May the Force be with You: The Future of Force-Sensitive Authentication

Katharina Krombholz, *Ruhr University Bochum and SBA Research*, Thomas Hupperich, *Ruhr University Bochum*, and Thorsten Holz, *Ruhr University Bochum*

***Abstract*—Modern smartphones provide a rich set of possible touchscreen interactions, but most authentication schemes still rely on simple digit or character input. Previous studies examined the shortcomings of such schemes e.g., digit-PINs.**

In this paper, we discuss the potential of a new PIN type called *force-PINs* [1]. The idea behind this approach is to augment the security of digit PINs by assigning a binary pressure value to each digit in the sequence. By adding this (practically) invisible pressure component, force-PINs help users to select stronger PINs that are harder to observe for a shoulder surfer. We also discuss implications for future research on force-sensitive authentication.

***Index Terms*—Usable Security, Authentication**

I. Introduction

With the introduction of pressure-sensitive touchscreens, new kinds of user interaction for smartphones become possible that could also be used to enhance existing authentication schemes. The scientific community has already examined the shortcomings of unlock patterns, PINs and passcodes [2]–[5] and presented alternative authentication schemes.

However, none of the proposed systems has shown to be capable of replacing passcodes and unlock patterns as means of authentication. On the one hand, many approaches, e.g., [6] rely on customized hardware that is not available off the shelf and thus makes large-scale deployment infeasible. As shown by Harbach et al. [2] in a field study on smartphone unlocking behavior, (un-)locking smartphones produces a significant task overhead. This highlights the need for novel authentication methods that perform equally fast as or even faster than currently deployed systems in terms of authentication speed.

Recently, biometric approaches such as fingerprint sensors have found their way into the mobile ecosystem. However, they still require PINs for fallback authentication. Fingerprint sensors have also shown to be easy to break by attackers [7] and difficult to use for people with weak fingerprints (e.g., due to manual labor).

In this paper, we summarize our research on *force-PINs*. This PIN scheme enhances digit-only PINs with tactile features using pressure-sensitive touchscreens as found in modern consumer hardware. Figure 1 provides an overview of the proposed scheme. In theory, force-PINs offer the benefit of a larger PIN space by design and are more difficult for an attacker to guess due to the additional invisible pressure component. In this paper, we summarize the findings from a comparative, repeated-measures lab study with 50 participants and a field study with 10 participants to evaluate the usability and security of force-PINs. Our findings suggest that force-PINs are more secure than digit-only PINs with only a minimal impact on usability. Based on the results from our studies, we discuss lessons learned and implications for future research in the field of force-sensitive authentication.

II. Force-PINs

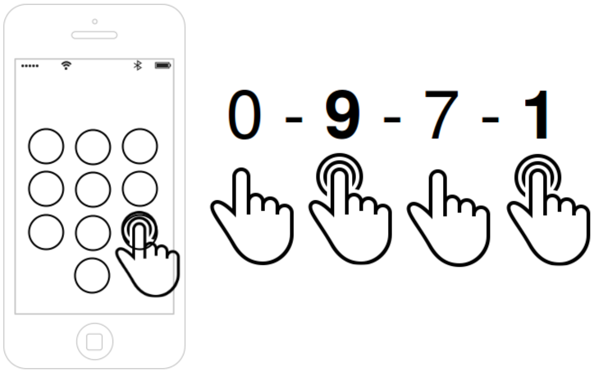

Fig. 1: Schematic overview of force-PINs: digits can either be entered with shallow or deep pressure (with vibration feedback) on a pressure-sensitive touchscreen.

Force-PINs are designed to provide a larger PIN space by design and to be more resistant to observation. To authenticate the user enters a digit either with shallow or deep pressure on a pressure-sensitive touchscreen. The user receives tactile feedback when entering a digit with deep force. The tactile component and vibration feedback may implicitly help users to memorize force-PINs [8].

An example force-PIN could be 0-**9**-7-**1** where bold and underlined numbers should be pressed more deeply than others on a pressure-sensitive touchscreen. The design is not only simple, it is also cheap and easy to deploy as it relies on off-the-shelf hardware. We expect that users who are already using pressure-sensitive touchscreens will find force-PINs easy to learn as they are based on interactions they are already familiar with. For our user study, we implemented a prototype app for iPhones with touch-sensitive screens. The app lets users set a force-PIN and presents a lock screen that looks just like a common lock screen from an off-the-shelf iPhone.

The design decision was based on a small pre-study with 9 participants where we evaluated subjective perceptions on different types of pressure encodings. We evaluated both relative and absolute differences in pressure with different thresholds, respectively. As two-stage pressure with a constant threshold for shallow and deep press performed best we implemented the prototype app accordingly. We also tested different thresholds and to our surprise it was often not easy to distinguish which threshold was higher and which one was lower. Therefore, we then set the threshold for deep pressure to 50% or more of the maximum possible pressure supported by the hardware.

III. Evaluation

We summarize the results from two studies presented in [1], namely a lab study with 50 participants and a field study with 10 participants. The lab study had a within-subjects design where each participant was exposed to the following conditions in random order: (C1) four-digit standard PINs, (C2) six-digit standard PINs, and, (C3) four-digit force-PINs. Each participant entered every PIN type three times in a row in a dedicated lab study app before proceeding to the next condition. We collected the duration of each successful authentication session i.e., the time between the first and last touch of the authentication session as defined by [6]. A successful authentication session can consist of up to three attempts to enter a PIN correctly. We consider erroneous attempts within a successful authentication session as *basic errors*. We also collected the number of failed authentication sessions i.e., authentication sessions that consisted of more than two basic errors and refer to those as *critical errors*. We used the collected PINs from the lab study for an entropy estimation and conducted basic shoulder surfing experiments. Additionally, we conducted a small field study with 10 participants to show that authentication time and error rate decrease over training. For our field study, we modified the app from our field study and deployed it on the participants' iPhones. We were not able to replace the actual PIN scheme on their phones due to the restrictions in iOS. The app issued a single daily notification to remind the participants of the study task. After the study task, the participants from the lab study completed a questionnaire and those from the field study completed debriefing interviews.

A. Usability Metrics

Regarding authentication time, four-digit standard PINs performed best with a mean of 2.34 compared to six-digit (mean = 3.33) and force-PINs (mean = 3.66) in our lab study. A one-way repeated-measures ANOVA followed by pairwise t-tests revealed that except for the difference between six-digit and force-PINs all differences in authentication speed were statistically significant.

TABLE I: Mean authentication time in seconds and error rate with different levels of the independent variables.

Authentication Speed	**Mean**	**SD**
4-digit	2.34	1.21
6-digit	3.33	1.56
Force (Lab Study)	3.66	1.96
Force (Field Study)	2.69	0.59

The number of basic errors was very similar for digit-only PINs (21 with four and 22 with six digit standard PINs). In contrast, 36 failed attempts were registered with force-PINs. Given that most of the participants have not been exposed to pressure-sensitive screens before, the number is rather low compared to the error rates registered with digit-only PINs. All critical errors (4) were registered with force-PINs. The results of our field study suggest that users of force-PINs improve over training and that both the number of errors and authentication time converge towards the metrics of four-digit standard PINs. Figure 2 provides a comparison of the average authentication time measured in the course of the field study grouped by 50 successful authentication sessions based on the median authentication time per participant. These results suggest a habituation to our mechanism and time decreases with training. As shown in [1], also the error rate decreases with training.

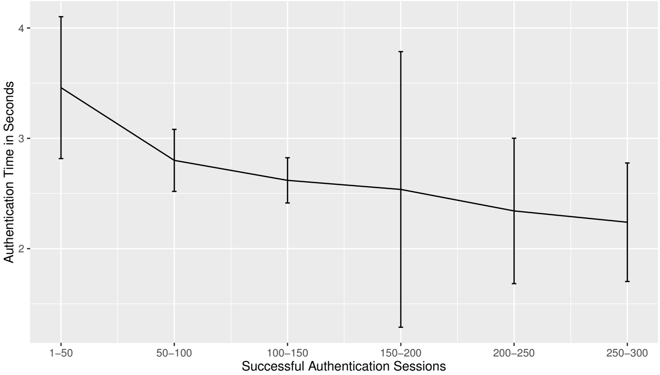

Fig. 2: Authentication time development based on the first 300 successful authentication sessions across all participants.

The post-lab study questionnaire revealed that 91 % of our participants thought that four-digit PINs were the least secure of the three tested PIN types. 95 % also thought that four-digit PINs were the fastest PIN type to enter and 80 % thought that they were the easiest to remember. 62 % thought that force-PINs were the most secure of the three methods but 55 % also thought that this was the most time-consuming PIN type to enter. In comparison, only 31 % thought that six-digit PINs were the most secure but 75 % also thought that they were the hardest to remember.

B. Force Pressure

Due to the low experience with pressure-sensitive screens, they could not easily distinguish different thresholds to separate deep and shallow press. The app also provided vibration feedback as soon as the user entered a digit with force. Through our lab study, we collected the exact values of the force registered by the device and then used it to evaluate how close or far the registered force was from the threshold and the upper and lower boundaries. Figure 3 shows the force intensities of all logged force-PIN digits during the lab study in percent of the maximum possible force.

C. Security

To estimate the security benefit of force-PINs, we performed entropy calculations. Table II summarizes our calculations of zero-order entropy and practical entropy based on collected

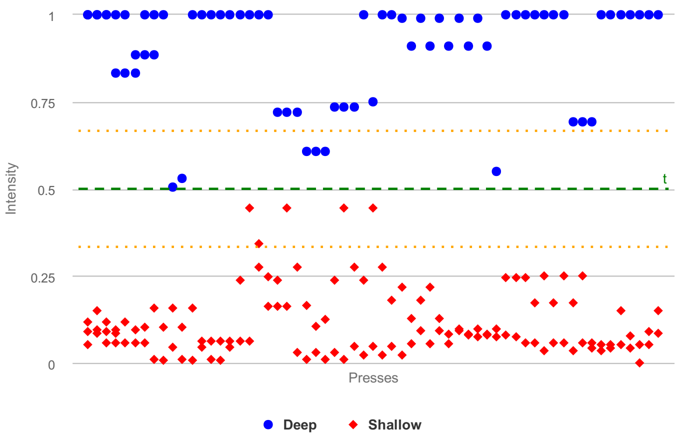

Fig. 3: Measured force relative to the maximum possible force. The green line at y = 0.5 represents the threshold for distinguishing between deep and shallow presses. The grey lines at 0.25 and 0.75 indicate two potential thresholds for a three-step force scale (e.g., *shallow-medium-deep*.)

data. Zero-order entropy is measured in bits and calculated as $L * \log_2 N$, where L is the length of the secret and N the size of the character set. In theory, if force patterns were evenly distributed, the theoretical entropy gain would be 4 bits. We calculate the practical entropy gain as $-\sum_{i=1}^{n} p_i * log_2(p_i)$ where p_i is the probability of a certain pattern occurring. Our calculations were based on a dataset of 56 user-chosen binary force patterns that were collected during the lab study (some participants renewed their PINs during the study). The collected force-PINs are not evenly distributed across the PIN space and the most popular position for a digit with deep press (**D**SSS) was the first with a probability of 14%. This indicates that the practical entropy is lower than the theoretical entropy. Symmetric patterns (**D**SS**D**, S**DD**S) occured with a probability of 19,2% which is slightly higher than in theory (13,3%). According to [9], the practical entropy of 4-digit PINs is estimated as 11.42. According to our collected user-chosen force patterns, an additional binary force-pattern of length 4 would result in an entropy gain of 23%.

TABLE II: Comparison of entropy.

	Combinations	Theoretical Entropy	Practical Entropy
4-digit	10^4	13.28 bit	11.42 bit [9]
6-digit	10^6	19.93 bit	-
Force	$20^4[-10^4]$	17.28 bit	14.83 bit

Regarding shoulder-surfing resistance, we conducted two basic experiments and found that force-PINs are more difficult to observe for an attacker than digit-only PINs. During the lab study, an experimenter tried to guess the force-PINs based on the least entered digit sequence per user and was only able to partially guess 21 force-PINs. In a camera-based experiment, two attackers managed to correctly guess 39 of the 50 shown digit sequences.

IV. Implications for Future Research and Design

We discuss the main lessons learned from our user studies and give suggestions for future work.

A. Three-Step Force

During our lab experiments, we measured the exact pressure intensities of the entered digits with either shallow or deep press. For our initial force-PIN implementation, we opted for a two-step scale based on the results from a pre-study which suggested that people who had never used 3D Touch before could not easily distinguish different thresholds to separate deep and shallow press. We found that most collected pressure intensities were rather close to the upper and lower boundaries. These results imply that a three-step force scale (e.g., shallow-medium-deep) is theoretically possible. While the security benefits of such an augmented pressure scale are obvious, it remains to study the implications on the user experience. A three-step scale is potentially harder to remember and more difficult to enter for inexperienced users. We propose to examine the feasibility of three-step force-PINs in the course of a longitudinal field study with users that have previously been exposed to pressure-sensitive touchscreens, and, ideally have been using two-step force-PINs before. Furthermore, we suggest to research whether ideal pressure thresholds should be customizable, i. e., whether user chosen thresholds vary across a larger user base or converge towards mathematically selected thresholds.

B. Memorability

The results from our post lab study survey suggest that users perceive four-digit force-PINs more memorable than six-digit standard PINs. The findings from our field study also support this statement as only two participants renewed their force-PINs throughout the study period. However, our field study does not provide long-term insights regarding force-PIN usability and was completed within a couple of days by most participants. It therefore remains to show that an additional force patterns is indeed easier to remember than additional digits. It also remains to show whether overall memorability of force-PINs is dominated by muscle memory instead of visual memory. Such a findings would support the potential of force- and other tactile components for user authentication.

C. Unlock Patterns

Our studies only considered force components in combination with digit-based authentication on iPhones. The ability to recognize pressure-sensitive input however has already been introduced in Android 1.0 and more and more Android devices come with compatible hardware (e. g., Nexus N, Huawai Mate S). Therefore, a natural idea is to integrate the feature in unlock patterns. As the interaction with unlock patterns is based on swipe gestures instead of touch, the pressure component can be applied in multiple ways. Similar to digit PINs, the single points from an unlock pattern can be assigned (binary) pressure values. Furthermore, force-gradients could be assigned to connections between points. As future work, we propose to implement force unlock patterns and conduct similar user studies to those from [1].

D. Force-Based Implicit Authentication

A new trending topic in authentication research is implicit authentication (IA). Many approaches have been proposed in scientific literature but to date none has been adopted on a large-scale in practice. As shown by Khan et al. [10], current methods for implicit authentication are not capable of replacing knowledge-based authentication because their real-world accuracy is significantly lower than in lab settings. Furthermore, they require a certain number of interactions to classify a user correctly. Therefore, these systems are often perceived as disruptive in cases where authentication fails and fallback authentication methods come into play. Buschek et al. [11] studied the feasibility of mobile keystroke biometrics and found that they can be used for user authentication with relatively low error rates. These findings highlight that typing behavior can be used to authenticate individuals. As future work, we suggest to examine whether force-patterns can be used to classify users. If the latter was true, individual pressure characteristics could be used as an additional security layer and implicit authentication method in addition to PIN or unlock pattern entry. We argue that this secondary channel could strengthen knowledge-based authentication and should not be used to replace it.

E. Attack Scenarios

The security evaluation presented in [1] suggests that force-PINs have higher entropy than digit-only PINs and provides a first look at shoulder surfing resistance. Due to several limitations, further investigation is needed to determine a lower bound for shoulder surfing resistance. We propose to alter the study design from [1] by a larger number of shoulder-surfers. To determine a reasonable lower bound, the attacker should be an experienced user of force-PINs and maybe even an experienced hacker. Furthermore, the attacking participant should be given an incentive to break the system similar to the reward in a real-world scenario. A pre-study with a non-tech savvy participant who had not yet used force-PINs before but full control of the video material resulted in 44 out of 50 guessed digit sequences and 11 completely guessed force PINs. Harbach et al. [2] argue that shoulder surfers in a private environment might anyway know the digits of a PIN. Force-PINs do not sufficiently address this threat scenario, as a social insider has the opportunity to observe the victim's PIN entry multiple times. Furthermore, if the digits are already known to the attacker, it is rather easy to guess the associated force pattern, especially if the distribution of selected force patterns is already known. Hence, force-PINs do not offer sufficient protection from social insiders. Furthermore, it remains to show whether force-PINs are resilient to smudge attacks [4].

F. Accessibility

The participants from our studies were recruited around the university campus. Therefore, the level of education was higher than expected from the general population. Hence, our results cannot be generalized to smartphone users with different demographics. We did not collect evidence on how elderly persons or people with disabilities interact with force-sensitive screens. Furthermore, it remains to show how error-resistant force-PINs are when entered under environmental constraints, e.g. while riding a moving train or multi-tasking. Such situational disabilities may impact the user experience with force-PINs as users are dependent on the subtle haptic feedback when digits are entered with force. We therefore argue that an extensive field study should be conducted with marginalized groups.

G. Beyond Smartphones

Four-digit PINs cannot only be found in smartphones but also on other devices such as ATMs where security is crucial. Various attacks for stealing ATM PINs have been presented in online media. We therefore argue that it is worth considering force-PINs as an enhancement to standard ATM and credit card PINs. A basic requirement for the large-scale deployment of such a pressure-sensitive PIN pad however is accessibility for a broad range of users.

V. Conclusion

In this paper, we discussed future research and design directions for force-sensitive authentication. We summarized the findings from two user studies to evaluate our recently proposed scheme which we refer to as force-PINs. While the results from our studies revealed that force-PINs have the potential to make PIN-based authentication more secure with a minimal impact on usability many other aspects still remain to be researched before the system can find its way into consumer applications. In order to motivate further research around our approach, we presented research and design challenges and ideas for future research.

References

[1] K. Krombholz, T. Hupperich, and T. Holz, "Use the force: Evaluating force-sensitive authentication for mobile devices," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016.

[2] Harbach, Marian and von Zezschwitz, Emanuel and Fichtner, Andreas and De Luca, Alexander and Smith, Matthew, "It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[3] De Luca, Alexander and Lindqvist, Janne, "Is Secure and Usable Smartphone Authentication Asking Too Much?" *Computer*, vol. 48, no. 5, pp. 64–68, 2015.

[4] Aviv, Adam J and Gibson, Katherine and Mossop, Evan and Blaze, Matt and Smith, Jonathan M, "Smudge Attacks on Smartphone Touch Screens." *WOOT*, vol. 10, pp. 1–7, 2010.

[5] Song, Youngbae and Cho, Geumhwan and Oh, Seongyeol and Kim, Hyoungshick and Huh, Jun Ho, "On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 2343–2352.

[6] De Luca, Alexander and Harbach, Marian and von Zezschwitz, Emanuel and Maurer, Max-Emanuel and Slawik, Bernhard Ewald and Hussmann, Heinrich and Smith, Matthew, "Now you see me, now you don't: protecting smartphone authentication from shoulder surfers," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2937–2946.

[7] Chaos Computer Club, "Chaos Computer Club breaks Apple TouchID," http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid, last accessed 11/11/2015.

[8] A. Bragdon, E. Nelson, Y. Li, and K. Hinckley, "Experimental analysis of touch-screen gesture designs in mobile environments," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 403–412.

[9] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? the security of customer-chosen banking pins," in *Financial Cryptography and Data Security*. Springer, 2012, pp. 25–40.

[10] Khan, Hassan and Atwater, Aaron and Hengartner, Urs, "A comparative evaluation of implicit authentication schemes," in *Research in Attacks, Intrusions and Defenses*. Springer, 2014, pp. 255–275.

[11] Buschek, Daniel and De Luca, Alexander and Alt, Florian, "Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 1393–1402.

Katharina Krombholz is researcher at SBA Research in Vienna, Austria and mainly interested in usable security, privacy and digital forensics. In 2015, she visited Ruhr University Bochum to collaborate with Thorsten Holz and his group.

Thomas Hupperich is a researcher at Horst-Görtz-Institute for IT-Security at the Ruhr-University in Bochum, Germany. His main research topics include system fingerprinting, user tracking and privacy – especially of mobile devices.

Thorsten Holz Thorsten Holz is full professor at the Ruhr-University in Bochum, Germany and a member of the Horst-Görtz-Institute for IT-Security. His research is focused on system security.