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

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 (digit-PINs, for example). Here, the authors discuss the potential of a new PIN type called force-PINs. 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 select stronger PINs that are harder to observe. The authors also discuss implications for future research on force-sensitive authentication.

Katharina Krombholz
Ruhr-University Bochum and SBA Research

Thomas Hupperich and Thorsten Holz
Ruhr-University Bochum

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, personal identification numbers (PINs), and passcodes[1-4] and presented alternative authentication schemes.

However, none of the proposed systems are capable of replacing passcodes and unlock patterns as a means of authentication. On the one hand, many approaches[5] rely on customized hardware that isn't available off the shelf and thus makes large-scale deployment infeasible. As Marian Harbach and colleagues showed in a field study on smartphone unlocking behavior,[1] (un)locking smartphones produces significant task overhead. This highlights the need for novel authentication methods that perform equally as 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 also are easy for attackers to break[6] and difficult for people with weak fingerprints (because of manual labor, for example) to use.

Here, we summarize our research on *force-PINs*. This PIN scheme enhances digit-only PINs with tactile features

 Published by the IEEE Computer Society 1089-7801/17/$33.00 © 2017 IEEE

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 because of the additional invisible pressure component. In this article, 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.

Figure 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

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 might implicitly help users memorize force-PINs.[7]

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's 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're based on interactions with which they're already familiar. 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 prestudy with nine 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, often it wasn't easy to distinguish which threshold was higher and which one was lower. Therefore, we then set the threshold for deep pressure to 50 percent or more of the maximum possible pressure supported by the hardware.

Evaluation

We summarize the results from our two studies,[8] 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 three conditions in random order:

1. four-digit standard PINs,
2. six-digit standard PINs, and
3. 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 — that is, the time between the first and last touch of the authentication session, as defined by Alexander De Luca and colleagues.[5] 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 (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

Table 1. Mean authentication time in seconds and error rate, with different levels of the independent variables.

Authentication speed	Mean	Standard deviation (SD)
Four-digit	2.34	1.21
Six-digit	3.33	1.56
Force (lab study)	3.66	1.96
Force (field study)	2.69	0.59

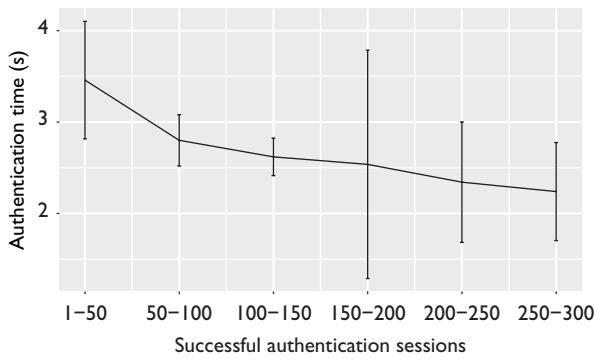

Figure 2. Authentication time development based on the first 300 successful authentication sessions across all participants. The results suggest a habituation to our mechanism and time decreases with training.

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 weren't able to replace the actual PIN scheme on their phones because of 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.

Usability Metrics

Regarding authentication time (see Table 1), 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 analysis of variance (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.

The number of basic errors was similar for digit-only PINs (21 with four-digit and 22 with six-digit standard PINs). In contrast, 36 failed attempts were registered with force-PINs. Given that most of the participants haven't 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 toward 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 we show elsewhere,[8] the error rate also decreases with training.

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

Force Pressure

Because of the low experience with pressure-sensitive screens, participants couldn't distinguish different thresholds easily to separate deep and shallow presses. 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 as a percent of the maximum possible force.

Security

To estimate the security benefit of force-PINs, we performed entropy calculations. Table 2 summarizes

our calculations of zero-order entropy and practical entropy based on collected 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 $-\Sigma_{i=1}^{n} p_i \log_2(p_i)$, 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 aren't evenly distributed across the PIN space, and the most popular position for a digit with deep press (DSSS) was the first, with a probability of 14 percent. This indicates that the practical entropy is lower than the theoretical entropy. Symmetric patterns (DSSD, SDDS) occurred with a probability of 19.2 percent, which is slightly higher than in theory (13.3 percent). According to Joseph Bonneau and colleagues,[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 percent.

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.

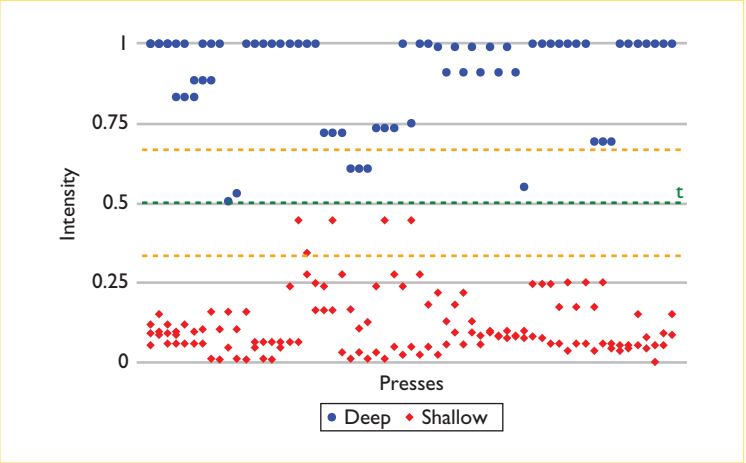

Figure 3. Measured force relative to the maximum possible force. The green line at y = 0.5 represents the threshold for distinguishing between deep and shallow presses. The gray lines at 0.25 and 0.75 indicate two potential thresholds for a three-step force scale (for example, shallow-medium-deep*).*

Table 2. Comparison of entropy.

PIN type	Combinations	Theoretical entropy	Practical entropy
Four-digit	10^4	13.28 bit	11.42 bit[9]
Six-digit	10^6	19.93 bit	—
Force	$20^4[-10^4]$	17.28 bit	14.83 bit

Implications for Future Research and Design

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

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 prestudy, which suggested that people who had never used 3D touch before couldn't 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 (such as *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 examining the feasibility of three-step force-PINs in the course of a longitudinal field study with users that previously have been exposed to pressure-sensitive touchscreens, and ideally have been using two-step force-PINs before. Further, we suggest researching whether ideal pressure thresholds should be customizable — that is, whether user-chosen thresholds vary across a larger user base or converge toward mathematically selected thresholds.

Memorability

The results from our post-lab study survey indicate that users perceive four-digit force-PINs as more memorable than six-digit standard PINs. The findings from our field study also support

this statement, because only two participants renewed their force-PINs throughout the study period. However, our field study doesn't provide long-term insights regarding force-PIN usability, and it was completed within a couple of days by most participants. It therefore remains to be seen whether additional force patterns are indeed easier to remember than additional digits. It also remains to be seen whether overall memorability of force-PINs is dominated by muscle memory instead of visual memory. Such findings would support the potential of force and other tactile components for user authentication.

Unlock Patterns

Our studies only considered force components in combination with digit-based authentication on iPhones. The ability to recognize pressure-sensitive input, however, already has been introduced in Android 1.0, and increasingly Android devices come with compatible hardware (for example, Nexus N and Huawei 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 implementing force-unlock patterns and conducting user studies similar to prior investigations.[8]

Force-Based Implicit Authentication

A new trend in authentication research is implicit authentication. Many approaches have been proposed in the literature, but to date none has been adopted on a large-scale in practice. As Hassan Khan and colleagues show,[10] current methods for implicit authentication aren't 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. Daniel Buschek and colleagues[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 examining whether force patterns can be used to classify users. If this is 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 shouldn't be used to replace it.

Attack Scenarios

Our security evaluation[8] suggests that force-PINs have higher entropy than digit-only PINs and provide a first look at shoulder-surfing resistance. Because of several limitations, further investigation is needed to determine a lower bound for shoulder-surfing resistance. We propose altering the study design from our previous work[8] 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 prestudy with a non-tech-savvy participant who hadn't used force-PINs before but had full control of the video material resulted in 44 out of 50 guessed digit sequences and 11 completely guessed force-PINs. Harbach[1] argues that shoulder surfers in a private environment might know PIN digits, anyhow. Force-PINs don't sufficiently address this threat scenario, as a social insider has the opportunity to observe the victim's PIN entry multiple times. Furthermore, if the attacker already knows the digits, it's rather easy to guess the associated force pattern, especially if the distribution of selected force patterns is already known. Hence, force-PINs don't offer sufficient protection from social insiders. It also remains unclear whether force-PINs are resilient to smudge attacks.[3]

Accessibility

The participants from our studies were recruited around the university campus. Therefore, the education level was higher than expected from the general population. Hence, our results can't be generalized to smartphone users with different demographics. We didn't collect evidence on how elderly persons or people with disabilities interact with force-sensitive screens. Furthermore, it remains uncertain how error-resistant force-PINs

are when entered under environmental constraints — for example, while riding a moving train or multitasking. Such situational disabilities might impact the user's experience with force-PINs, because users are dependent on subtle haptic feedback when digits are entered with force. We therefore argue that an extensive field study should be conducted with marginalized groups.

Beyond Smartphones

Four-digit PINs can be found not only on smartphones but also other devices, such as ATMs, where security is crucial. Various attacks for stealing ATM PINs are shown online. We therefore argue that it's 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.

In this article, we discussed future research and design directions for force-sensitive authentication. To evaluate force-PINs, we conducted two user studies. 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, other aspects require further research before the system can find its way into consumer applications. To motivate further research around this approach, we presented challenges and ideas for future research.

References

1. M. Harbach et al., "It's a Hard Lock Life: A Field Study of Smartphone (Un)locking Behavior and Risk Perception," *Proc. Int'l Symp. Usable Privacy and Security*, 2014; www.usenix.org/system/files/conference/soups2014/soups14-paper-harbach.pdf.
2. A. De Luca and J. Lindqvist, "Is Secure and Usable Smartphone Authentication Asking Too Much?" *Computer*, vol. 48, no. 5, 2015, pp. 64–68.
3. A.J. Aviv et al., "Smudge Attacks on Smartphone Touch Screens," *WOOT*, vol. 10, 2010, pp. 1–7.
4. Y. Song et al., "On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks," *Proc. 33rd Annual ACM Conf. Human Factors in Computing Systems*, 2015, pp. 2343–2352.
5. A. De Luca et al., "Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers," *Proc. Sigchi Conf. Human Factors in Computing Systems*, 2014, pp. 2937–2946.
6. Chaos Computer Club, "Chaos Computer Club Breaks Apple TouchID," blog, 21 Sept. 2013; www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid.
7. A. Bragdon et al., "Experimental Analysis of Touch-Screen Gesture Designs in Mobile Environments," *Proc. Sigchi Conf. Human Factors in Computing Systems*, 2011, pp. 403–412.
8. K. Krombholz, T. Hupperich, and T. Holz, "Use the Force: Evaluating Force-Sensitive Authentication for Mobile Devices," *Proc. 12th Symp. Usable Privacy and Security*, 2016; www.usenix.org/system/files/conference/soups2016/soups2016-paper-krombholz.pdf.
9. J. Bonneau, S. Preibusch, and R. Anderson, "A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking Pins," *Proc. Int'l Conf. Financial Cryptography and Data Security*, 2012, pp. 25–40.
10. H. Khan, A. Atwater, and U. Hengartner, "A Comparative Evaluation of Implicit Authentication Schemes," *Research in Attacks, Intrusions and Defenses*, Springer, 2014, pp. 255–275.
11. D. Buschek, A. De Luca, and F. Alt, "Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices," *Proc. 33rd Ann. ACM Conf. Human Factors in Computing Systems*, 2015, pp. 1393–1402.

Katharina Krombholz is researcher at SBA Research in Vienna, Austria. In 2015, she visited Ruhr-University Bochum to collaborate with Thorsten Holz and his group. Her research focuses on usable security, privacy, and digital forensics. Krombholz has a PhD in media informatics from TU Wien. Contact her at kkrombholz@sba-research.org.

Thomas Hupperich is a researcher in the Horst Görtz Institute for IT Security at Ruhr-University Bochum. His research focuses on system fingerprinting, user tracking, and privacy — especially for mobile devices. Hupperich has a PhD in IT security from Ruhr-University Bochum. Contact him at thomas.hupperich@rub.de.

Thorsten Holz is a full professor in the Horst Görtz Institute for IT Security at Ruhr-University Bochum. His research focuses on system security. Holz has a PhD in computer science from the University of Mannheim. Contact him at thorsten.holz@rub.de.

myCS

Read your subscriptions through the myCS publications portal at **http://mycs.computer.org.**