. User responses converted to three-point scales.

Property	Technique	Agree	Neutral	Disagree
More secure than slide-to-unlock	*Sequential*	100%	0%	0%
	Timed	87.5%	0%	12.5%
Relatively easy to use	*Sequential*	87.5%	0%	12.5%
	Timed	25%	25%	50%
Easy to memorize the password	*Sequential*	87.5%	0%	12.5%
	Timed	25%	25%	50%
Want to use it dominantly on mobile device	*Sequential*	75%	12.5%	12.5%
	Timed	37.5%	12.5%	50%

3.4 Discussion

Results show that *sequential* performs relatively well compared to *conventional*. *Timed* was substantially slower and more error-prone, which is not unexpected considering the mechanism of the technique. Both techniques performed relatively well compared to digit-lock. Almost all users found the new techniques more secure than *conventional*. Most also found *sequential* relatively easy to use and to memorize a password, and wanted to use it dominantly on their devices. However, user opinions were divided regarding *timed*. About one half of the users found it difficult to use and to memorize a password, while the others were either in favour of the new technique or were neutral.

We asked users to interact with the device as they usually would with theirs. We noticed that about 50% users held the device with their dominant hand and gestured using the thumb of the same hand, while 37.5% used the index and 12.5% used the long finger of their non-dominant hand. On average, the password length for *sequential* was six, and for *timed* was four plus one timeframe.

4. CONCLUSION AND FUTURE WORK

We developed two new mobile user authentication techniques to encourage users who are reluctant to use an authentication technique to start using one. Results of a study showed that the new techniques perform relatively well and that most users found at least one of the techniques relatively easy to use.

We evaluated the new techniques only in terms of performance and user preference. In the future, we intend to evaluate their security, especially how they perform when under smudge attack or observed by bystanders. We would also like to investigate how the new techniques perform in real-life scenarios, i.e. while walking.

We would like to thank SSHRC for funding this project.

5. REFERENCES

[1] Arif, A. S., Pahud, M., Hinckley, K., and Buxton, B. A tap and gesture hybrid method for authenticating smartphone users. MobileHCI '13, ACM, 486-491.

[2] Ben-Asher, N. Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., and Möller, S. On the need for different security methods on mobile phones. MobileHCI 2011, ACM, 465-473.

[3] Henshaw, S. Two thirds of British smartphone users failing to implement basic security settings. TigerMobiles Press Releases. Jul. 31, 2014. http://goo.gl/hCwLq6

[4] Smart Phone Thefts Rose to 3.1 Million Last Year. Consumer Reports. May 28, 2014. http://goo.gl/Uk8kTX