Spin-lock Gesture Authentication for Android: Usability in a Soft-Interface

Stefania Raimondo
University of Toronto
Toronto, Canada
stefania.raimondo@mail.utoronto.ca

Alan Yusheng Wu
University of Toronto
Toronto, Canada
yusheng.wu@mail.utoronto.ca

Yomna Aly
University of Toronto
Toronto, Canada
yomna.aly@mail.utoronto.ca

Molly Wei
University of Toronto
Toronto, Canada
molly.wei@mail.utoronto.ca

ABSTRACT

The screen-lock mechanisms currently distributed with touch-screen mobile devices suffer from usability issues that hinder their adoption and from security risks including smudge attacks. We present an alternative touch-based authentication method for mobile devices based on the single-dial combination lock, with the goal of reducing smudge attack risk and presenting users with a new, intuitive and appealing interaction method. The usability of this Spin interface was compared to the prevalent Android PIN and Pattern locks in a 21 participant, between-participant study using passwords of varying levels of difficulty. While the Pattern lock had the fastest unlock time, participants did not perceive differences in unlock speed between this and the slower, similar PIN and Spin locks. While the Spin lock had nearly double the error rate of the PIN and Pattern locks, participants attributed this to unfamiliarity with the interface. Despite no quantitative superiority, participants enjoyed using the Spin lock the most, suggesting that developing novel and interesting interaction methods may be a fruitful avenue to increase lock-screen adoption.

Author Keywords

lockscreens; lock; authentication; smart phone; combination lock

INTRODUCTION

Mobile devices contain an immense amount of confidential information and provide access to personal services such as banking, emailing, and social networking. Yet over 50% of smartphone users disable the lock-screen authentication mechanisms provided by manufacturers [10] due to the inconvenience associated with repeated unlocking [6]. For lock-screen users, the amount of time spent unlocking can accumulate to up to one hour per month, and less than one quarter of these unlocks are considered necessary by the user [11, 7].

Currently, popular touch-screen authentication methods include the text-based password, the PIN lock where users enter a sequence of digits, and the gesture-based Pattern lock that requires users to swipe specific patterns through a 3x3 grid of dots on the screen [1]. However, all of these lock interfaces suffer from usability issues that result in security risks even if they are adopted by users. For example, although text-based passwords provide a large space of complex passwords, these are time-consuming to input, are error-prone, and are difficult for users to memorize [12, 1, 6]. Thus, users opt to use predictable passwords, reuse passwords, or abandon them [4] entirely. Unfortunately, PIN and Pattern locks also suffer from predictable password selection [14, 3, 2], and these have significantly smaller input spaces than text-based passwords.

Another security risk associated with all of the mentioned methods, and especially the Pattern lock, comes from observational attacks. These include Shoulder Surfing [17, 6], where an attacker directly observes password entry in a public setting, and Smudge Attacks, where an attacker infers a password based solely on the oily residues or "smudge" left on the device [6]. Much research has been aimed at reducing these risks: [3] incorporates pressure input and [2] incorporates swiping gestures into PINs, while [13, 17] allows patterns to be inputted on unique images that may be transformed via rotation and shape alteration. However, the former reduces input speed and password usability, on top of requiring extra hardware [3, 2], while the latter still suffers from predictable password selection based on landmarks in the images [1].

Other active screen-lock research has moved away from touch interfaces and towards using external devices [18], biometrics [5], implicit context [9, 12, 16] or machine learning [11]. Although these designs show promising results, they are still relatively immature and unreliable [13]. In some cases, they actually reduce security in favor of usability [8, 9]. Further-

more, [11] suggests that there remains a need for explicit authentication in certain circumstances.

In this study, we propose an alternative touch-based explicit authentication method for mobile devices based on the single dial combination lock. This is inspired partially by users' affinity to the swipe-based Pattern lock for its ease of use [15], despite having slower input speeds and higher error rates than PIN passwords [16]. It is also inspired by the ubiquity and ease-of-use of the physical combination lock as well as the potential for reducing informative "smudge" residues with overlapping circular gestures. To our knowledge, no research has been performed into the usability or security of a Spin-lock based lock-screen, or the transferability of this mechanism from a physical to soft-interface. As users tend to value efficiency and satisfaction over the security provided by a lock screen [9], our goal is to explore potential improvements in usability which may lead to greater user adoption and, subsequently, better protection for the users. In order to do so, we will investigate the usability of the new Spin lock interface and compare it to the existing PIN and Pattern interfaces.

RESEARCH QUESTION AND HYPOTHESIS

To investigate the usability of our proposed spin-dial combination lock (which we will call the Spin lock from this point forward), we will compare it to the PIN and Pattern locks with respect to unlock speed, error rate, and user acceptance. Our hypotheses are as follows:

- H1: The Spin lock and Pattern lock will have similar unlock times that are significantly higher than the PIN lock, given same password complexity, due to their similarity in using gesture-based interactions.
- H2: The Spin lock and Pattern lock will have similar error rates that are significantly higher than the PIN lock, given same password complexity, due to their similarity in using gesture-based interactions.
- H3: The Spin lock will be received positively by users. However, the PIN and Pattern locks will have similar levels of user acceptance and will still be higher than the Spin lock due to users' potential familiarity with these existing methods.

We predict that the Pattern and Spin lock will be very similar with regards to speed, error rate and acceptance since they require similar gesture-based interactions to unlock the phone. However, they will be prominently superseded by the PIN lock. We hope that our users report higher user acceptance ratings to the new Spin lock interface despite its unfamiliarity.

METHODOLOGY

Apparatus

Hardware

A Nexus 5 (2013) running Android 6.0 Marshmallow served as the primary testing platform. This particular model was chosen based on hardware availability and performance characteristics required to create smooth interactions for this study. This device has a 5-inch screen (4.95 inch).

Software Interface

The software locking mechanisms were implemented as part of an Android application which guides the participant through all stages of the in-lab experiment. The application simulates lock screens onto which a user must correctly enter passwords. While the user interacts with the lock screen, usage statistics were collected in the background by the application for later analysis.

Three different lock screens were assessed in this study: the Pattern lock was developed using a library of the native Android Pattern lock, the PIN lock was developed to emulate the functionality of the Android PIN lock, and the Spin lock was developed from scratch with a custom display and custom gestural interactions. The password input method of each lock screen are briefly summarized in Table 1.

Interface	*Unlock Interaction*
PIN	Enter the numeric password using the number pad
Pattern	Swipe through a Pattern of dots in the 3 x 3 grid
Spin	Enter the numeric password by swiping in a circular gesture through the numbers to the target number, changing the direction of rotation for each digit

Table 1. Lock screen interface interaction guidelines

Participants

For this study, 21 lock-screen users were recruited as participants. While this experiment was performed on an Android device, both Android and iPhone users with a variety of lock screen preferences were included to increase the universality of this study. A breakdown of the user demographics are shown in Figure 1. No restrictions were placed on user demographics, including physical characteristics, since we expect the effect of these variables on the experiment to be insignificant and thus for the results to generalize well to the population of smart phone users at large.

Experimental design

We performed a controlled within-participant experiment, in which the primary independent variable was the lock screen interface (with three levels: PIN, Pattern and Spin locks). In order to determine the *general usability* of the interfaces, passwords of varying difficulty were tested. For each interface, 7 passwords of "easy", "medium" and "hard" difficulties were tested by each participant, for a total of 21 passwords per interface. Each password was completed 3 times, for a total of $21 \times 3 = 63$ successful trials per interface.

Password difficulty was measured based on total finger movement, considering both the number of strokes and total distance moved as shown in Table 2. Participants tested all passwords in each difficulty level in a random order, but tested the password levels in order of increasing difficulty. Given that "identical" passwords cannot be used across interfaces,

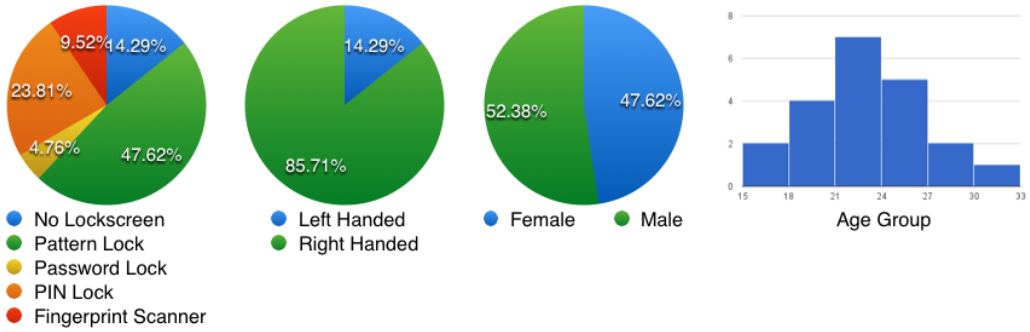

Figure 1. Participants demographics

even with careful password selection, the password remains a confounding variable. Furthermore, passwords were selected in order to provide a representative measure of the overall usability of the interface and do not necessarily conform to users' "real-life" password selection.

Complexity	*No. of Strokes*	*Distance*
Easy	2~3	7.5~8 cm
Medium	3~4	10~10.5 cm
Hard	4~5	15~15.5 cm

Table 2. Password complexity specifications

Additionally, the order in which the interfaces were tested was counterbalanced across participants using Latin squares to compensate for order effects.To compensate for potential fatigue, participants were also given 30 seconds break every 21 trials (or between each difficulty level). Lastly, in an attempt to compensate for learning effects from both the interfaces and the testing platform, participants were given a tutorial for each interface and a 5-minute period to practice unlocking with a distinct set of practice passwords.

The controlled trials in this experiment were run with identical setup, ambiance and testing procedure. Participants were also asked to perform tasks with their dominant hand only in order to reduce variance caused by input preferences.

Tasks and procedures

Step 1, Introduction: Participants were introduced to the study and given an overview of the tasks in the experiment. Emphasis was placed on performing the tasks to the best of their ability and as quickly as possible. They were also told that they must utilize their dominant hand only when unlocking the interfaces. Participants were then presented with the test phone with the test application pre-loaded , ready to start the experiment.

Step 2, Interface Demo Video: Participants were introduced to each interface through a demonstration video played by the test application explaining how to unlock the interface.

Step 3, Interface Practice Time: Participants were given up to 5 minutes to practice using the lock screen before trials began. The practice session interface was identical to test interface except that the practice passwords were a distinct set from those used in the test.

Step 4, Interface Trials: Each participant performed the unlocking task using passwords presented by the application on the lock screen. If the participant incorrectly entered a password, the application notified them of the failed attempt and asked them to enter it again. Only a successful password entry constituted a completed trial. The test interfaces are shown in Figure 2.

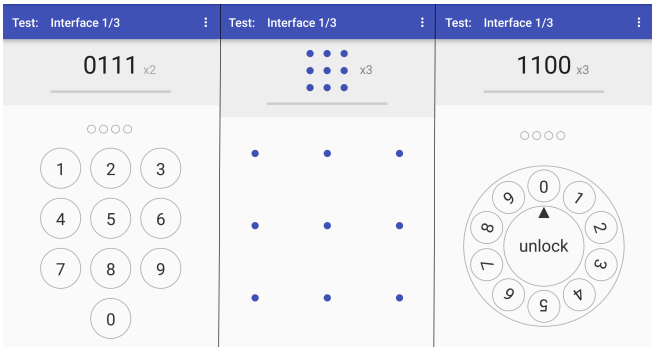

Figure 2. Test interfaces, from left to right: PIN, Pattern, Spin

After completing each difficulty level of passwords on a given interface, the participants were given a 30 second break.

Step 5, Repeat: Steps 2-4 were repeated for the subsequent two interfaces.

Step 6, Post-experiment: After the participants had completed the experiment, they filled out the Post Study Questionnaire about their experience with the various interfaces. The survey collected the users' subjective evaluation of the usability of the interfaces and users' willingness to adopt them on their personal devices. Additional comments were also collected.

Measures

The following dependent variables measured during this experiment were selected in order to evaluate the usability of the three locking interfaces:

1) Unlock Speed: Unlock speed (equivalently, password entry time) was measured for each trial and compared across interfaces. Entry time was only measured for successful password entries; unsuccessful trials were accounted for through error rate calculations. The unlock speed was measured from the moment that the participant touched the screen to begin password entry to the moment that a successful password entry had been completed.

2) Error Rate: Error rate is measured as the ratio of the number of failed attempts to the total number of attempts. Each password entry attempt was identified as either a success or failure. Thus, while a given password is used for three trials, it may be entered in more than three password attempts. Per trial error rate is taken as the percentage of failed attempts per trial.

3) Acceptance/Perception: Error rate and unlock speed, as demonstrated by users' preference of the Pattern lock over the PIN [15, 16], are not sufficient to determine whether an interface is deemed highly "usable" and preferred by users. Thus, we used qualitative measures to ascertain user acceptance. To measure user acceptance, participants answered questions regarding perceptions of speed, ease of use, likelihood of adoption, and feedback of the interfaces. These questions were created using the 7-point scale NASA-TLX format. Users were also asked to reflect on difficulties they encountered during the experiment and record their reflections in a free-form manner. During the experimental trials, the experimenter also noted any interesting behavior or comments of the participants.

Data collection

Data were collected through two methods: quantitative data on unlock speed and error rate was collected by the testing application, and qualitative data on user's subjective opinion was collected using questionnaires.

RESULTS

Unlock Speed

Average unlock times of successful attempts for each interface are provided in Figure 3. Significant differences were observed between unlock times (Anova: $F_2 = 186.64$, $p < 0.001$), with a Tukey-Kramer post-hoc test indicating that the Pattern lock was significantly faster than the Spin and PIN locks ($p(PIN, Pattern) < 0.001$, $p(Spin, Pattern) < 0.001$), but no significant difference was observed between the Spin and PIN locks (with $p > 0.1$).

Differences across participants

The average unlock times of participants were significantly different, even averaged across all interfaces. Thus, users were subsequently grouped into "slow" and "fast" categories using standard 2 group k-means clustering. For "fast" users, again only the Pattern interface was observed to be significantly faster than the PIN and Spin interfaces. However, for "slow" users, significant differences were observed between all interface unlock speeds, with the Spin lock being slower than the PIN lock.

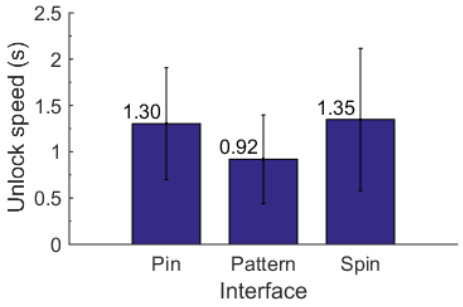

Figure 3. Average unlock time across interfaces

Differences between password difficulties

Statistically significant differences were observed in the average unlock times of the various password difficulty levels, even averaged across all interfaces (Anova: $F_2 = 503.01$, $p < 0.001$), with average unlock times increasing with password difficulty. Examining attempts from each password level independently, the results differ somewhat from those reported above. These are shown in Figure 4. For medium passwords, again the Pattern interface was significantly faster, with no significant difference between Spin and PIN interfaces. However, for Easy passwords, the Spin was significantly slower than the PIN. For Hard passwords, the PIN was significantly slower than the Spin.

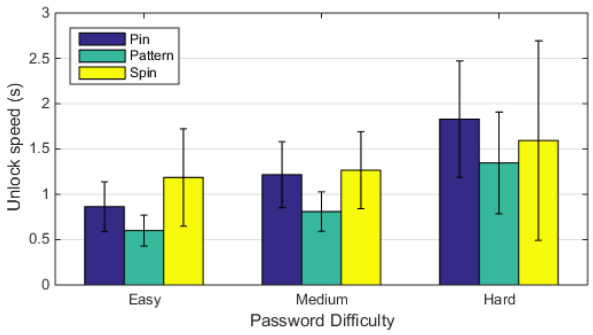

Figure 4. Average unlock time across interfaces, across different password difficulty levels

Differences across interface orders (counterbalancing)

Participants who tested the Pattern interface first were, averaged across all three interfaces, significantly slowest (Anova: $F_2 = 33.47$, $p < 0.001$). Pattern-first participants were significantly slower than PIN-first participants on all three interfaces. They were also significantly slower than Spin-first users on all but the PIN interface. Average speeds for the three user groups across interfaces are provided in Figure 5.

Learning effect for entering new password

The learning effect is observed in unlock speeds between the 1st, 2nd, and 3rd trials on each given password, averaged across passwords and interfaces. For each interface, statistically significant differences are observed across trials, with the 1st trial being slowest for all interfaces ($F_2 = 28.24$,

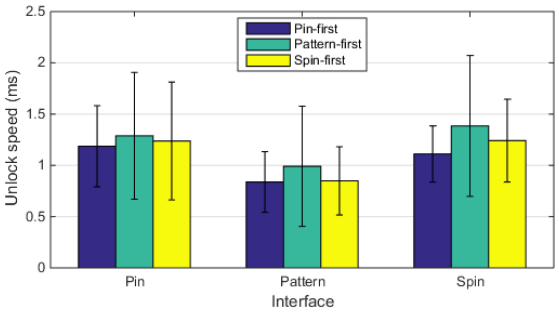

Figure 5. Average unlock time across interfaces, across different interface-first user groups

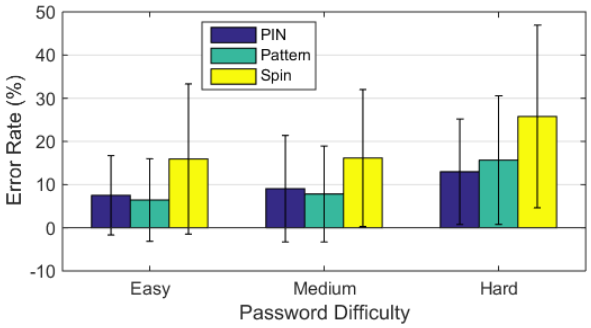

Figure 7. Average unlock error rate across interfaces

$p < 0.05$). However, even with the learning effect minimized by only considering the 3rd trials, the average unlock speeds of all interfaces were still statistically significant ($F_2 = 18.84$, $p < 0.05$) and align with the overall unlock speed results.

Error Rate

Significant differences exist in error rates for each interface, averaged across all trials (Anova: $F_2 = 19.78.84$, $p < 0.01$), as shown in Figure 6. The Spin lock had a significantly higher error rate, validated by a Tukey-Kramer post-hoc test ($p(PIN, Pattern) < 0.01$, $p(S\,pin, Pattern) < 0.01$), but no significant difference was observed between PIN and Pattern locks ($p(S\,pin, Pattern) > 0.5$).

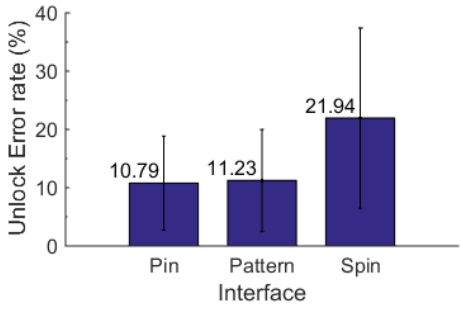

Figure 6. Average unlock error rate across interfaces

Differences across participants

No significant differences were observed in the average unlock error rates for all interfaces across participants. Grouping participants into "error prone" and "not error prone" categories using standard 2 group k-means clustering produced similar results to those for all participants.

Differences between password difficulties

Examining each password level independently, the results confirm those reported above: considering easy, medium and hard passwords separately, no statistical difference was observed between PIN and Pattern error rates, while the Spin interface was consistently more error-producing. Average error rates for each difficulty level are provided in Figure 7. As expected, hard passwords have a significantly higher error rate, but no significant difference was observed between medium and easy passwords, averaged across interfaces.

Differences across interface orders (counterbalancing)

For participants who tested the Pattern and Spin interfaces first, the Spin lock was again observed to have a significantly higher error rate than either the Pattern or PIN interfaces. However, for users who tested the PIN first, while error rates for the Spin lock were significantly higher than for the PIN, they were not significantly higher than for the Pattern lock.

User Acceptance

Figure 8 shows the average Post-Experiment survey responses for each interface using NASA-TLX. The Friedman Test was used to assess the participants' responses. Differences between average responses on quickness of password entry, clarity of input feedback and willingness to adopt the interface are shown to be insignificant. However, significant results have been reported for two categories: ease of use and input accuracy.

There is a significant difference in ease of use between the three interfaces ($\chi^2 = 13.774$, df = 2, $p_{PIN,\,PATTERN,\,S\,PIN} = 0.001 < 0.05$). Furthermore, the Friedman test indicated that users felt the Spin lock interface was significantly easier to use compared to the PIN lock ($p_{S\,PIN,\,PIN}$ using Conover's F, $df = 1 > 0.450$). Moreover, the Pattern Lock interface was found to be significantly easier to use than the PIN ($p_{Pattern,\,PIN} > 0.450$).

Regarding input accuracy, there is a significant difference between the three interfaces ($\chi^2 = 5.792$, df = 2,

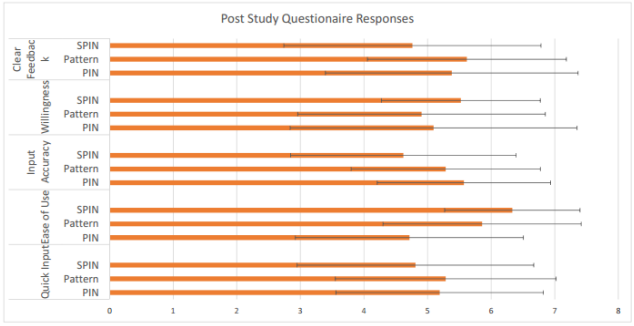

Figure 8. Questionaire Responses on User Acceptance : Bar Graphs represent the average responses , Error Bars represent Standard Deviation

$p_{PIN,PATTERN,SPIN} < 0.01$). A post-hoc multiple comparisons test identified that users felt the PIN lock provided significantly higher input accuracy than the Spin lock ($p_{PIN,SPIN}$ using Conover's $F, df = 1 > 0.449$). Users have also reported, in the free-form feedback section, that accurate password entry is much easier using the PIN lock than the Spin interface.

DISCUSSION

The results presented above run counter to our hypotheses regarding unlock speed, error rate, and user acceptance. A summary of these results is presented in Table 3 and is discussed in depth below. In short, the newly designed Spin lock did not surpass the performance of either the existing PIN or Pattern locks on Android in terms of speed or error rate. However, speed and error rates are not directly comparable, and users enjoyed interacting with the Spin lock more than the existing PIN and Pattern locks. Overall, the Spin lock was surprisingly well received by the participants.

	Predicted	*Result*
H1	Spin lock and Pattern lock have similar unlock speed Spin lock and Pattern lock are slower than PIN lock	Spin lock and PIN lock have similar unlock speed Pattern lock is fast than Spin lock and PIN lock
H2	Higher error rates: Spin and Pattern lock Lowest error rate: PIN lock	Highest error rate: Spin lock Lower and similar error rates: PIN and Pattern lock
H3	Spin lock have lowest acceptance	Spin lock have highest acceptance

Table 3. Hypotheses and results

Unlock Speed

The Pattern lock had, on average, a significantly faster unlock time than the PIN and Spin locks. This contradicts the results from [16], which reports an average PIN unlock time of 1.501 s and Pattern unlock time of 3.136 s. This Pattern unlock time is over twice as slow as the average times we observed for both Hard Pattern passwords and for slow users, while the PIN time is approximately twice as slow as for Easy passwords, but similar to those of Hard passwords and slow users. This disparity is likely due to differences in the complexity of the passwords tested in the two studies. [16] used only one level of difficulty, with all PIN passwords consisting of four digits and all Pattern passwords being five-stroke patterns on a 3x3 grid, which were directly compared. However, our finger-movement based password comparison would results in a four digit PIN being categorized as an easy password, while a five-stroke Pattern would be categorized as hard. Given that the average unlock times *across all interfaces* increased with password complexity in our study, we believe that our results regarding Pattern and PIN speeds are more representative of the actual unlock speeds of the interfaces.

Another possible reason for the disparity is the inclusion of an "undo" button in the PIN lock in [16]'s design. Thus, users were able to "fix" mistakes in a PIN unlock trial, but not in a Pattern trial. Our design did not provide undo options for any of the interfaces. However, we also did not include unsuccessful attempts in the calculations of unlock speed. Thus, one might expect higher PIN unlock times in [16]'s study, since "undo"s might lengthen trial time, but this is not the case. Additionally, the lack of an undo button may have caused some confusion since it is incorporated in the stock Android PIN lock; one user commented that they required the back-space button.

While the Pattern lock was also significantly faster than the Spin lock, the PIN lock was *not* significantly faster. This is surprising given that the Spin lock is a new interface for all users (whereas many have used the PIN and Pattern interfaces in the past), and would be expected to have higher unlock times. Multiple users acknowledged this need for more time to adjust to the Spin interface, but also that it was the "fastest [and] most enjoyable" after they began to master it. This suggests that the Spin interface speed could surpass the traditional PIN and perhaps approach the Pattern speeds given further practice.

Furthermore, while for Hard and Easy passwords a significant difference was observed between Spin and PIN passwords, this was not the case for Medium passwords. Given that users were presented Easy trials first, they might not have yet adjusted to the interface, and thus the disparity may only exist between PIN and Spin for Easy passwords due to learning effects.

Error Rate

Again, contrary to the results in [16], where PIN was observed to have a significantly lower error rate (5%) than Pattern (16%), we observed no significant difference in error rates between the two (~11%), regardless of password difficulty or users being "error-prone" or not "error-prone". As mentioned in , this may again be due to the complexity of passwords tested in our study and our attempt to make them comparable across interfaces.

We found the Spin lock to have a significantly higher error rate of 21.9% which was nearly double the error rate of the PIN and Pattern locks, and in line with our hypothesis that it would be higher than the PIN lock. However, we cannot discount the possibility that this is due to the novelty of the interface for participants. Although participants were given 5 minutes to practice beforehand, most users did not use the entire time which may have been insufficient to familiarize themselves with the interface. Future experiments could be improved by enforcing longer practice sessions and a "test" to ensure competence.

Our hypothesis that the Pattern and Spin locks would have similar error rates was also disproved. Yet, unlike [16], the gesture-based Pattern lock did not have significantly higher error rates than the PIN interface. This may suggest that gesture-based input does not lead to higher error-rates, and that the higher error rates for the Spin interface are a result of unfamiliarity, which would be expected to decline with practice.

User Acceptance

Although the quantitative data on unlock speed and error rate indicated that participants generally perform better with Pattern or PIN locks, our survey results showed that performance does not translate into user acceptance. Based on the Post-Experiment survey, participants made no distinction between the three interfaces in terms of input-speed and input feedback and did not differ in willingness to adopt the three interface. However, users did feel that input with PIN lock was more accurate than the Spin lock, which aligned with the quantitative error rate results. Interestingly, despite the error rate of the Spin lock being almost twice as high as that of the Pattern lock, participants felt these two lock screens had similar unlock accuracies. This could be due to users perceiving these gesture-based interactions in the same way. On the other hand, participants did acknowledge that the Spin lock was more error prone than the PIN lock. Yet despite this, they still liked the interface and enjoyed interacting with it. One user even explicitly identified the Spin lock to be the most usable of the interfaces.

Multiple users reported that they believed their performance on the Spin lock would have improved with more practice using it. We cannot discount the impact of practice and familiarity on users' preferences and performance in this study. The Pattern lock, for example, had the fastest unlock speed, lower error rate and also high user acceptance scores. This might be a consequence of familiarity: according to the participant acquisition questionnaire, 47.62% of the participants used the Pattern lock screen regularly (compared to only 23.81% who used PIN locks). The lack of familiarity and feeling of requiring further adjustment-time to the Spin lock, may be the reason that users did not express a clear preference for adopting the new Spin interface, even though they rated it to be significantly more usable than the Pattern lock.

Conclusion

In this study, we designed a new lock screen interface, inspired by the physical combinational lock, and compared it to the existing Android PIN and Pattern locks. Since this new interface requires complex and novel interactions, it was no surprise that it did not surpass existing commercial lock-screen unlock times and produced higher error rates. The high error rates may be a result of unusual circular gestures required to spin the virtual dial, which are less common than straight-line strokes and swipes. With further exposure to the interface, error rates would likely improve. However, even with such little exposure, the Spin interface had comparable unlock speeds to the standard PIN lock. Furthermore, survey results suggest that participants actually find the Spin and Pattern locks easier to user than the PIN lock. This may be due to the interesting and intuitive interactions of the Spin and Pattern locks.

Due to the scope of the study, our participant pool was limited to university students and the results may not generalize well to other populations. Furthermore, due to the availability of our participants, each trial was limited to 15 to 20 minutes, and some participants could not adjust to the new interface over that period of time: their first exposure to it was during the experiment, with only 5 minutes of practice time.

Another limitation of this research is the selection of tested passwords. There is little existing literature on creating comparable passwords across different interfaces, which is necessary to compare their usability. Further research is required to validate our method of determining password complexity. Furthermore, the selected passwords may not be representative of passwords that will be actually selected by users. Further studies are required into the performance and security of the Spin interface for user-selected passwords, as compared to the PIN and Pattern interfaces, given the differences in unlock speeds across different password complexities. Other research directions include utilizing Fitts's law as a measure of human performance, and also studying the security aspect of the Spin lock with respect to shoulder surfing and smudge attacks

Overall, we were able to demonstrate that the alternative Spin lock created in this study achieves great user acceptance, despite having more more complicated interactions. We expect the Spin lock to deliver same or higher performance compared to the PIN lock in real-world use where the user will have fully acclimatized to the interface. Further work on the Spin lock could provide improvements in lock-screen security and user experience, which could be easily passed on to mobile device users.

REFERENCES

1. Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, and Can Yildiz. 2013. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, 1–6. http://dl.acm.org/citation.cfm?id=2462098

2. Ahmed Arif, Michel Pahud, Ken Hinckley, and WIlliam Buxton. 2013. A Tap and Gesture Hybrid Method for Authenticating Smartphone Users. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '13)*. ACM, New York, NY, USA, 486–491. DOI:http://dx.doi.org/10.1145/2493190.2494435

3. Ahmed Sabbir Arif, Ali Mazalek, and Wolfgang Stuerzlinger. 2014. The Use of Pseudo Pressure in Authenticating Smartphone Users. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MOBIQUITOUS '14)*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 151–160. DOI:http://dx.doi.org/10.4108/icst.mobiquitous.2014.257919

4. Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. 2012. Graphical passwords: Learning from the first twelve years. *Comput. Surveys* 44, 4 (Aug. 2012), 1–41. DOI:http://dx.doi.org/10.1145/2333112.2333114

5. N.L. Clarke and S.M. Furnell. 2007. Advanced user authentication for mobile devices. *Computers &*

Security 26, 2 (March 2007), 109–119. DOI: http://dx.doi.org/10.1016/j.cose.2006.08.008

6. Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are You Ready to Lock?. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*. ACM, New York, NY, USA, 750–761. DOI: http://dx.doi.org/10.1145/2660267.2660273

7. Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. Itsa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *Symposium on Usable Privacy and Security (SOUPS)*. https://www.usenix.org/system/files/conference/soups2014/soups14-paper-harbach.pdf

8. Hassan Khan, Aaron Atwater, and Urs Hengartner. 2014. Itus: An Implicit Authentication Framework for Android. In *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (MobiCom '14)*. ACM, New York, NY, USA, 507–518. DOI: http://dx.doi.org/10.1145/2639108.2639141

9. Nicholas Micallef, Mike Just, Lynne Baillie, Martin Halvey, and Hilmi Gne Kayacik. 2015. Why Aren'T Users Using Protection? Investigating the Usability of Smartphone Locking. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 284–294. DOI: http://dx.doi.org/10.1145/2785830.2785835

10. Consumer Reports. 2014. Smart phone thefts rose to 3.1 million in 2013 Industry solution falls short, while legislative efforts to curb theft continue. (May 2014). http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

11. Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos. 2012. Progressive Authentication: Deciding When to Authenticate on Mobile Phones.. In *USENIX Security Symposium*. 301–316. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final154.pdf

12. Roland Schlglhofer and Johannes Sametinger. 2012. Secure and Usable Authentication on Mobile Devices. In *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia (MoMM '12)*. ACM, New York, NY, USA, 257–262. DOI: http://dx.doi.org/10.1145/2428955.2429004

13. Stefan Schneegass, Frank Steimle, Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2014. SmudgeSafe: Geometric Image Transformations for Smudge-resistant User Authentication. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. ACM, New York, NY, USA, 775–786. DOI: http://dx.doi.org/10.1145/2632048.2636090

14. Sebastian Uellenbeck, Markus Drmuth, Christopher Wolf, and Thorsten Holz. 2013. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13)*. ACM, New York, NY, USA, 161–172. DOI: http://dx.doi.org/10.1145/2508859.2516700

15. Dirk Van Bruggen, Shu Liu, Mitch Kajzer, Aaron Striegel, Charles R. Crowell, and John D'Arcy. 2013. Modifying Smartphone User Locking Behavior. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, New York, NY, USA, 10:1–10:14. DOI: http://dx.doi.org/10.1145/2501604.2501614

16. Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. ACM Press, 261. DOI: http://dx.doi.org/10.1145/2493190.2493231

17. Emanuel Von Zezschwitz, Anton Koslow, Alexander De Luca, and Heinrich Hussmann. 2013. Making graphic-based authentication secure against smudge attacks. In *Proceedings of the 2013 international conference on Intelligent user interfaces*. ACM, 277–286. http://dl.acm.org/citation.cfm?id=2449432

18. Christian Winkler, Jan Gugenheimer, Alexander De Luca, Gabriel Haas, Philipp Speidel, David Dobbelstein, and Enrico Rukzio. 2015. Glass Unlock: Enhancing Security of Smartphone Unlocking Through Leveraging a Private Near-eye Display. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1407–1410. DOI: http://dx.doi.org/10.1145/2702123.2702316