A Tap and Gesture Hybrid Method for Authenticating Smartphone Users

Ahmed Sabbir Arif[1,2], Michel Pahud[1], Ken Hinckley[1], Bill Buxton[1]
[1]Microsoft Research
One Microsoft Way
Redmond, WA 98052 USA
{mpahud, kenh, bibuxton}@microsoft.com

[2]York University
Department of Computer Science & Engineering
4700 Keele Street
Toronto, Ontario M3J 1P3 Canada
a.s.arif@gmail.com

MobileHCI 2013, Aug 27 – 30, 2013, Munich, Germany.
ACM 978-1-4503-2273-7/13/08.
http://dx.doi.org/10.1145/2493190.2494435

Abstract
This paper presents a new tap and gesture hybrid method for authenticating mobile device users. The new technique augments four simple gestures – up, down, left, and right, to the dominant digit lock technique, allowing users to either tap or perform any one of the four gestures on the digit keys. It offers in total 6250000 unique four-symbol password combinations, which is substantially more than the conventional techniques. Results of a pilot study showed that the new technique was slower and more error prone than the digit lock technique. However, we believe with practice it could get faster and more accurate. Also, most users were comfortable and all of them felt more secured while using the new technique.

Author Keywords
Authentication; mobile; security; PIN; gesture; hybrid.

ACM Classification Keywords
K.6.5 Security and Protection: Authentication.

General Terms
Design; Performance; Security.

Introduction
Smartphones are becoming an integral part of our everyday life. A recent survey [13] showed that 55% of

Figure 1. The device and the custom application used during the study. The first picture illustrates the initial state of the hybrid condition, where a random hybrid password 9→ 6◦ 5↓ 7◦ was generated by the system. The password can be located at the top of the application. Here, to unlock the device, one has to make a left gesture on the "9" key, tap on the "6" key, make a down gesture on the "5" key, and then tap on the "7" key. The second picture illustrates a state where a user already inputted the first two items. Note that, here and similar to the default Windows Phone 7 lock-screen, the "cancel" button has changed to the "backspace" («) button to accommodate error correction.

all U.S. mobile phone users own a smartphone and about two thirds of the new buyers are opting for one. Smartphones are built with more advanced computing capability and connectivity than regular mobile phones. This allows users to perform variety of tasks on these devices. Thus, smartphones usually accrue sensitive information over time and often gain access to wireless services and organizational intranets. This makes it vital to secure the data stored in these devices. Although, it has been established that user authentication is the most practical method for securing smartphone data, maintaining a sensible balance between the usability and the effectiveness of the password schemes remains a persistent problem [9]. Users are reluctant to use schemes that are too complex, while using simpler schemes compromises the security [14]. At present, the most popular password authentication technique is digit lock. Reportedly, 88% mobile users use this method on their devices [8]. With this method, users usually select a four-digit personal identification number (PIN) that they memorize and input using a virtual keypad to unlock a locked phone. This method offers 10000 unique four-digit password combinations. Recently, a graphical method, called pattern lock, is becoming popular amongst the Android OS users [1]. With this technique, users select a pattern by connecting four or more dots from a 3×3 grid. All connecting dots have to be unique. Users are allowed to connect a dot, which requires going through other dots, only when those dots have already been used. Under these conditions, this method offers 389112 distinct patterns [1]. Both of these methods have been criticized for their vulnerability to attacks due to the limited number of possible combinations [15] and guessability. Pattern locks usually leave oily residue or smudge on the screen, from which it is often possible to guess the password patterns [1]. Numerous alternate methods have been proposed to enhance mobile security, such as image selection [9, 12] that requires users to select sequence of images as passwords, stroke-based textual passwords [17], where users have to input textual passwords using gestures, multi-word passwords [7, 15] that enforce users to select multiple words as passwords, object-based schemes [2] that automatically construct textual passwords from digital objects such as images, etc., biometrics [4] that authenticate users through their fingerprints, typing pattern, face recognition, etc. Several issues have been identified with these techniques as well. The use of complex graphical passwords can enhance mobile security significantly. However, in practice, users often select patterns that are easily predictable [3]. Multi-word methods, in contrast, are usually error-prone and time consuming as it is often challenging to input such passwords using virtual mobile keyboards, mainly due to smaller key-sizes and the need for swapping between multiple keyboard layouts to input special characters [11]. Biometrics, on the other hand, is difficult to adjust due to the trade-off between impostor pass rate and false alarm rate [5]. Besides, most of these techniques are substantially different from the dominant digit lock technique. This often discourages users to switch to a new technique. This also increases the production cost for smartphone manufactures.

The New Technique

We propose a new hybrid user authentication technique that augments four gestures: up, down, left, and right, to the ten digit keys from 0 to 9 of a virtual keypad. To initiate these gestures, one has to first touch a key and then stroke up, down, left, or right, respectively. While

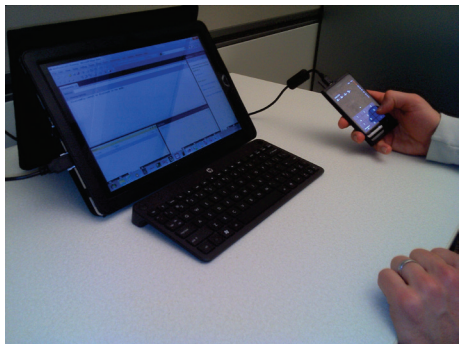

Figure 2. The experiment setup. Here, a user is inputting PINs using the custom software.

selecting a password, one could either tap on a key to select the corresponding digit or initiate any one of the four gestures. As the gestures are differentiated based on where they were initiated, a gesture on a specific key is different from the same gesture that was initiated on a different key. Based on a pilot, a threshold of 0.5 cm was used for the minimum gesture length. That is, a gesture had to be at least 0.5 cm long from touch-down to touch-up, to be considered as a gesture. Otherwise, the system recorded a tap.

Motivation

The new technique looks and feels similar to the most popular digit lock method (see Figure 1), which may encourage users to give it a try. Also, it allows users to select passwords that contain only digits, only gesture, or both digits and gestures. This eliminates the need for switching between different techniques. This is also beneficial to manufacturers as they do not have to develop multiple systems. The hybrid technique provides five choices per key, one digit and four gestures. This increases the total number of unique combinations significantly compared to the dominant ones. Furthermore, a recent study [1] indicated that combinations of taps and gestures are relatively harder to retrieve from smudges on the touchscreens than individual taps or gestures. Finally, as the gestures can be relatively short, 0.5 cm and above, it may be difficult for shoulder-surfers to differentiate between the gestures and the digits, and also to determine the directions of the gestures.

A Pilot Study

We conducted a pilot study to compare the new technique with the dominant digit lock technique. The intention was not to evaluate the security but to investigate how it performs in terms of speed, accuracy, and usability compared to the dominant one.

Apparatus

We used a Nokia Lumia 800 (116.5×61.2×12.1 mm, 76 cm^3, and 142 grams) during the study. The device ran on Windows Phone 7 OS at 800×480 pixel resolution and ~252 ppi pixel density. A custom application was developed with WPF/C# to replicate the default Windows Phone 7 lock-screen. See Figure 1. During the study the device was connected to a tablet using a USB data cable. See Figure 2. This allowed the application to log all interactions with timestamps and record user performance directly to the tablet.

Participants

Twelve participants took part in the study. Their age ranged from 24 to 32 years, average 27. Three of them were female and two of them were left-handed. Eight users owned touchscreen smartphones, while the rest owned conventional mobile devices. They all used their devices frequently, that is, every day for at least three hours. They received a small gratuity for participating.

Design and Procedure

The study investigated three four-symbol password combinations: 1) *digit* only that contained four digits, similar to the digit lock approach, 2) *gesture* only that contained four gestures, and 3) *hybrid* that contained two digits and two gestures. A within-subjects design was used to explore the three password combinations in three counterbalanced conditions. The custom application generated one random password per condition for each participant at run-time. During a condition, participants were asked to input the corresponding password for 105 times in three equal

Limitations

Similar to almost all recently proposed techniques, the hybrid method assumes that users will indeed use a hybrid password to secure their smartphone data. However, in practice, users have the tendency of selecting short and easy-to-guess textual passwords [10]. Likewise, they often select patterns that are easy to predict [3]. Such tendencies can hinder the efficacy of the new technique, making it comparable to the digit lock.

Smudge attack is another concern for the new method. Although, the combination of tap and gesture has a comparatively lower retrieval rate from the smudges left on the screen [1], the possibility of such incidents remains.

Finally, as performing gestures take more time than tapping, theoretically a hybrid password will take more time to input than a digit-based password. Some users may find this frustrating.

blocks (3×35 attempts). Participants practiced inputting the password(s) for 15 times before each condition. Thus, in summary the design was: 12 participants × 3 conditions (*digit*, *gesture*, *hybrid*) × 3 blocks × 35 attempts per block = in total 3780 attempts, excluding the 3×15 practice attempts.

The system represented the gestures in the passwords using the following symbols: ↑ for up, ↓ for down, ← for left, → for right, and ◦ for taps. See Figure 1. We used symbols instead of texts to reduce visual scan time and the mental processing and preparation time, as it takes less time to process a symbol than multi-character texts. The passwords were visible on the screen throughout the conditions to allow users to refer to those when they cannot remember the passwords. See Figure 1. However, we instructed them to look at the passwords only before or after an attempt. We did not allow them to select their own passwords in an attempt to avoid situations where multiple users selected the same password(s), which is not unusual [10]. This also allowed us to investigate a wide range of digits and gestures by eliminating the possibility of the selection of the most common patterns [3]. Note that, as discussed earlier, the intention of this study was to compare the performance of the new technique with the dominant one, and not to analyze the security.

Users were instructed to hold the device with their dominant hand and then input the password(s) using the thumb of the same hand. A tap or gesture was recorded from the moment they touched the screen to the moment they lifted their finger(s). They could rest between the conditions or before they started inputting a password. Participants were allowed to correct their mistakes using the "Backspace" key. However, it was not enforced as users usually find it difficult to verify their input in the password field where dots are displayed for each attempt. Similar to the default Windows Phone 7 lock-screen, the custom software provided users with haptic feedback on incorrect input attempts. When a password was inputted incorrectly, the device vibrated for 200 ms. The following metrics were calculated during the study:

- *Entry Speed (seconds):* This denotes, on average, how much time it took to input one password.
- *Error Rate (%):* This denotes the average percentage of incorrect operations i.e. taps or gestures per password. For example, if "**5**234" was inputted instead of "**1**234", the error rate was 25%. Note that this metric does not consider error correction efforts.

In addition, participants were asked to fill out two short questionnaires. One prior to the study that investigated what sort of user authentication method they use on their mobile devices. Another after the study, where they were asked to rate the investigated techniques, i.e. how secured they felt using the techniques, how hard it was to memorize the random passwords, etc.

Results

An Anderson-Darling test revealed that the study data was not normally distributed. This is most likely due to the insufficient number of different values. Thus, we used nonparametric tests for all analyses. We also filtered (2%) outliers beyond 3σ from the mean.

Entry Speed

A Friedman test identified a significant effect of method on entry speed (χ^2=20.67, p<.0005, df=2). On average entry speed for *digit*, *gesture*, and *hybrid* were 1.01,

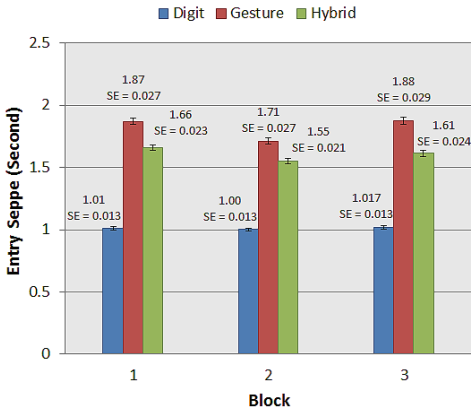

Figure 3. Average entry speed (seconds), with standard error (SE), for all investigated techniques.

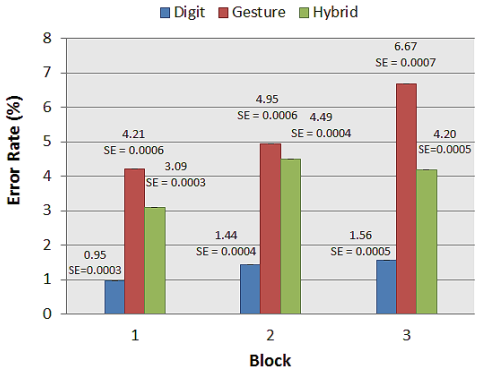

Figure 4. Average error rate (%), with standard error (SE), for all investigated techniques.

1.82, and 1.61 seconds, respectively. Post-hoc pairwise comparisons revealed that *digit* was significantly faster than *gesture* and *hybrid*, and *hybrid* was significantly faster than *gesture*. A significant effect of block was also identified for *gesture* (χ^2=10.17, p<.05, df=2) but not for digit (χ^2=1.17, p>.05, df=2) or hybrid (χ^2=5.17, p>.05, df=2). Figure 3 illustrates average entry speed for all technique during the three blocks.

Accuracy

A Friedman test identified a significant effect of method on accuracy (χ^2=11.62, p<.005, df=2). Average error rate for *digit*, *gesture*, and *hybrid* were 1.31, 5.28, and 3.93%, respectively. Post-hoc pairwise comparisons revealed that *digit* was significantly more accurate than *gesture*. No such indications were identified for the other groups. There was also no significant effect of block on accuracy for *digit* (χ^2=0.64, ns, df=2), *gesture* (χ^2=4.35, p>.05, df=2), or *hybrid* (χ^2=4.54, p>.05, df=2). Figure 4 illustrates average error rate for all technique during the three blocks.

Tap Error vs. Gesture Error

A Wilcoxon Signed-Rank test identified significance regarding action type (i.e. tap or gesture) on error rate (z=-3.06, p<.005). Users made significantly more mistakes while inputting gestures (73%) than digits (27%). A deeper analysis revealed that 28% tap errors were committed when users mistakenly inputted gestures instead of digits, while 33% gesture errors were caused by accidental digit inputs.

User Evaluation

Most users (67%) responded that they found the hybrid technique comfortable to use, while the rest 33% found it uncomfortable.

REMEMBERING THE PASSWORDS

A Friedman test identified a significant effect of technique on users' difficulty in remembering the passwords (χ^2=16.89, p<.0005, df=2). Almost all users (83%) found *gesture* and *hybrid* harder to remember than *digit*.

SENSE OF SECURITY

A Friedman test found a significant effect of technique on users' sense of security (χ^2=16.55, p<.0005, df=2). Almost all users (92%) felt more secured using *gesture*, while all of them (100%) felt more secured using *hybrid* than *digit*.

Discussion

The hybrid technique yielded a lower entry speed and higher error rate compared to the digit lock technique. We expected this as gestures takes more time than taps. Results also showed that most of the input errors were committed while performing the gestures. Two additional factors contributed to the hybrid technique's lower accuracy rate. First, it was often hard for users to memorize the randomly generated passwords. Thus, they often mistyped the numbers or mis-performed the gestures. This phenomenon may reduce in real life scenarios when users will select their own passwords. Second, the gestures performed on the bordering keys often ended on the bezel, which caused misrecognition. However, we noticed that after some time users realized that they have to complete the gestures within the screen and the gestures do not have to be that long (≥0.5 cm). This encouraged them to initiate and complete the gesture within the keys. We did not observe any significant effect of learning, other than on entry speed for gestures, most probably due to insufficient data. However, prior studies showed that

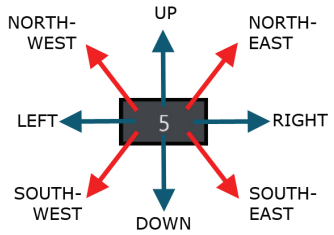

Figure 5. A variation of the hybrid method that will allow users to apply four additional gestures: north-west, north-east, south-west, and south-east, on each key. This will increase the total number of possible unique four-symbol password combinations from 6250000 to 65610000.

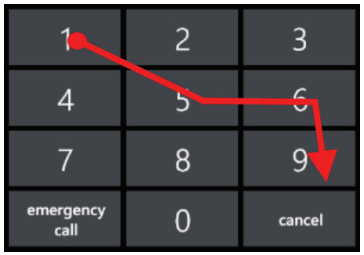

Figure 6. Another variation of the hybrid method that will allow users to input their PINs by drawing shapes through the digits, similar to the ShapeWriter [16] approach. Here, the user entered his/her four-digit PIN "1569" by connecting the digits. The dot indicates the starting end of the gesture.

users' gesture input performance improve with practice [16]. Encouragingly, most users found the new technique comfortable, and all of them felt more secured while using it.

Conclusion and Future Work

We presented a new tap and gesture hybrid mobile user authentication scheme that augments four gestures to the conventional digit lock technique. It provides in total 6250000 unique four-symbol password combinations. A pilot study comparing the new and the digit lock technique revealed that the former was significantly slower and more error prone. However, most users found the new technique comfortable to use and all of them felt more secured while using it. In the future, we plan on conducting a longitudinal study to investigate if users' entry speed and accuracy improves with practice. The study will also examine memorability to determine the effects of user-chosen passwords and the security of this system. We also plan on exploring two variations of the hybrid technique. The first will allow users to perform eight gestures on a key, see Figure 5, and the second will allow users to input the PINs by connecting the digits, see Figure 6.

References

[1] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., and Smith, J. M. Smudge attacks on smartphone touch screens. In *Proc.WOOT '10*. USENIX (2010), 1-7.

[2] Biddle, R., Mannan, M., Van Oorschot, P. C., and Whalen, T. User study, analysis, and usable security of passwords based on digital objects. *Trans. Info. For. Sec.* 6, 3 (2011), 970-979.

[3] Chiasson, S., Forget, A., Biddle, R., and Van Oorschot, P. C. User interface design affects security: patterns in click-based graphical passwords. *Int. J. Inf. Security* 8, 6 (2009), 387-398.

[4] Clarke, N. L. and Furnell, S. M. Advanced user authentication for mobile devices. *Computers & Security* 26, 2 (2007), 109-119.

[5] Davies, D. W. and Price, W. L. Security for Computer Networks. John Wiley & Sons, Inc., 1989.

[6] Dhamija, R. and Perrig, A. Déjà Vu: a user study using images for authentication. In *Proc. SSYM '00*. USENIX (2000), 4-4.

[7] Jakobsson, M. and Akavipat, R. Rethinking passwords to adapt to constrained keyboards. In *MoST Workshop '12*. IEEE (2012).

[8] Jakobsson, M., Shi, E, Golle, P., and Chow, R. Implicit authentication for mobile devices. In *Proc. HotSec '09*. USENIX (2009), 9-9.

[9] Jansen, W. Authenticating mobile device users through image selection. *Data Security*, 2004.

[10] Kim, I. Keypad against brute force attacks on smartphones. *IET Information Security* 6, 2 (2012), 71-76.

[11] Mannan, M. and Van Oorschot, P. C. Passwords for both mobile and desktop computers: ObPwd for Firefox and Android. *USENIX* 37, 4 (2012), 28-37.

[12] Nazir, I., Zubair, I., and Islam, M. H., User authentication for mobile device through image selection. In *Proc. NDT '09*. IEEE (2009), 518-520.

[13] Nielsen Holdings. Two thirds of new mobile buyers now opting for smartphones. http://shar.es/xfZvs

[14] Raguram, R., White, A. M., Goswami, D., Monrose, F., and Frahm, J-M. iSpy: Automatic reconstruction of typed input from compromising reflections. In *Proc. CCS '11*. ACM (2011), 527-536.

[15] Skillen, A. and Mannan, M. Myphrase: Passwords from your own words. Spectrum, Concordia University, Montreal, Quebec, Canada, 2013.

[16] Zhai, S. and Kristensson, P.-O. Shorthand writing on stylus keyboard. In *Proc. CHI '03*. ACM (2003), 97-104.

[17] Zheng, Z., Liu, X., Yin, L., and Liu, Z. A stroke-based textual password authentication scheme. In *Proc. ETCS '09*. IEEE (2009), 90-95.