MIBA: Multitouch Image-Based Authentication on Smartphones

Daniel Ritter
Institute of Media Informatics
Ulm University
89069 Ulm, Germany
daniel.ritter@uni-ulm.de

Florian Schaub
Institute of Media Informatics
Ulm University
89069 Ulm, Germany
florian.schaub@uni-ulm.de

Marcel Walch
Institute of Media Informatics
Ulm University
89069 Ulm, Germany
marcel.walch@uni-ulm.de

Michael Weber
Institute of Media Informatics
Ulm University
89069 Ulm, Germany
michael.weber@uni-ulm.de

CHI 2013 Extended Abstracts, April 27–May 2, 2013, Paris, France.
ACM 978-1-4503-1952-2/13/04.

Abstract

Graphical password schemes can provide better usability than text passwords, especially on smartphones where typing complex passwords on a virtual keyboard can be tedious. However, in order to achieve password strength comparable to text passwords, graphical password schemes require multiple rounds and, therefore, have longer entry times. We propose MIBA as an image-based authentication method that leverages multitouch in order to increase the password space by supporting multiple fingers for click point selection. We outline the MIBA concept, report on practical constraints for multitouch click point selection, and discuss preliminary results that indicate short entry times and the usability of MIBA.

Author Keywords

Image-based authentication; graphical passwords; smartphone; multitouch; cued recall

ACM Classification Keywords

H.5.2 [Information interfaces and presentation]: User Interfaces—*Graphical user interfaces (GUI, Haptic I/O)*; K.6.5 [Management of computing and Information Systems]: Security and Protection—*Authentication*

General Terms

Human Factors, Design, Security

Introduction

Current smartphones provide virtual keyboards for text entry. However, entering text-based passwords on virtual keyboards is more tedious compared to physical keyboards due to varying typing effort for characters from different categories (lowercase/uppercase characters, numbers, special characters). This is especially apparent for passwords containing special characters, which can require up to three taps for entry due to navigation of additional keyboard pages [9].

As an alternative to text-based passwords, graphical authentication methods have emerged. Instead of characters, a graphical password consists of a number of graphical elements or patterns that the user selects or draws on the screen. Nowadays, graphical passwords are already being employed on smartphones to unlock the screen, e.g., the Android Pattern Lock based on Pass-Go [10]. Graphical passwords promise higher usability and better memorability of passwords [1]. However, from a security perspective, graphical passwords often have a smaller theoretical password space than text passwords, which increases the risk of successful guessing attacks. To compensate this, many graphical password schemes require multiple rounds, which can result in longer password entry times compared to text passwords or PINs [1].

We argue that by leveraging the multitouch capabilities of smartphone displays the password space of graphical authentication schemes can be increased without increasing required password entry time. We propose a multitouch image-based authentication method called *MIBA* that allows simultaneous use of multiple fingers for entering graphical passwords. We show that MIBA requires shorter and quicker to type passwords to reach the same entropy, and therefore security, as other graphical password schemes or PIN entry. The use of multiple fingers has the additional advantage that the hand used for password entry also partially obscures the screen, which makes it difficult for others to observe the password (*shoulder surfing*) without hindering password entry for the user.

Related Work

Many graphical password schemes have been proposed in recent years. In their extensive survey, Biddle et al. [1] distinguish three categories: *recall-based schemes* require users to reproduce passwords completely from memory. Examples are *Draw a Secret (DAS)* [4] and *Pass-Go* [10], which require users to draw patterns on a grid. Recognition-based schemes, such as *PassFaces* [7], ask users to correctly recognize a series of images as their password. Cued recall schemes, such as *PassPoints* [11] and *Cued Click Points (CCP)* [2], combine recognition and recall aspects, e.g., by showing images to users and letting them select certain points on the image. While PassPoints uses a sequence of click points on one image as a password, a CCP password consists of a series of images with one click point per image. In CCP, the next image depends on the previous click. Thus, users can recognize wrong clicks when unexpected images appear. Cued recall approaches promise better usability because the provided external cues help users remember associated password information.

Most existing graphical password schemes have been designed originally for the desktop context, yet, many of them could also be used on modern smartphones with touchscreens. However, they are limited to single finger (or pointer) entry. Kim et al. [5] propose multitouch authentication approaches for tabletops in which the

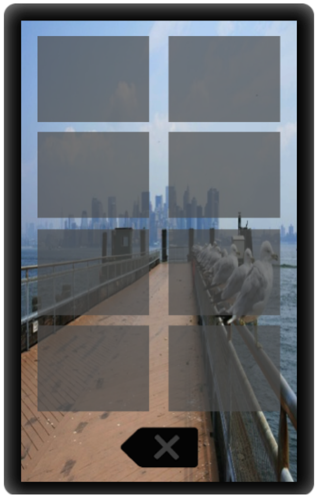

Figure 1: The MIBA scheme with a 4x2 grid of click points.

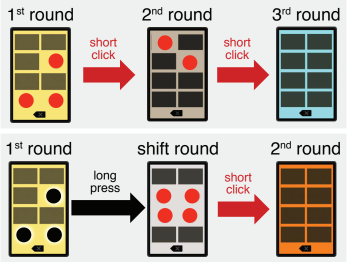

Figure 2: Three normal rounds (top) and two rounds with a shift round activated by a long press (bottom).

second hand serves as a shield or multiple fingers are used to draw rings around password symbols. However, their approaches are optimized for larger screen sizes and tabletop interaction. Similarly, Sae-Bae et al. [8] propose an authentication scheme based on multitouch gestures optimized for tablets. The Android Pattern Lock has also been extended to allow strokes with multiple fingers [6], but the effects for longer passwords have not been studied so far.

The MIBA Scheme

The motivation behind MIBA is to obtain a larger theoretical password space in order to reduce password entry time without sacrificing usability. Therefore, MIBA takes a cued-recall approach and extends the cued click points idea for multitouch use on smartphones.

Authentication Method

A MIBA password can consist of multiple rounds, where in each round the user can mark multiple points on an image. Click points have the advantage that they can be entered quickly, even with multiple fingers simultaneously, while drawing complex patterns requires more time. Like CCP [2], MIBA uses background images as cues and determines the image for the next round based on the user's input in the current round. Thus, the user can instantly recognize if the points selected in the previous round were correct or wrong (expected vs. unexpected image in next round). A back button allows for correction of errors. Each image should also only appear once in a password sequence to prevent memory interference between two instances of the same image.

In comparison to CCP, the supported grid size needs to be drastically reduced in order to account for smaller screen size on smartphones and the reduction of accuracy when marking points with fingers instead of a mouse pointer. In MIBA, the background image is overlaid with a half transparent grid of potential click points to support correct placement of fingers (see Figure 1). Potential click points become fully transparent when a user places a finger on them, as shown in Figure 3. While displaying the grid of potential click points could theoretically also help shoulder surfers, the larger occlusion of the display by the hand used for password entry likely mitigates those effects.

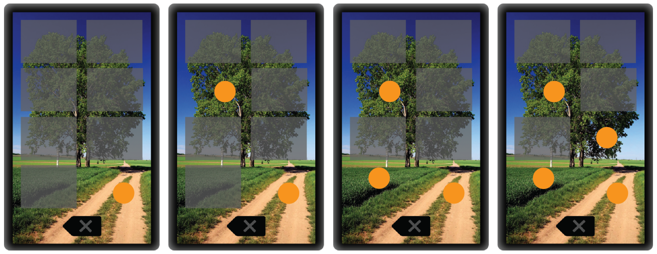

Figure 3: Selecting click points with multiple fingers in MIBA.

Similar to Jansen et al. [3], we further introduce a *shift* function to increase the theoretical password space. The basic idea of the shift function is to provide an additional entry mode that extends the entropy of a round but is not easily discernible from a normal round by an observer. In MIBA, a click with multiple fingers leads to the next round, while a slightly longer press activates a shift round. While in both cases a new image is shown, the phone vibrates to provide feedback about the activation of the shift function to the user. Figure 2 shows the difference between normal round transition and the shift function. As in any normal round, the user selects multiple click points in round 1. However, instead of lifting the fingers off the screen directly, they stay on the screen until the phone's vibration signals activation of the shift round and the image changes. In the shift round, a set of click points fitting to that image are selected and a short click leads to the next normal round. As a result, three normal rounds and two rounds with a shift round in the middle are difficult to distinguish by observers.

Considering the Smartphone
We implemented MIBA on the Android platform. In the process, we identified a number of practical aspects and constraints that need to be considered by graphical password schemes for smartphones.

Initially, we planned to use a 3x4 grid of click points. However, early user experiments on a 3.7 in screen showed that it resulted in too complex and unnatural finger postures for many finger combinations. Thus, the effective password space would be significantly smaller than the theoretical one. We chose a 2x4 grid instead, which resulted in more ergonomic hand postures when using multiple fingers for input. We further considered using all five fingers of the primary hand for input as the second hand is required for holding the phone anyway. Again, many five finger postures on a 2x4 grid are anatomically difficult and using five instead of four fingers results only in a marginal gain in effective password space size. Therefore, the current MIBA implementation supports 1-4 simultaneous click points per round on a 2x4 grid. After each round, MIBA verifies if the input was correct. If the complete password has been entered correctly, MIBA automatically proceeds with an associated action (e.g., login). MIBA does not provide explicit feedback about incorrect input and also continues to provide rounds after the expected password length has been exceeded. This makes brute force guessing attacks more difficult, because MIBA does not reveal any information about the correct password. However, the user can easily recognize incorrect input when an unknown image is displayed.

Performing a click with multiple fingers simultaneously is error prone. To ensure that MIBA recognizes the intended number of click points, input is only recognized on the up event, i.e., when all fingers are lifted off the screen. As a result, users can subsequently place fingers on the grid rather than simultaneously and can also correct finger placement before input is processed. The shift function is implemented by monitoring click points on the screen. The shift function is activated if all detected click points remain static for a certain time t. The threshold t and allowed finger variations can be calibrated to the sensitivity of the specific touchscreen. In our experiments, a threshold of 1s proved to be a good compromise between robust input detection and entry time.

Password Space
With eight potential click points and the use of up to four fingers, the current MIBA implementation supports 162 combinations per round without the shift function. The shift function adds another 162×162 combinations because it can be activated with any combination and then supports the same number of combinations in the shift round. Thus the theoretical password space for MIBA per round is 14.7 bit. Thus, 3 rounds are sufficient to obtain an entropy of 44 bit, which corresponds to common text passwords [1] or a 13 digit PIN (41 bit). CCP would require 9 rounds with single clicks to achieve 44 bit under the assumption that a CCP smartphone implementation could support 30 click points per image due to error margins for finger input.

Preliminary Evaluation

We performed an initial between subjects study in our lab to assess the required entry time of MIBA in comparison to CCP and PIN entry, as well as perceived usability of the MIBA scheme.

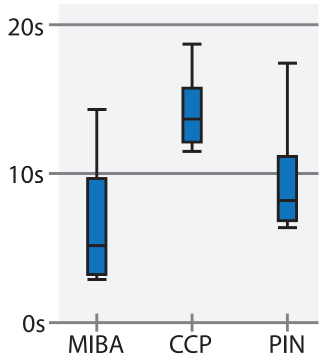

Figure 4: Entry time results for a 42 bit password.

Entry Time
In order to compare MIBA entry time with CCP and PIN, we also implemented a simple PIN interface and an Android version of CCP, which allows for error margins around click points to accommodate finger input.

We recruited participants from the campus population (n=30) and assigned them evenly to one of the three systems. Participants received an introduction to the assigned password scheme and were given ample training time. Then participants were asked to create their own passwords corresponding to 42 bit entropy. Subsequently, the password had to be entered five times. Mental rotation tasks had to be solved after each try to shortly distract participants, as suggested by Chiasson et al. [2].

Figure 4 shows the entry time results per group. With MIBA, 75% of all password entry attempts required less than 10 s (Mdn=5.1), while all CCP attempts required more than 10 s (Mdn=13.6). A Kruskal-Wallis test with Games-Howell post hoc analysis shows that MIBA is significantly faster for entering 42 bit passwords than CCP. No significant differences could be found for PIN entry time (Mdn=8.2), likely due to the range of PIN entry time overlapping with both other systems. However, our preliminary results indicate that MIBA is likely also faster for entering 42 bit passwords than PIN entry.

Usability
Participants were also asked about the usability of the MIBA system. While some participants reported initial difficulties when using multiple fingers for input, participants were overall satisfied with the user experience of MIBA and considered it useful. The required two hand operation was not considered an issue. It is likely that multi finger input would improve with long term use of MIBA, as the short exposure to the system during the study was sufficient for the participants to successfully and quickly enter MIBA passwords with multiple fingers.

Conclusions

MIBA is a cued-recall graphical password scheme that supports multiple fingers for simultaneous selection of click points on an image. As a result, MIBA has an increased theoretical and effective password space compared to single click systems. In contrast to related work, MIBA has been explicitly designed for use on smarthones with multitouch capable screens. In the design process, we identified constraints on grid size and the number of supported click points imposed by device size and hand posture. Nevertheless, our preliminary user study shows that MIBA passwords (42 bit) can be entered faster than comparable schemes. The results also suggest better or at least similar performance than PIN entry.

Future Work
We plan to extend the evaluation of the MIBA scheme to better understand the effects of user chosen passwords on entry time, success rate, password memorability, and shoulder surfing resilience, as well as the effects of image hotspots and preferred finger postures on password entropy. We plan to conduct a field study to obtain insights on practical use of the MIBA scheme and how well users can remember MIBA passwords. Memory interference of multiple passwords also needs to be analyzed.

We expect MIBA to be quite resilient against shoulder surfing, because the simultaneous use of multiple fingers results in natural occlusion of larger portions of the display compared to single finger password entry. Our preliminary results suggest that this occlusion does not affect password entry time. We plan to conduct shoulder surfing experiments to analyze the actual resilience of MIBA in comparison to other graphical password schemes.

Applications
Although graphical password schemes such as MIBA provide usability and memorability advantages over text passwords, their usefulness is rather limited in an online world dominated by text passwords. Currently, the primary application of graphical passwords is unlocking the smartphone screen. However, rather than replacing text passwords on smartphones, graphical passwords can complement them. Similar to unlocking the screen, a graphical password scheme can be used to unlock a password manager on the smartphone. Different graphical passwords could even be defined to unlock password groups with varying sensitivity. Through such integration, smartphone users would only need to use a small number of graphical passwords on their smartphone, while still being able to work with all their text passwords—just without the need of typing them.

Acknowledgements

The authors would like to thank the anonymous reviewers for their helpful feedback. MIBA Background images are courtesy of Martin Linsbauer and used with permission.

References

[1] Biddle, R., Chiasson, S., and Van Oorschot, P. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys 44*, 4 (2012), 1–41.

[2] Chiasson, S., Van Oorschot, P., and Biddle, R. Graphical Password Authentication Using Cued Click Points. In *Proc. ESORICS '07*, Springer (2007).

[3] Jansen, W., Gavrila, S., Korolev, V., Ayers, R., and Swanstrom, R. Picture password: A visual login technique for mobile devices. Tech. Rep. NISTIR 7030, NIST, 2003.

[4] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D. The design and analysis of graphical passwords. In *Proc. 8th USENIX Security Symposium*, USENIX Association (1999).

[5] Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J., Nicholson, J., and Olivier, P. Multi-touch authentication on tabletops. In *Proc. CHI '10*, ACM (2010).

[6] Oakley, I., and Bianchi, A. Multi-touch passwords for mobile device access. In *Proc. UbiComp '12*, ACM (2012).

[7] Passfaces. Science behind passfaces. White Paper. `http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf`.

[8] Sae-Bae, N., Ahmed, K., Isbister, K., and Memon, N. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In *Proc. CHI '12*, ACM (2012).

[9] Schaub, F., Deyhle, R., and Weber, M. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proc. Mobile and Ubiquitous Multimedia (MUM '12)*, ACM (2012).

[10] Tao, H., and Adams, C. Pass-Go : A Proposal to Improve the Usability of Graphical Passwords. *Int. Journal of Network Security 7*, 2 (2008), 273–292.

[11] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, a., and Memon, N. PassPoints: Design and longitudinal evaluation of a graphical password system. *Int. J. Human-Computer Studies 63*, 1-2 (2005), 102–127.