The Use of Pseudo Pressure in Authenticating Smartphone Users

Ahmed Sabbir Arif[1], Ali Mazalek[1], Wolfgang Stuerzlinger[2]
[1]Synaesthetic Media Laboratory
Ryerson University
Toronto, Ontario, Canada
{asarif, mazalek}@ryerson.ca
[2]School of Interactive Arts + Technology
Simon Fraser University
Surrey, British Columbia, Canada
w.s@sfu.ca

ABSTRACT
In this article, we present a new user authentication technique for touchscreen-based smartphone users that augments pseudo touch pressure as an extra security measure to the conventional digit-lock technique. The new technique enhances security by offering more unique password combinations than the most popular ones, by making each password specific to its owner, and by reducing the threat of smudge attacks. A study comparing the new technique with the digit-lock technique showed that overall it is slower and more error-prone, but performs substantially better in short term. Also, most users felt more secure using it and wanted to use it dominantly on their smartphones. A second study confirmed that it does enhance security by making it relatively more resistant to smudge attacks and less vulnerable to situations where attackers are already in possession of users' passwords.

Categories and Subject Descriptors
H.5.2 [**User Interfaces**]: Interaction styles (e.g., commands, menus, forms, direct manipulation); K.6.5 [**Security and Protection**]: Authentication.

General Terms
Performance, Design, Experimentation, Security, Human Factors.

Keywords
User authentication; digit-lock; touchscreen; smartphones; mobile security; mobile phones; pressure; pseudo pressure; password; PIN; force.

1. INTRODUCTION
Smartphones are becoming an integral part of our everyday life. A recent survey showed that about 68% of the mobile subscribers in the U. S. already own a smartphone and 84% of the new buyers chose smartphones for their new handsets [26]. Smartphones are built with more advanced computing capability and connectivity than regular mobile phones. This allows users to perform a variety of tasks on these devices. As a result, 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, user authentication is one of the most practical methods for securing smartphone data, maintaining a sensible balance between the usability and the effectiveness of the password schemes remains a persistent problem [19]. Users are reluctant to use schemes that are too complex, then again using simpler schemes compromises security [30].

To address this, we present a new user authentication method that augments pseudo touch pressure as an extra security measure to the conventional digit-lock technique. While selecting a password with the new technique, user can *actively* pick the level of pressure on the keys. The system records both the key sequence and the amount of pressure applied on each key. Later, when users are re-entering their passwords to authenticate themselves, it matches both the pressure levels and the key sequences, and unlocks the device only when both of these parameters match.

We start this article with a brief review of the most popular user authentication techniques and the challenges they face. We also discuss the use of pressure in user authentication. Then, we compare the performance of the proposed technique with the conventional one in a user study. We investigate users' password selection process and user experience of the new authentication method. Then, we present results of a second user study that validates our claim that the proposed technique is more secure than the conventional one. Finally, we conclude with future extensions of this work.

2. Related Work
Currently, the most popular user authentication technique for mobile devices is locking the screen with a four-digit Personal Identification Number (PIN). This method is often referred to as digit-lock. A recent survey showed that about 67% mobile users, who use a user authentication technique on their devices, use digit-lock [34]. It requires users to select and memorize a four-digit PIN, and then input it using a keypad or keyboard to unlock a locked device. This method offers 10,000 unique four-digit password combinations.

Lately, a graphical method called pattern-lock is becoming popular amongst the Android OS users [4]. Pattern-lock requires users to select a pattern by connecting four or more dots from a 3×3 grid. All connecting dots need to be unique. Users are allowed to connect a dot that requires going through other dots, only when those dots have already been used. Under these conditions, this technique offers 389,112 distinct password patterns [4]. A recent survey showed that about 20% mobile users, who use a user authentication technique on their devices, use pattern-lock [34].

Both digit-lock and pattern-lock techniques have been criticized for their vulnerability to attacks due to the limited number of possible password combinations [33] and guessability [12]. Graphical passwords are relatively easier to spy on by *shoulder surfing* [13, 36]. In addition, touch interactions usually leave oily residues or

MOBIQUITOUS 2014, December 02-05, London, Great Britain

DOI 10.4108/icst.mobiquitous.2014.257919

smudges on the touchscreen, from which it is often possible to guess a password pattern [4]. Therefore, many argue that the two most popular user authentication techniques do not fully meet the requirement of adequately protecting the user's data stored on the device [12].

Many alternatives have been proposed to enhance mobile security, such as image selection that requires users to select a sequence of images as passwords [20, 27], stroke-based textual passwords that require one to input textual passwords using gestures [37], tap and gesture hybrid passwords that include directional gestures to digit-lock [3], multi-word passwords that enforce users to use multiple words as passwords [18, 33], object-based schemes that automatically create textual passwords using digital objects such as images [5], and biometrics that authenticate users through their fingerprint, face, hand geometry, voice, iris, or input pattern [9, 31, 35].

Various issues have been identified with these techniques as well. The use of complex graphical passwords enhances mobile security significantly. But, in practice, users usually select patterns that are easily predictable [8]. Multi-word methods are usually error-prone and time consuming, as it is 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 [24]. Biometric, on the other hand, require additional hardware, such as fingerprint scanners and is difficult to adjust due to the trade-off between impostor pass rate and false alarm rate [10]. There are also user concerns regarding the storage of physiological features [29]. Besides, most of these techniques are substantially different from the most popular digit-lock technique. This often discourages mobile users to switch to a new and more secure technique. Similarly, manufacturers are reluctant on providing the support for these methods, as they usually increase the production cost for smartphones.

2.1 Pressure in User Authentication

Several techniques have used pressure as an additional measure for authenticating smartphone users. Malek et al. [23] integrated pressure as a binary input with two variances of the pattern-lock method. Their technique allowed users to use either regular or extra pressure while connecting dots to draw patterns. They conducted a study to evaluate the new technique's usability, where users inputted self-selected patterns using a PHANTOM Haptic Device. They, however, did not evaluate the technique's security.

Similarly, De Luca et al. [12] integrated touch coordinates, touch pressure, and touch area with pattern-lock. They conducted a longitudinal study, where users inputted patterns assigned to them once a day for three weeks using touchscreen-based smartphones. Results found their technique to be 77% accurate. Likewise, Bo et al. [6] developed a framework to authenticate smartphone users based on their touch coordinate, touch pressure, and touch duration. Results of a user study showed that their framework could reduce both false acceptance and false rejection rates substantially (< 1%). Shahzad et al. [32] proposed a similar method that augmented touch velocity, stroke time, and device acceleration with simple gestures. In a study, their technique yielded about 95% accuracy rate. They, however, used very simple gestures (mostly straight lines) to evaluate their technique.

Recently, Kim et al. [21] developed a new user authentication technique for tabletops, where uses have to touch the screen with both hands to see a grid of objects, and then have select some of those objects in a predetermined sequence and pressure-levels to unlock the device. A more recent paper mentioned that pressure could be used with digit-lock as an extra security measure [28], but did not elaborate on (or evaluate) the approach.

3. The New Technique

We propose a new user authentication technique that adds an extra layer of security to the most popular digit-lock technique by augmenting the detection of pseudo pressure. When selecting a PIN with the proposed techniques, the user can apply different pressure levels on the digit keys. The system records both the key sequence and the amount of pressure applied on each key. In other words, the selected digits in sequence and their corresponding pressure levels becomes the user's PIN. Later, when the user is re-input his/her PINs to unlock a locked device, the technique compares both the key sequence and the amount of pressure on each key, and unlocks the device only when both of these parameters match. Figure 1 illustrates this process.

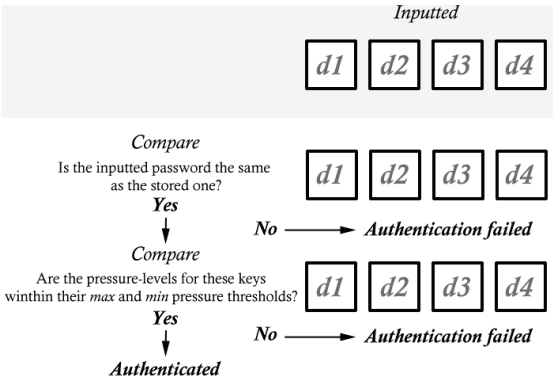

Figure 1. User authentication process with the new pressure-based technique. Here, "d" represents a digit.

3.1 Pressure Detection Simulation

Current mobile devices do not provide the hardware support for measuring pressure and simulate pressure using either the time- or the touch-point/area-based approach. Here, we used a hybrid of these two approaches to simulate pressure detection [2]. This approach originally detected two pressure levels, regular and extra, by using the average time it takes to perform a task and the average touch-point movement for that task as baselines. It simulated extra pressure when users took more time and/or their touch-point moved a larger distance than the baselines. We modified this approach to support more than two pressure levels. The customized version simulates multiple pressure levels by mapping different tap times and touch-point movements to different pressure levels. To be more exact, based on the data from the PIN selection phase, the system determines different ranges of *acceptable* tap times and touch-point movements for different pressure levels. It then simulates a pressure level when the time users take to tap on a key and/or the distance their finger slides, is/are within that level's predetermined range(s). In our system, the maximum and minimum values for a pressure level's tap time and touch-point movement are simply the values from one standard deviation above and below their means, respectively. We used this thresholds based on a pilot study, where we explored other alternatives, such as ±0.5-3.0 standard deviations and ± 0.5-3.0 standard errors.

We used the hybrid approach, as a prior study showed that it is able to support a larger group of users compared to the existing pressure detection simulation techniques [2].

3.2 Active vs. Passive Pressure

In our system, we use *pressure* as an active form of input. That is, users have to actively select a particular pressure level for a key.

Theoretically, users could ignore the presence of pressure detection simulation (i.e. treat *pressure* as passive input) and enter the

numbers as they usually would. The system will still compare the pressure levels applied on each key on authentication attempts. While this offers a more natural input experience for users, we argue, this alone is not sufficient to differentiate between users, as prior studies showed that users apply almost the same amount of pressure while tapping on flat surfaces [2, 25]. This means, the addition of *passive* pressure detection and comparison will not enhance the security of the technique, as it will cause frequent false positives. Another issue with passive pressure detection is that the system will generate false negatives when users apply a different pressure level on a key by accident. An awareness of the *pressure detection* will at least allow them to consider the possibility that they may have applied incorrect pressure levels on the keys, while not knowing will create further confusions.

3.3 Memorability

One may argue that it should be difficult for users to memorize a PIN with different pressure levels. We agree that, theoretically, it should be more difficult than memorizing a digit-only PIN. However, prior studies showed that users are able to memorize and control two pressure levels without any difficulties [2]. Another study claimed that users could control 6±1 pressure levels without major difficulties [25]. Thus, we believe that, although relatively more difficult, users should not have any major difficulties to remember a pressure-based password. We tested this hypothesis in the first user study.

3.4 Motivation

The design of the technique was motivated by the following factors.

3.4.1 Learnability

Users are usually reluctant to use authentication schemes that are too complex or too different from the schemes they are already familiar with [30]. As illustrated in Figure 2, the new technique looks and feels similar to the most popular digit-lock technique. This reduces the learning effect and might encourage users to give it a try. However, our investigation revealed that different devices use different colour schemes for their lock-screen interface. Apple iPhone 5, for example, uses a multicolour background, while Google Nexus 4 uses a green one. Thus, we used a white background, which is more generic, to eliminate the effect of background colour.

3.4.2 Convenience

Our technique allows users to disable pressure detection simulation from the settings and to input PINs like the conventional digit-lock technique. This eliminates the need for switching between different user interfaces. This is also beneficial to smartphone manufacturers, as they do not have to develop multiple systems.

3.4.3 Password Combinations

A study showed that users could easily control two pressure levels on touchscreens [2]. This gives users at least two pressure choices per key and increases the total number of unique four-digit password combinations from digit-lock's 10,000 to 160,000. However, another investigation claimed that users could control 6±1 pressure levels without major difficulties [25]. Thus, in theory, the new technique can provide at most seven pressure choices per key, increasing the total number of unique four-digit password combinations to 24,010,000. This is substantially more than what most popular user authentication techniques offer [3].

3.4.4 Security

A prior work showed that it is not very difficult to retrieve passwords from the smudges left on the touchscreens [4]. Theoretically, it should be more difficult to guess different pressure levels from the smudges. Besides, it should be relatively more difficult to unlock a device even when imposters know the correct PIN, as the device owner may have used different pressure levels on the keys. We verify these hypotheses in the second user study.

In addition, as the new technique allows users to define their own pressure levels, it should be more challenging for imposters to guess a password, even when they know, for example, that *soft touch* was used on a key, as different users could interpret *soft touch* in different ways. We, however, do not verify this hypothesis in this work.

3.5 Limitations

Here we discuss the limitations of the proposed technique.

3.5.1 Possible Password Combinations

The new technique offers at least 160,000 unique four-digit password combinations with two pressure levels and at most 24,010,000 unique combinations with seven pressure levels. However, the *true* number of possible unique password combinations would be somewhere in between these two numbers, especially when pressure simulation approaches are used, as the virtual thresholds for different pressure levels may overlap.

3.5.2 Password Selection

Most commercial techniques allow users to pick a password by inputting it twice—once to select it, then again, to verify it. The pressure-based technique requires more input attempts than that to calculate the pressure thresholds. Although, the accuracy of the technique increases with increasing training data, we allow users to select a password by inputting it fifteen times. This is because, it is rather unlikely for users to use a technique that enforces a lengthy password selection process upon them, despite it being more secured. However, in a pilot study the system was able to acquire about 80% accuracy rate with only ten samples.

3.5.3 Entry Speed

Prior studies showed that it usually takes more time to perform a task with extra pressure [7]. Therefore, the input of a pressure-based PIN might take more time when extra pressure is applied. Some users might find this frustrating.

Hence, to provide a better comparison and to acquire user feedback, during the first user study, we asked participants to apply *extra* pressure on their pressure-based PINs. We believe when the technique performs moderately well and the users do not show reluctance to use it when extra pressure is enforced, it makes a case for the new technique, as theoretically it should yield relatively favourable results with regular and lower pressure levels.

Figure 2. The device and the custom application used during the user studies.

4. User Study 1—Performance

This user study compared the new technique with the most popular digit-lock technique. The intent was to investigate how it performs in terms of speed and accuracy compared to the conventional one. It also explored user preference for pressure as an extra security measure for authenticating smartphone users.

4.1 Apparatus

We used a custom application, developed with the Android SDK, on a Google Nexus 4, 133.9×68.7×9.1 mm, 139 g, for the user study. The device ran on Android 4.4.2 KitKat at 1280×768 pixel resolution and 320 ppi. The application looked and behaved like the default Android lock-screen. See Figure 2. However, we used a more generic white background, as different devices use different colour schemes for their lock-screen interface. See Section 3.4.1. It logged all user interactions with timestamps and recorded user performance directly to the device's internal storage.

4.2 Participants

Twelve participants, aged from 19 to 34 years, mean 24.17 (SD = 4.98), participated in the study. They were recruited through online communities, local university emailing lists, and by word of mouth. Six of them were male and six were female. One was left-handed and one was ambidextrous. They were all frequent touchscreen users, that is, owned and used their touchscreen-based device for on average four years. None of them were expert in mobile security.

Eight participants used the digit-lock technique on their mobile phones, while the remaining used pattern-lock.

4.3 Procedure

We compared two user authentication techniques: the new and the existing digit-lock technique. During the study all participants inputted self-selected PINs with both techniques. The conditions were counterbalanced to eliminate the effect of learning.

During the *new* condition, participants were asked to pick a four-digit password by inputting it with the pressure-based technique fifteen times. They had to input their passwords fifteen times to make sure that the system had enough data to calculate the pressure thresholds (see Section 3.5.2). They were instructed to select a password that they would feel comfortable using on their own device and to apply *extra* pressure *at least* on one key (see Section 3.5.3). Participants were then asked to complete a short questionnaire that asked about their password selection process. This imposed roughly a two-minute break before the main condition. The intention for this was to investigate whether users can remember the pressure levels, when they do not get to input the passwords right after selecting them. The questionnaire also provided us with a rough idea of how users selected their passwords. During the main condition, participants inputted their passwords fifty times with the new technique. Only fifty input attempts were given, as we observed that users get tired easily and suffer from fatigue when inputting PINs for extended periods of time.

Participants followed the same procedure during the *digit-lock* condition. However, they did not have to use different pressure levels on the keys. They were allowed to use the same digits they used with the *new* technique.

In both conditions, we instructed users to hold the device in the portrait position with their dominant hand and then to input using the thumb of that hand. We used this position as mobile users use it most frequently [16]. Interestingly, our post experiment interview revealed that in real-life all of our participants usually use this position to input PINs.

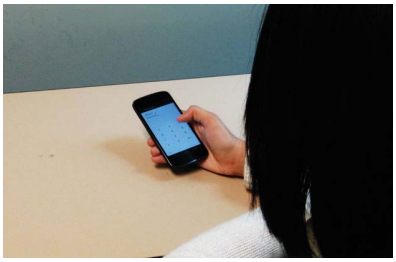

Figure 3. A user is inputting self-selected password using the custom software.

The system recorded a tap from the moment users touched the touchscreen to the moment they lifted their finger. They could rest between the conditions or before they started inputting a PIN. Participants were allowed to correct their mistakes using the Backspace key. However, this was not forced, as it was difficult for them to verify their input in the password field that masked inputted characters with the *bullet* character. See Figure 2.

Nowadays, it has become a common practice to hide passwords as they are typed to avoid bystanders reading the password. Consequently, we did not provide users with visual feedback on pressure input. However, similar to the default Android OS, the custom application provided the users with haptic feedback on incorrect input attempts. That is, when a password was inputted incorrectly, the device vibrated for 250ms. The device also provided haptic feedback on a key press. That is, it vibrated for 25ms when users tapped on a key. It did not provide the users with any auditory feedback.

Upon completing the study, participants were interviewed and asked to fill out a second short questionnaire, where they could rate and comment on the investigated techniques.

4.4 Performance Metrics

The following performance metrics were calculated during the user study.

- **Entry Speed (seconds)**: This signifies the average time it takes to input a PIN.
- **Error Rate (%):** This denotes the average percentage of incorrect operations, such as an incorrect tap or an incorrect pressure level, per PIN [3]. For example, when users input "1235" instead of "1234", the average error rate is 25%. Similarly, when users input all four digits correctly but apply wrong pressure level on one of the keys, the average error rate is still 25%. This metric considers a tap, and the pressure level associated with it, as a single operation. It does not account for users' error correction efforts.
- **Match Rate (%):** This denotes the average percentage of passwords that were correctly inputted (i.e. matched with the recorded password).
- **Keystrokes per Character (KSPC):** This denotes the average number of taps required to input a digit [1].

4.5 Design

We used a within-subjects design, where the independent variables were the two investigated techniques. In summary, the design was:

12 participants ×
2 conditions (*new* and *digit-lock*, *counterbalanced*) ×
Password selection (*15 input attempts*) +
5 blocks × 10 input attempts each
= 1,560 input attempts, in total.

4.6 Results

Anderson-Darling tests on the dependent variables confirmed that the data were normally distributed. Also, a Mauchly's test confirmed that the data's covariance matrix was circular in form. Therefore, we used repeated-measures ANOVA for all analysis. A Chi-Square test was used to analyse the nonparametric questionnaire data.

4.6.1 Entry Speed

An ANOVA revealed that there was a significant effect of technique on entry speed ($F_{1,11} = 39.91$, $p < .0001$). The average entry speeds for the digit-lock and the pressure-based techniques were 1.62 (SE = 0.1) and 2.46 seconds (SE = 0.1), respectively. Figure 4 illustrates this. There was no significant effect of technique × block ($F_{4,44} = 0.31$, ns).

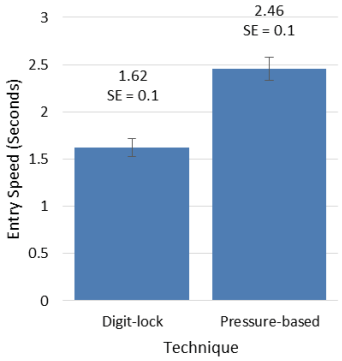

Figure 4. Average entry speed (seconds) for both techniques. Error bars represent ±1 standard error.

4.6.2 Error Rate

An ANOVA revealed that there was a significant effect of technique on error rate ($F_{1,11} = 22.96$, $p < .001$). The average error rates for the digit-lock and the new techniques were 0.57 (SE = 0.2) and 8.8% (SE = 1.6), respectively. Figure 5 illustrates this. There was no significant effect of technique × block ($F_{4,44} = 2.18$, $p = .09$).

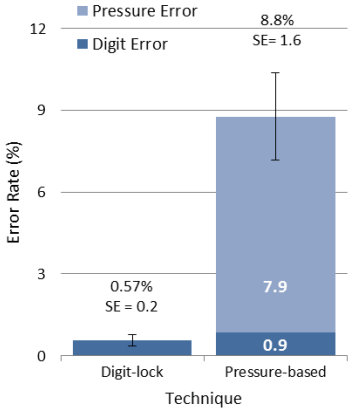

Figure 5. Average error rate (%), separated by pressure and digit errors, for both techniques. Error bars represent ±1 standard error.

Further analysis on the data from the *new* condition revealed that incorrect pressure input caused significantly more errors (90%) than incorrect digit input (10%). Although, there was no significant effect of technique × block, on average the last two blocks of the new technique were more error-prone than the first three. In Figure 6 one can see that the new technique got more error-prone with time. No such trend was observed for the digit-lock technique.

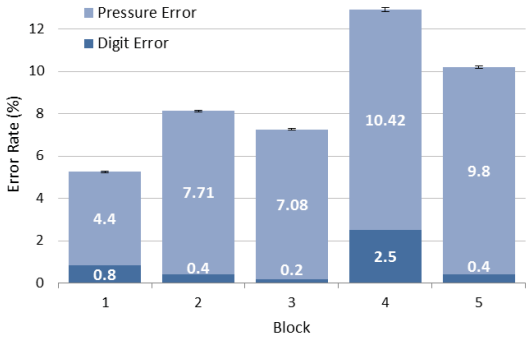

Figure 6. Average error rate (%), separated by pressure and digit errors, in each block for the new techniques. Error bars represent ±1 standard error.

4.6.3 Match Rate

An ANOVA revealed that there was a significant effect of technique on match rate ($F_{1,11} = 38.06$, $p < .0001$). The average match rates for the digit-lock and the new techniques were 98 (SE = 0.7) and 72.7% (SE = 3.7), respectively. See Figure 7. There was also a significant effect of technique × block ($F_{4,44} = 2.82$, $p < .05$).

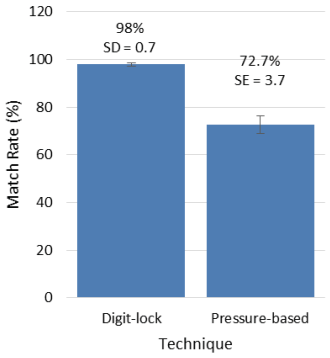

Figure 7. Average match rate (%) for both techniques. Error bars represent ±1 standard error.

A Tukey-Kramer multiple-comparison test revealed that the last two blocks of the new technique yielded significantly less match rates than the first block. This is also apparent in Figure 8, where one can see that the average match rate for the new technique decreased with time. No such trend was observed for the digit-lock technique.

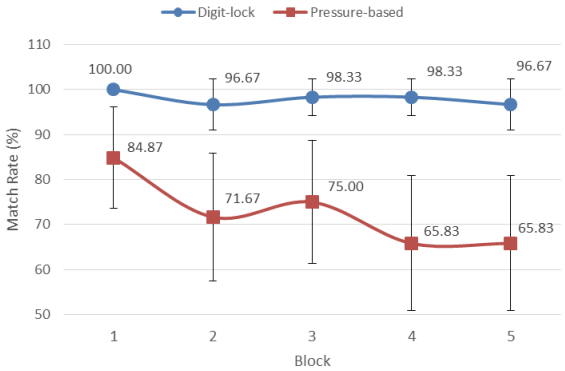

Figure 8. Average match rate (%) by block for both techniques. Error bars represent ±1 standard error.

4.6.4 Keystrokes per Character (KSPC)

An ANOVA failed to find a significant effect of technique on KSPC ($F_{1,11} = 0.08$, ns). The average KSPC for the digit-lock and

the new techniques were 1.01 (SE = 0.007) and 1.02 (SE = 0.009), respectively. Figure 7 illustrates this. Also, there was no significant effect of technique × block ($F_{4,44} = 0.51$, ns).

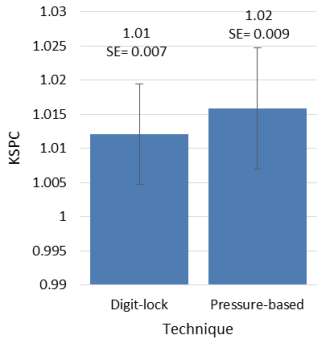

Figure 9. Average Keystrokes per Character (KSPC) for both techniques. Error bars represent ±1 standard error.

4.7 User Evaluation

Upon completion of the study participants responded to a questionnaire on seven-point Likert scales. Some of the scales were later converted to three-point scales using linear transformation to calculate ratios (%). That is, all ratings below four on the seven-point scale were mapped to one, all fours to twos, and all ratings above four to three. Some responses were converted to binomial data. That is, everything above four was rated as *accept* and below four as *reject* or vice versa depending on the phrasing of the question. Ratings of four were disregarded. Such mappings are common practice in statistics [11].

4.7.1 Sense of Security

Participants were asked how secure they would feel using the new technique compared to the one they use on their devices. Substantially more users responded that they would feel more secure using the new technique (75%) compared to those who were impartial (17%) or would feel less secure (8%). See Figure 10. A Chi-squared test found this to be statistically significant ($\chi^2_{(2)} = 9.5$, $p < .01$).

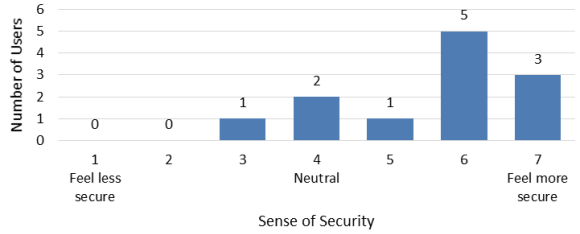

Figure 10. User feedback on how secure they would feel using the new technique compared to the one they use on their devices, on a seven-point Likert scale.

4.7.2 Willingness to Use

Participants were asked whether or not they would use the new technique as their dominant user authentication method on their mobile devices. 50% users responded that they would use the new technique dominantly, while about 33% said that they would not, and the remaining 17% were neutral. See Figure 11. A Chi-squared test did not identify a significant difference between these three groups ($\chi^2_{(2)} = 2.0$, $p = .37$).

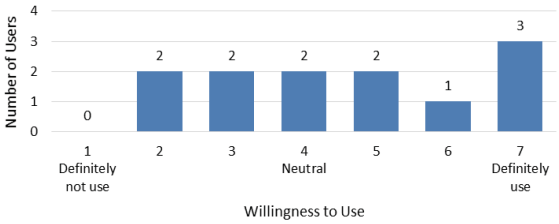

Figure 11. User feedback on whether or not they would use the new technique dominantly on their devices, on a seven-point Likert scale.

4.7.3 Ease of Use

Participants were asked how easy they found the new technique to use, in terms of usability and physical comfort, compared to the technique they use on their mobile devices. Substantially more participants responded that they found the new technique easy to use (67%) compared to those who were neutral (8%) and found the new technique more difficult to use (25%). See Figure 12. A Chi-squared test found this to be statistically significant ($\chi^2_{(2)} = 6.5$, $p < .05$).

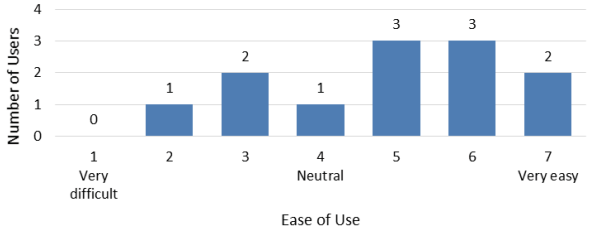

Figure 12. User feedback on how technically and physically easy they found using the new technique, on a seven-point Likert scale.

4.7.4 Perceived Pressure Detection Accuracy

While asked about how accurate they thought the pressure detection simulation approach was, about 33% participants responded that they found it to be accurate, 33% found it to be error-prone, while the remaining 33% were neutral. See Figure 13. A Chi-squared test failed to find significance regarding this ($\chi^2_{(2)} = 6.5$, $p < .05$).

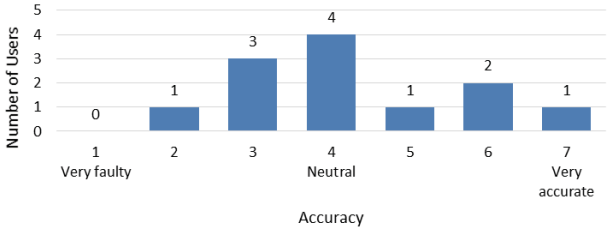

Figure 13. User feedback on how accurate they thought the pressure detection simulation approach was, on a seven-point Likert scale.

4.7.5 Memorability

Participants were asked whether it was difficult for them to memorize a pressure-based PIN. About 92% user responded that it was easy to remember the PINs, while 8% found it somewhat difficult. See Figure 14. A Chi-squared test found this to be statistically significant ($\chi^2_{(2)} = 18.5$, $p < .0001$).

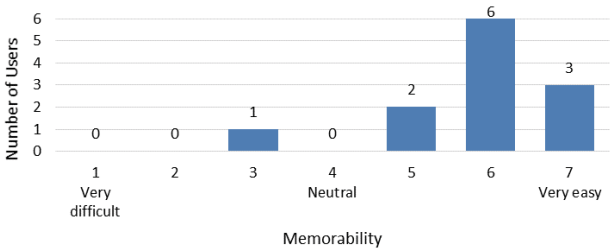

Figure 14. User feedback on how difficult it was for them to memorize a pressure-based PIN, on a seven-point Likert scale.

4.8 Password Selection Process

About 58% participants used the same digit sequence with the two techniques, while the others used minor variations, such as "1123" instead of "1223". About 58% users responded that they picked a password because it formed an *easy-to-remember* or *easy-to-enter* pattern on the virtual keypad. About 33% users used mnemonics, such as the last four digits of their parents' home phone number. The rest picked their password for superstitious reasons, such as their lucky numbers. A Chi-squared test failed to identify a significant difference between these different password selection criterion ($\chi^2_{(2)} = 4.5$, $p > .05$).

Further investigation revealed that users usually use three different patterns while selecting a PIN. A *left-to-right* PIN starts from the digits on the left column of the keypad, and then extends towards the other two. A *vertical* PIN is composed only of the digits on the middle column. Finally, a *right-to-left* PIN starts from the right column, and then expands towards the other two. Examples are "1569", "2280", and "9657", respectively.

50% participants picked a left-to-right PIN, 25% picked a vertical PIN, while the remaining 25% picked a right-to-left PIN. A Chi-squared test failed to find a significance regarding this ($\chi^2_{(2)} = 1.5$, $p > .05$). While handedness may have an effect on this, we did not have enough data to test this hypothesis, as 83% of our participants were right-handed.

However, we failed to find any pattern in pressure level selection. About 58% users picked only one key with extra pressure, 25% picked two keys, while the remaining 17% picked three keys with extra pressure. A Chi-squared test failed to identify a significance regarding this ($\chi^2_{(2)} = 3.5$, $p > .05$).

4.9 Discussion

Results showed that users took significantly more time to input PINs with the new technique. This was anticipated as we specifically asked users to apply *extra* pressure on one or more keys. The reason for this was discussed and justified in Section 3.5.3. One may speculate that entry speed would improve when users apply low or regular pressure on the keys. However, we do not have enough data to support this hypothesis. The pressure-based technique was also more error-prone than the conventional technique. A deeper investigation revealed that users mostly made mistakes in inputting extra pressure.

An ANOVA failed to find a significant effect of technique ×block on accuracy. However, one can see in Figure 8 that the new technique gradually became more error-prone, while the performance of the conventional technique remained indifferent. This is mainly due to fatigue, as applying extra pressure becomes more difficult with time. User responses during the post-experiment interview session also supported this. Initially most users found the new technique easy to use, however, many complained that inputting pressure for extended period of time compromised their performance. For instance, one female user (18 years) commented, "[Repetitive pressure input] is not as comfortable as regular input."

Results showed that there was no significant difference in terms of keystrokes per characters (KSPC). This suggests that both techniques require pretty much the same effect for error correction.

Relevant to our work, De Luca et al. [12] developed and evaluated a new pressure-based technique that integrated touch coordinates, touch pressure, and touch area with the pattern-lock technique. In their long-term evaluation, they asked participants to input pressure-based patterns only once a day for three consecutive weeks. Results found their technique to be 77% accurate. Our technique yielded a better accuracy rate (85%) in the first block. However, as we tested our technique in a lab setting, the accuracy rate may reduce in some real-world scenarios, such as while walking. Accuracy may also decrease when users decide to use a different finger or position to input the PIN. Yet it may be possible to compensate for extraneous movement while walking or commuting by using the device's built-in tri-axis accelerometer [14] and update pressure thresholds based on the position of the fingers or the device.

In Section 3.2 we made a point that *active* pressure input should be more accurate than *passive*, because the former will generate less false positives and false negatives. Also, if users do not know about the *pressure detection*, they will be less careful about the amount of pressure they apply on the keys. This will cause more system errors. This may also confuse users when the system rejects a correctly inputted PIN due to the use of different pressure levels on the keys. To explore this matter further, we recorded the amount of pressure applied on the keys while inputting PINs with the conventional technique (i.e. passive pressure input). We wanted to investigate whether users apply the same amount of pressure on the keys throughout the study (when they do not know about the *pressure detection*) to predict the false negative rate for passive pressure. Results showed that on average 27% input attempts in the first block with passive pressure would have caused false negatives. As assumed, this is substantially more compared to the false positive rate for active pressure input (from 0% to 15%).

Users generally liked the new technique. Almost all users stated that they would feel more secure using the new technique. Also, majority of them wanted to use the new technique dominantly on their touchscreen-based devices. Many praised the pressure-based approach in the comment section of the questionnaire. For example, one male participant (26 years) wrote, "The extra level of security is great". Many made enthusiastic remarks such as "Cool" or "Great!" A number of Android device users also enquired whether they could download the application from Google Play.

The percentages of participants, who perceived the pressure detection simulation approach as accurate, fair, or erroneous, were equally distributed. Nevertheless, many were excited to discover that it is possible to detect different pressure levels on smartphones. One female participant (19 years) commented, "It was interesting to see that a phone could tell how much pressure someone applies to the screen!"

Several participants wanted to have visual feedback on different pressure levels, such as in a progress bar. They thought this would enhance their overall PIN entry performance. We initially decided against this considering bystanders observing the users (see Section 4.3). However, it may be beneficial to provide the users with visual feedback during the PIN selection process. This might give them a better awareness of the amount of pressure they are applying on the touchscreen, and consequently, maintain the same level of pressure during PIN entry.

Another option was to vibrate the device in relation to the amount of pressure applied on the touchscreen. In other words, the device vibrates more when extra pressure is applied. We did not use this approach based on a prior research that showed that tactile feedback close to 46 mA drive current for the piezo actuator and 16ms drive time for the vibration motor create the most pleasant tactile feedback [22]. In other words, vibrating the mobile device harder may cause users discomfort.

5. User Study 2—Security

This user study consists of two parts. The first part investigates whether the new technique is less prone to smudge attacks than the conventional technique. The second part investigates, whether it is less vulnerable to situations where attackers are already in possession of users' passwords.

5.1 Apparatus

We used a Symphony Xplorer W60, 122×65×9.9 mm, 120 g and a Samsung Galaxy S III, 136.6×70.6×8.6 mm, 133 g, during the user study. We also used a jumpstart LED desk lamp, an 18″ black light, and two transparent sheets with the tracings of the two devices' lock-screens, see Figure 15. The second part of the study used the same apparatus as the first user study.

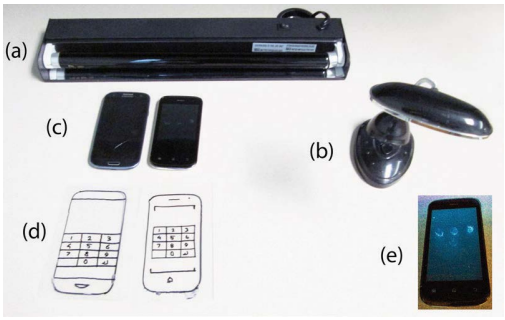

Figure 15. Instruments used during the second study: (a) black light, (b) jumpstart LED lamp, (c) Samsung Galaxy S III and Symphony Xplorer W60, (d) transparent sheets with tracings for the above mentioned devices, and (e) in the inset illustrates how smudges often glow under black light.

5.2 Participants

Thirteen participants, aged from 19 to 34 years, mean 24.31 (SD = 4.81), participated in the user study. They were recruited through online communities, local university emailing lists, and by word of mouth. Six participants were female. One of the participants was left-handed and one was ambidextrous. All were frequent touchscreen users, that is, owned and used a touchscreen-based device for on overage four years. None of them were expert in mobile security.

5.3 Procedure and Design

During the first part of the user study participants tried to retrieve passwords by studying the smudges left on touchscreens. A prior study showed that in about 68% of the cases it is possible to retrieve touch patterns by studying the smudges on the touchscreens [4]. This rate increases if the device was in contact with the face prior to touch interactions. During the study we tried to replicate the latter scenario. Towards that, the experimenter held the devices to his right ear, in contact with his face, for about ten seconds. Then, he entered two different PINs using both regular and extra pressure on the two devices. We replicated this scenario, as we wanted to investigate whether users are able to guess a pressure-based PIN when they are provided with the most optimal setting for PIN retrieval.

The experimenter washed his hands before inputting the password on the Galaxy S III (standard hand), but applied a popular hand moisturizer before inputting the password on the Xplorer W60 (moisturized hand). The password picked for the first device was 1682 that followed a left-to-right pattern, while the one picked for the second device 3251 that follow a right-to-left pattern. The underlined digits represent the keys that were inputted with extra pressure.

The user study took place in a dark room, where participants were provided with a jumpstart LED table lamp and two transparent sheets with tracings of the two devices' lock-screens. They were also provided with an 18″ black light, as many hand moisturizers glow under UV-A. See Figure 15 (e). Both devices were available to them at the same time. Thus, they could work on either one device at a time or both devices simultaneously.

They were asked to study the smudges under the dark light and/or the LED lamp using different angels, positions, or any other approach that they would use to guess a right-handed user's PIN. They were asked not to touch the touchscreens, as we used the same devices with all participants. They were, however, allowed to place the transparent sheets on the touchscreens to correspond the smudges to the devices' virtual keypads. See Figure 16.

Each participant made ten guesses per condition, by writing down the first ten PINs they would try to unlock the devices in a paper form. At this time, they were unaware of the fact that the PINs were inputted using the pressure-based technique. Thus, they guessed only the digits and the sequence in which they appeared.

Figure 16. A user trying to guess a PIN by studying the smudges left on the touchscreen during first part of the second user study.

During the second part of the study, we demonstrated the pressure-based technique to the participants. Then, they were asked to practice inputting a self-picked pressure-based PIN with the custom application for at least fifteen times.

We then provided them with the PIN that was used with the Samsung Galaxy S III, but without the digits' corresponding pressure levels. We asked them to restudy the smudges and try to guess the pressure levels by inputting the PIN with the custom application and the device used during the first user study for ten times.

The intention was to examine if users can guess the pressure levels by examining the smudges, when they already know the digits and the sequence in which they were inputted. Note that, we asked them to guess and input only the left-to-right PIN, because results of the first study showed that most participants prefer such PINs.

5.4 Results

As the user study data were nonparametric, we used a Wilcoxon Signed-Rank test for the following analysis.

5.4.1 Retrieving the Digits

About 85% participants were able to correctly guess the four digits with the standard input state. The remaining 15% were able to guess at least three of the four digits. However, all participants (100%) were able to guess the four digits with the moisturized state. A Wilcoxon Signed-Rank test failed to find a significant difference between the two conditions ($z = -1.414$, $p > .05$).

5.4.2 Digit Sequences

About 46% participants were able to accurately guess the digit sequence for the left-to-right password, while about 23% participants were able to guess the digit sequence for the right-to-left password. A Wilcoxon Signed-Rank failed to find a significance difference between the two groups ($z = -1.134$, $p > .05$). However, when compared with the success rate for the right-to-left PINs, a Chi-squared test revealed that significantly more users were successful in guessing the digit sequence for the left-to-right password ($\chi^2_{(1)} = 3.9$, $p < .05$).

5.4.3 Pressure Levels

About 30% participants were able to accurately guess the pressure levels. Yet, when asked to re-enter the password with the same pressure levels, only 8% users were able to do so. A Chi-squared test revealed that pressure retrieval rate for the PIN was significantly lower than its digit retrieval rate ($\chi^2_{(1)} = 28.96$, $p < .0001$). However, no significant difference was identified when compared with the PIN's sequence retrieval rate ($\chi^2_{(1)} = 2.79$, $p = .09$).

5.5 Discussion

Results showed that almost all users were able to guess the digits by studying the smudges with both input states, i.e. standard and moisturized. Yet, significantly more users were able to guess digit sequence for the left-to-right password than the right-to left one. This may be because most of our participants were right-handed (85%), who usually prefer left-to-right patterns. User responses on the strategies they used to guess the sequences also supported this. About 70% of users responded that they tried to organize the digits in sequences that they would feel comfortable using on their devices, while the remaining 30% used random selection.

Participants were significantly less successful in retrieving pressure levels. About 30% of them managed to retrieve the pressure levels, and only 8% of them were able to maintain that pressure level in the following attempts. This indicates towards the possibility that these users managed to apply the right level of pressure by chance. This also verifies our hypothesis that it is more difficult to retrieve pressure-based passwords. Note that during the study participants were provided with the correct digit sequence, thus, only had to salvage the pressure levels. In practice, it would be even more difficult to retrieve pressure-based passwords, as that would require guessing or retrieving the both.

6. Conclusion

This article presented a new pressure-based technique for authenticating smartphone users. It allows user to *actively* pick the level of pressure on each digit key. When authenticating a user the system compares both the pressure levels and the key sequences of a PIN, and unlocks the device only when both of these parameters match. Theoretically, the new technique can offer from 160,000 to 24,010,000 unique four-digit password combinations using two to seven pressure levels, compared to digit-lock's 10,000 and pattern-lock's 389,112.

A user study comparing the new and the most popular digit-lock technique showed that the new technique was relatively slower and more error-prone, mainly because its performance reduced with time due to fatigue. Consequently, it performed substantially better in the first block and yielded a better result than a similar pressure-based approach. This suggests that the new technique is more suitable for short-term usage. User feedback revealed that most users felt more secure while using the new technique and wanted to use it dominantly on their touchscreen devices. Most of them did not find it difficult to memorize and use a pressure-based PIN.

A subsequent study confirmed that compared to the digit-lock technique the new technique is less prone to smudge attacks and less vulnerable to situations where attackers are already in possession of users' passwords.

7. Future Work

In this paper we investigated the new pressure-based technique's security in terms of smudge attack and situations where an attacker is already in possession of the user's PIN. We, however, did not test the technique's resistance to shoulder surfing. Although, in theory it should be more difficult to guess the amount of pressure applied on a key just by observing the user, in the future we plan on conducting a user study to validate this hypothesis.

We also plan on improving the pressure detection simulation approach by utilizing readings form the sensors available on most smartphones, such as microphone, gyroscope, and accelerometer. Some attempted to utilize these sensors for pressure detection [15, 17], but not in collaboration with the time and touch-point-based hybrid approach. We believe the proposed user authentication technique can be further improved by using correction models to compensate for extraneous movement while walking, commuting, etc. by using the device's inertial sensors [14]. We would like to explore this idea further and conduct a user study to test the improved technique in real-world scenarios.

We evaluated our technique only in the portrait position, as mobile users use it most frequently [16]. Yet, in the future, we would like to test it in landscape position as well. Also, our approach did not account for scenarios where users use a different hand or finger to input PINs. We would like to further improve our technique to address such situations.

In the future, we would like to provide the users with visual feedback on pressure input during the PIN selection phase. The intention would be to investigate whether this improves the performance of the new technique. We would also like to use vibration as a form of haptic feedback, such as the device will vibrate more with more pressure. Initially, we did not use this approach as vibration often causes discomfort [22]. However, we would like to investigate the effect of this in a pilot study.

It is possible to reduce system errors by fine-tuning the pressure thresholds. This, however, would require the collection of more data, which will reduce the immediate usability of the technique. One solution to this dilemma is to keep collecting data while users are using the technique. We would like to explore this idea in the future.

8. ACKNOWLEDGMENTS

We would like to thank SSHRC for funding this project and Marie Crosta for helping us with participant recruitment.

9. REFERENCES

[1] Arif, A. S. and Stuerzlinger, W. Analysis of text entry performance metrics. *TIC-STH '09*, IEEE (2009), 100-105.

[2] Arif, A. S. and Stuerzlinger, W. Pseudo-pressure detection and its use in predictive text entry on touchscreens. *OzCHI '13*, ACM (2013), 383-392.

[3] Arif, A. S., Pahud, M., Hinckley, K., and Buxton, B. A tap and gesture hybrid method for authenticating smartphone users. *MobileHCI '13*, ACM (2013), 486-491.

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

[5] Biddle, R., Mannan, M., Van Oorschot, P. C., and Whalen, T. User study, analysis, and usable security of passwords based on digital objects. *IEEE Transactions on Information Forensics and Security 6*, 3 (2011), 970-979.

[6] Bo, C., Zhang, L., Li, X., Huang, Q., and Wang, Y. SilentSense: Silent user identification via touch and movement behavioral biometrics. *MobiCom '13*, ACM (2013), 187-190.

[7] Cechanowicz, J., Irani, P., and Subramanian, S. Augmenting the mouse with pressure sensitive input. *CHI '07*, ACM (2007), 1385-1394.

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

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

[10] Davies, D. W. and Price, W. L. Security for computer networks: An introduction to data security in teleprocessing and electronic funds transfer. John Wiley & Sons, 1989.

[11] Dawes, J. Do data characteristics change according to the number of scale points used? An experiment using 5-point, 7-point and 10-point scales. *International Journal of Market Research 50*, 1, 2008.

[12] De Luca, A. D., Hang, A., Brudy, F., Lindner, C., and Hussmann, H. Touch me once and I know it's you! Implicit authentication based on touch screen patterns. *CHI '12*, ACM (2012), 987-996.

[13] De Luca, A., Denzel, M. and Hussmann, H. Look into my eyes! Can you guess my password? *SOUPS '09*, ACM (2009), 7:1-12.

[14] Goel, M., Findlater, L., and Wobbrock, J. WalkType: using accelerometer data to accomodate situational impairments in mobile touch screen text entry. *CHI '12*, ACM (2012), 2687-2696.

[15] Heo, S. and Lee, G. Forcetap: Extending the input vocabulary of mobile touch screens by adding tap gestures. *MobileHCI '11*, ACM (2011), 113-122.

[16] Hoober, S. How do users really hold mobile devices? UXmatters. 2013. Mar. 8, 2013. http://shar.es/N0Vxw

[17] Hwang, S. and Wohn, K-Y. PseudoButton: Enabling pressure-sensitive interaction by repurposing microphone on mobile device. *Ext. Abstracts CHI '12*, ACM (2012), 1565-1570.

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

[19] Jansen, W. Authenticating mobile device users through image selection. *The Internet Society: Advances in Learning, Commerce and Security 1*, (2004), 183-194.

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

[21] Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J. W., Nicholson, J., and Olivier, P. Multi-touch authentication on tabletops. *CHI '10*, ACM (2010), 1093-1102.

[22] Koskinen, E., Kaaresoja, T., and Laitinen, P. Feel-good touch: finding the most pleasant tactile feedback for a mobile touch screen button. ICMI '08, ACM (2008), 297-304.

[23] Malek, B., Orozco, M., and El Saddik, A. Novel shoulder-surfing resistant haptic-based graphical password. *EuroHaptics '06*, Vol. 6. 2006.

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

[25] Mizobuchi, S., Terasaki, S., Keski-Jaskari, T., Nousiainen, J., Ryynanen, M., and Silfverberg, M. Making an impression: Force-controlled pen input for handheld devices. *Ext. Abstracts CHI '05*, ACM (2005), 1661-1664.

[26] Multiplying Mobile: How Multicultural Consumers Are Leading Smartphone Adoption. Nielsen. Mar. 04, 2014. http://shar.es/N0VNj

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

[28] Pedersen, E. W. and Hornbæk, K. Expressive touch: Studying tapping force on tabletops. *CHI '14*, ACM (2004), 421-430.

[29] Pons, A. P. and Polak, P. Understanding user perspectives on biometric technology. *Communications of the ACM 51*, 9 (2008), 115-118.

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

[31] Rokita, J. Krzyzak, A., and Suen, C.Y. Cell phones personal authentication systems using multimodal biometrics. *ICIAR '08*, Springer (2008), 1013-1022.

[32] Shahzad, M., Liu, A. X., and Samuel, A. Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it. *MobiCom '13*. ACM (2013), 39-50.

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

[34] Smart Phone Thefts Rose to 3.1 Million Last Year, Consumer Reports Finds. Consumer Reports. May 28, 2014. http://www.consumerreports.org/cro/news/2014/04/smartphone-thefts-rose-to-3-1-million-last-year/index.htm

[35] Sonkamble, S., Thool, R., Sonkamble, B. Survey of biometric recognition systems and their applications. *Journal of Theoretical and Applied Information Technology 11*, 1 (2010), 45-51.

[36] Weiss, R. and De Luca, A. PassShapes: Utilizing stroke based authentication to increase password memorability. *NordiCHI '08*, ACM (2008), 383-392.

[37] Zheng, Z., Liu, X., Yin, L., and Liu, Z. A strokebased textual password authentication scheme. *ETCS '09*, IEEE (2009), 90-95.