PRESSURE-BASED AUTHENTICATION: A SECURE AND USABLE APPROACH

A Thesis
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Zhangyu Meng

In Partial Fulfillment of the Requirements
for the Degree of
MASTER OF SCIENCE

Major Department:
Computer Science

August 2018

Fargo, North Dakota

North Dakota State University
Graduate School

Title

Pressure-Based Authentication: A Secure And Usable Approach

By

Zhangyu Meng

The Supervisory Committee certifies that this ***disquisition*** complies with North Dakota State University's regulations and meets the accepted standards for the degree of

MASTER OF SCIENCE

SUPERVISORY COMMITTEE:

Jun Kong
Chair

Pratap Kotala

Ying Huang

Approved:

8/21/2018
Date

Kendall Nygard
Department Chair

ABSTRACT

Due to its invisibility feature, pressure force is useful to enhance the security of authentication, especially preventing shoulder surfing. However, it is challenging to memorize a pressure-based password. This paper presents a pressure-based authentication system with personalizing the detection of pressure force, which concretizes a pressure-based password as a decimal number to reduce the effort of memorization, improve the accuracy, and enhance the security. We conducted two user studies to compare the four-pin password with our pressure-based password regarding their usability performance and security evaluation. The results of the first study indicated that the pressure-based password is more secure, but the four-pin password is faster and has higher subjective satisfaction. We have conducted a second study that asked participants to use the pressure-based password once every day for 10 continuous days. The second study revealed that both the completion time and subjective satisfaction of the pressure-based password were significantly improved.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

Smartphones have become pervasive in daily life, and much sensitive data is stored in a personal smartphone. Therefore, authentication is essential to access a smartphone. However, traditional usernames and passwords are not user friendly in mobile interaction since a smartphone lacks a large tactile keyboard, which makes data entry tedious and error prone. Lock pattern replaces typing with drawing, and thus improves the usability of mobile interaction. However, lock pattern is vulnerable to smudge attack that analyzes the reflective properties of oily residues [Avi10]. Furthermore, both username/password and lock pattern suffer from shoulder surfing, which limits their usage in a public environment.

Recently, biometric authentication schemes (e.g., fingerprint or face ID) have been applied to mobile applications. In general, biometric authentication requires some specialized sensor, which is not available on all types of mobile devices, especially low-end smartphones. In addition, security concern increased since the biometrics hacking team of the Chaos Computer Club (CCC) has successfully bypassed the biometric security of Apple's TouchID [Fra13].

With the fast development of pressure-enabled sensors, pressure force provides an alternative solution to enhance the security of authentication. It especially mitigates the shoulder surfing due to its invisible feature. For example, Force-PINs [Kro16] combined pressure force with the traditional four-digit PINs, and showed that pressure force can reduce the risk of shoulder surfing. However, pressure-based passwords raise two challenging issues. First, unlike traditional passwords that are represented with a detailed sequence of character and number, pressure force itself is invisible and abstract, which increases the memory load to memorize a pressure-based password. Second, users can have different habits when pressing a touchscreen. A user may simply press lighter than another user. Therefore, instead of using a constant threshold to determine a deep

or shallow pressure force, adjusting the threshold for each user can fit a user's individual pressure habit and thus improve the detection accuracy.

In order to address the above two issue, this research developed a usable and secure pressure-based authentication system, in which a pressure-based password refers to a sequence of deep/shallow pressure force levels. Our approach is distinct from other approaches, with the following features:

- **Easy to Memorize**. Pressure is invisible and thus enhances the security. However, it is challenging to memorize a sequence of pressure force levels. Since a deep or shallow pressure force can be naturally mapped to a binary number of 1 or 0, respectively, our approach therefore instantiates the sequence of pressure force levels as a sequence of binary bits. However, people without a computer background in general do not understand binary bits. Our approach further converts a sequence of binary bits to its equivalent decimal number that is used in daily life. In summary, in our approach, a user defines a pressure-based password as a decimal number, whose equivalent binary bits indicate the sequence of different pressure force levels. For example, if a user chooses decimal number 6 as a four-bit pressure-based password, the sequence of pressure force levels is defined "Shallow Deep Deep Shallow", which is consistent with the binary sequence of decimal number 6.
- **Personal Detection of Pressure Force**. In order to fit each user's pressure habit, our approach builds a personal model for each individual user to detect his/her pressure force. A user starts with a training process for collecting the personal pressure-sensitive data. Based on the training, a personalized pressure model is calculated and built. The personalized detection address the diversity issue of pressure habits and thus improves the detection accuracy. Personalization also enhances the security. Even a pressure-based

password is compromised, but the attacker's input may not pass the authentication due to a different pressure habit.

- **Backward Compatibility**. The pressure sensor is not available in all types of smartphones. In order to apply our approach to both high- and low-end smartphones, our approach combines the readings of pressure (if applicable), pressing duration, and pressing size to detect a pressure level. Therefore, our approach is even applicable to touchscreens without a pressure sensor, which can derive the pressure force through pressing time and size.

In summary, our approach mapped a sequence of different pressure force levels to a decimal number, which facilitates users to memorize the pressure password. A personalized detection further improved the security since an attacker's input must be consistent with the user's pressure habit.

In order to evaluate the security and usability, we conducted a serial of user studies to compare the traditional four-pin password with our pressure based password. The evaluation results of the first study indicated that the pressure based password was more secure than the four-pin password. On the other hand, the four-pin password was faster and easier to remember than the pressure based password. Since the participants were the first to use the pressure based password, the low completion time and low memorability may have been caused by the first time usage. Therefore, we conducted a second study, which asked participants to use the pressure based password once every day for 10 continuous days. The comparison between the first and last days indicated that both the completion time and the memorization of the pressure-based password were significantly improved.

The remainder of the paper is structured as follows. Section 2 reviews the related work. Section 3, we introduce the concept of concept of our pressure-based-password and describe the

goal an objective of our work. In section 4 and 5, we discuss the two design of the comparative user studies, and analyzes the evaluation results. Section 6 discusses the conclusion to conclude our findings and future work.

2. RELATED WORK

Pressure based password on mobile device has been studied on iPhones with 3D touch technique. Krombholz et al. proposed the Force-Four-Pin on iPhone to combine the normal Four-Pin with pressures on each digit and they simply use a static threshold which is 0.5 to indicate the pressure levels[Kro16]. Furthermore, they evaluated their approach against the shoulder-surfing attack model. Saevanee et al. proposed a authentication system using keystroke dynamic and finger pressures they are using the pressure data from touchscreen but also use the static threshold of the pressure level [Sae09]. Compared to their research, we are using the dynamic threshold to indicate the pressure levels, we applied the machine learning approach to identify the deep/shallow press, different from their force-four-pin combine pressure and digits, we only take the pressure levels to authenticate the users.

Stewart et al. studied the characteristics of pressure -based input for mobile devices and they are evaluating the external pressure input devices. They found that that non-visual pressure input can be executed without degradation in selection time but suffers from accuracy problems [Ste10]. In addition, Clarke et al. proposed a biometric authentication system for mobile devices by using the latency of keystroke and the hold time duration as the inputs to classify the different users [Cla06]. They focused on the device with the small keypad like PDAs which is hard to get the pressure data from the user inputs. Also, they conducted a user study and proved the feasibility of the biometric data can increase the security of the mobile device. Ali et al. proposed a keystroke pressure based typing biometrics authentication system on physical keyboard [Ali09]. They implemented artificial neural-network (ANN) and adaptive neuro-fuzzy inference system (ANFIS) based classifiers to identify the authorized and unauthorized user. As the development of touch screen technology, pressure data can be collected from the touch screen interaction on the mobile

phone nowadays, so we focus on the pressure based authentication on mobile devices with touch screen, so we can get the pressure data from the touch screen feedback, and combine the pressure with duration and size of pressing as the composite key to authenticate the device. We implemented the system on the Android device with touch screen to calculate the data from touch screen feedback. Also, In their system, they adopted latency between consecutive keystrokes to combine with maximum pressure when user typing to be the features to classify the pressure levels. In our system, we adopted duration of the pressing and the pressing size to combine with the pressure to classify the actual pressure level.

As more and more existing authentication systems implemented the classification techniques to identify the users, implicit authentication is a new trending research topic in authentication area. Khan et al. showed that current implicit authentication methods have low real-world accuracy to replace knowledge based authentication systems, they evaluated the popular implicit authentication schemes found that combine the different data to build the classifier would improve the accuracy of the authentication system[Kha14]. Futhermore, Buschek et al. researched on the feasibility of mobile key stroke biometrics and found that this kind of data can be used for user authentication with low error rates [Bus15]. Chang et al. proposed a graphical-based password key stroke dynamic authentication system to combine the pressures with pictures for the pin entry, they applied the classification algorithms to detect the pressure levels, and they use the duration and pressure as the combination of the password[Cha12]. Orozco et al. proposed a haptic-based sensible graphical password to combine pressure and gesture as the password to authenticate the mobile device with touch screen. Their idea is to let user to connect specific nodes in a grid based unlock interface with finger press and record the pressure on the nodes. In addition, they implemented artificial neural network and nearest-neighbor algorithms to build the classifier

[Oro06]. Malek et al. combined the pressure inputs with graphical pattern password to be haptic-based sensible graphical password, and analyzed two classification algorithms—Artificial Neural Network and Nearest-Neighbor [Mal06], but they did not conduct within subject user study to evaluate the usability of their scheme. In addition, they did not prove the theoretical calculations of a larger password space by empirical evidence. This paper focused on the pressure conversion to make users easy to remember the pressure password, so we are using only one digital number as the password and use the binary conversion of the number to guide user to press heavily or lightly on specific buttons to record the data and use only pressing force to authenticate the device. We combined the pressure, size of touch area, and duration of the touch hold on the touch screen as the data to build the classifier to classify the user's behavior of deep or shallow press to distinguish the different users. Also, we applied 10 most popular classification algorithms at the first and select the most accurate one with lowest execution time based on the training data to be saved as the final classifier to individual user. Therefore, in our system, different user may have different classifier with the most applicable algorithm for the user's touch behavior.

Harbach et al. conducted a real-world study on mobile authentication and figured out that users take a significant of usage time on the unlocking process with PINs and unlock patterns. In their study, participants unlocked their phones around 47 times throughout the day on average. They found that mobile authentication time is a key factor regarding to the usability of authentication method [Har16]. In addition, De Luca et al. figured out that large authentication time was a reason for mobile users to stop using Android Face Unlock. They also proved that the key reason make users stop using biometric authentication methods is the usability concern and primary focus on the completion time [DeL15](1)(2). However, Krombholz et al. showed that more practices on the biometric authentication can reduce the completion time of unlocking

significantly [Kro16]. We conducted the pressure based password to achieve the low error rate with high accuracy to avoid the overhead for users to get to use the pressures in a short time period.

To avoid shoulder surfing, De Luca et al. proposed an authentication scheme which allows user to enter passwords at both the front and the back of the device [DeL13]. Even though their mechanism has the benefits of shoulder-surfing resilience, the limitation of it is there is no such device which has a touch-sensitive back to allow this kind of input now. Krombholz et al. did the experiment about the shoulder surfing concern and showed that the combination of pressure and digit can reduce the risk of the shoulder surfing attack on mobile device [Kro16]. Kim et al. introduce and evaluate a number of novel tabletop authentication schemes that exploit the features of multi-touch interaction in order to inhibit shoulder surfing, and they proved that pressure-based authentication scheme can reduce the visibility of the secret to an attacker [Kim10]. We also conducted a shoulder surfing attack experiment to expose all the unlock process to the user who is not legit user of the device, to evaluate the performance of the invisible pressure only password against the shoulder surfing attacks.

Smudge attack is a problem that attacker can discern the password pattern of the device with touchscreens. The oily smudges left on the touchscreen by the user's fingers when operating the device can be traced by the attackers especially from the pattern based authentication. Arif et al. studied the use of pseudo pressure in authenticating smartphones and proposed a authentication scheme to combine the pseudo pressure with PINs then proved the invisible pressure input can reduce the risk of smudge attack on the device with touchscreen. However, they only use the simple pressure threshold that without the personal classification technique [Arif14]. Our system is based on the implicit authentication that implemented the customized pressure detection model. Also, we did the similar experiment to test the false acceptance rate that expose the password to the

participants of our user study, and got a low false acceptance rate even the participants already known the passwords.

Weiss et al. studied on the memorability of mobile authentication, and found the increasing number of PINs and passwords led users to forget password and implied several security risks. They found most users have the experience to forget the knowledge based passwords, therefore they proposed a stroke based authentication method to increase password memorability and proved the shape is easier to remember [Wei08]. Tetsuji et al. proposed an image-based authentication system for mobile phones which using user's favorite images to help user remember the password. They talked about the difficulty of remembering the long text or digit based password is the issue of the existing popular authentication systems to ensure the security, they use the images instead of the texts or digits which are users can recognize easily to help the user to remember the password and enhance the security of the authentication[Tak03]. The key idea to increase the memorability of authentication methods is to convert the password to an easy to remember representation so they implemented the stroke based authentication which allows the user only needs to remember the shapes of gestures to unlock the device to reduce the memorability load. Compared to their work, we convert the pressure to binary digits of a certain digital number to reduce the memory load of the password for users to remember the password easily.

3. A PRESSURE BASED AUTHENTICATION SYSTEM

This section describes a personalized pressure based authentication system. On the other hand, invisibility also makes it challenging for users to memorize a pressure-based password. Since only a memorable password is useful, we concretize a pressure-based password as a digital number to facilitate the memorization. Furthermore, our approach is distinct from any other approach because building a personalized model to recognize a pressure force. The personalization makes our approach harder to compromise since an attacker's pressure must be consistent with the user's pressure habit.

The force used to press a touchscreen is invisible and can only be felt by the user. The invisibility nature of pressure makes it suitable to enhance security. Especially, it is hard for attackers of shoulder surfing to observe the entry of a shallow or deep press. However, pressure force is abstract and invisible, which makes it challenging for users to memorize a pressure-based password. In order to facilitate users to memorize a pressure-based password, our approach concretizes a pressure-based password as a digital number.

When classifying pressure forces into two levels (i.e., deep or shallow), it is natural to use the binary bit 0 to represent a shallow press and 1 for a deep press. Correspondingly, the sequence of pressure force levels in a pressure-based password can be concretized as a sequence of binary bits. For example, a pressure-based password with the sequence of pressure forces of "deep, deep, shallow, deep" can be concretized as a binary number of "1101". Then, the binary number can be further converted to a decimal number that users are familiar with. Accordingly, a pressure-based password can be defined as a decimal number, which is much easier to memorize than a sequence of abstract pressure force levels.

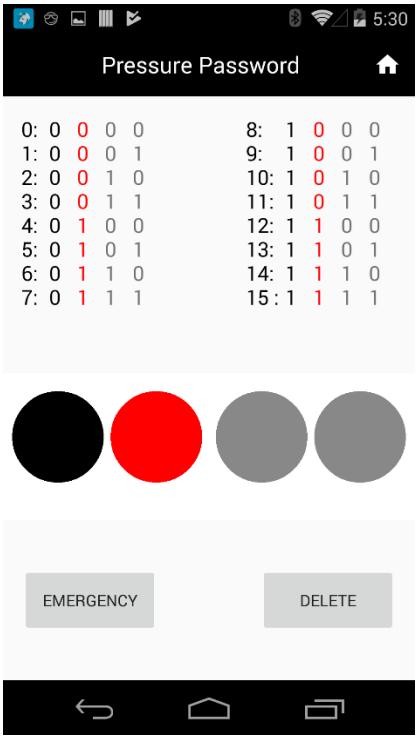

Figure 1. Concretizing a Pressure-based Password

In order to input a pressure-based password, a user needs to first convert a decimal number to its equivalent binary code and then sequentially press the touchscreen with an appropriate pressure force based on the binary code. However, it is not trivial to convert a decimal number to its equivalent binary code. In order to mitigate the effort of converting a decimal to binary, our approach divides the authentication interface into two areas, as shown in Figure 1. The top area displays a set of decimal numbers, including the decimal number defined by the user, and their corresponding binary codes. The bottom area presents a sequence of four circles that accept the user's pressure[1]. When inputting a password, a user skims the numbers displayed in the top area and recognizes the defined number. Its equivalent binary code guides the user to press the touchscreen sequentially with an appropriate pressure force. In order to minimize the risk of

[1] Without losing generality, the above example presents a four-bit pressure-based password.

leaking a defined password, the user defined number is randomly mixed with other unrelated numbers to make it hard for attackers to guess the defined number. Even if a defined number is comprised, a personalized detection model can further prevent an attacker from passing the authentication.

Our approach builds a personalized model to detect pressure force for each individual user because users have different pressure habits, where a constant threshold may not reflect the actual feeling for a pressure force of a specific user. For example, a user with great muscle strength probably performs a shallow press with more force than another user's deep press. In order to build the model, a user needs to complete a training process in the beginning by pressing the touchscreen 20 times, which includes both heavy and shallow presses in a predefined sequence. For each press, the system will collect three pieces of data, i.e., pressure force (if applicable), pressing size, and pressing duration. The information of pressing size and pressing duration is used to predict the pressure force when a touchscreen does not support a pressure-enabled sensor. Therefore, our approach is applicable to different types of touch screens, with or without a pressure sensor.

Based on the data collected during the training, we used the Weka[2] library to calculate a personalized model for each user. We chose 10 popular classification algorithms (see Figure 2) and used the cross-validation approach to selecting the one with the highest accuracy. Specifically speaking, 20 pressing data were collected and randomly divided into two groups, 15 to the training set and 5 to the test set. The training set was used to calculate a personalized model for each classification algorithm, and the test set to compare the 10 models to choose the one with the highest accuracy. If two models had the same accuracy, we chose the model with the shorter execution time. Then, the personalized model was used in the authentication to classify a user's

[2] https://github.com/rjmarsan/Weka-for-Android

pressure force. Since both the training data collection and the calculation of a personalized model are only performed once in the first time usage, our approach will not slow down the authentication speed.

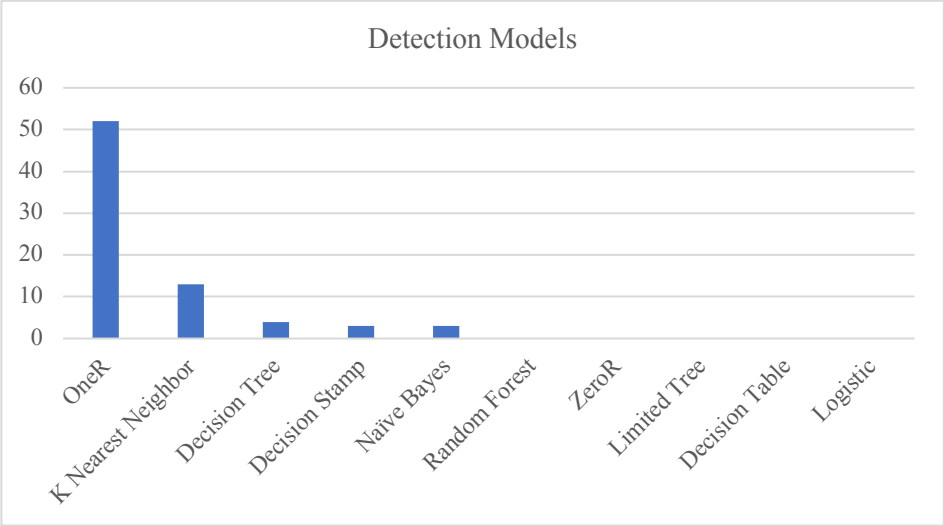

Figure 2. Classification Models

In Figure 2, the x-axis lists the 10 classification algorithms while the y-axis presents their corresponding successful rates adopted by users (i.e., the number of users using this model). Based on the data collected from 75 participants, the simple oneR algorithm is adopted by a majority of users, i.e., 52 out of 75 participants, which implies that pressure force can be predicted by one single predictor.

4. USER STUDY 1

This section describes a comparative study between a pressure-based password and a traditional four-pin password. This study focuses on the user experience for a first time user experience.

4.1. Research Hypotheses

Goal Question Metric (GQM) [Bas94] was used to define the goals for our study.

Goal 1: Analyze a pressure-based password and a traditional four-pin password for the purpose of their evaluation with respect to efficiency.

Hypothesis 1: There is no difference in efficiency between the two treatment methods.

Goal 2: Analyze a pressure-based password and a traditional four-pin password for the purpose of their evaluation with respect to error rate.

Hypothesis 2: There is no difference in error rates between the two treatment methods.

Goal 3: Analyze a pressure-based password and a traditional four-pin password for the purpose of their evaluation with respect to subjective feedback.

Hypothesis 3: There is no difference in subjective feedback between the two treatment methods.

Goal 4: Analyze a pressure-based password and a traditional four-pin password for the purpose of their evaluation with respect to security.

Hypothesis 4: The pressure-based password is more secure than the four-pin password.

4.2. Participating Subject

38 participants were recruited by email at a mid-west university for this experiment. There are 76.3% of participants identified themselves as males, and 23.7% as females. 86.8% of the participants were between 18 and 24 years old, 10.6% between 25 and 34 years old, and the

remaining 2.6% were 35 or older. There were 63.2% of participants that identified themselves as iPhone users, 42.1% as Android users, and 2.7% as Windows Phone users. Regarding the authentication method, a participant could choose multiple authentication methods he/she was using to access their phone. Among 38 participants, 36.8% were using 4-digit PINs as the password for their phones, 13.2% participants were using 6-digit PINs, 2.6% participant was using a character and digit password, 18.4% participants were using unlock patterns, 60.5% participants were using fingerprint identification, and 10.5% participants did not use any unlock method. In addition, 42.1% of participants had no knowledge of the 3D Touch technique, while 57.9% of participants used this technology.

4.3. Apparatus

Without losing generality, a Google Nexus 5 was used as the mobile device in our lab study. The Nexus 5 has a 4.7" high resolution touch screen. A smartphone without a pressure sensor is chosen to justify the backward feature of our approach, which can be applicable to different types of smartphones.

4.4. Experiment Design

The objective of this experiment was to compare the pressure-based password with the traditional pin-based password on mobile devices. Since the four-pin digital password was most commonly used to unlock a smartphone, it was selected as a benchmark in the experiment. In order to make a fair comparison with the four-pin password, the pressure-based password was limited to four touchscreen presses, which implies a decimal password number in the range of 0 to 15.

The study was conducted as a pretest-posttest, repeated-measures experiment. Participants were randomly divided into two invisible groups in order to minimize the learning effect of the treatment order. Each subject in group 1 first used the four-pin password, followed by the pressure-

based password. Conversely, each subject in group 2 used the authentication methods in the reverse order. This design allowed the researchers to minimize potential learning effects. Our study started with a pre-study questionnaire, followed by a training session. In the training, the participants were briefed about two treatment methods. Next, the participants were asked to define and input a user-defined password by using each method. At the end of each treatment method, the participants were measured for their subjective satisfaction utilizing the post-study questionnaire. The researchers also recorded the time it took the participants to complete each authentication and counted the errors when inputting a password. The experiment's operations included the following steps.

Step 1: *Pre-Study Survey*. The first step was to collect background information from the subjects regarding their reading-comprehension skills, their prior knowledge about mobile authentication. The information gathered during the pre-study was used to gain additional insight about the subjects' individual performances during the experiment.

Step 2: *Training*. Following the pre-study survey, the subjects were trained for an authentication method (i.e., pressure-based password or four-pin password), by the same researcher, prior to starting the study. In the pressure-based password, a user also pressed the touchscreen for 20 times with a predefined sequence of different pressure force levels to train a detection model.

Step 3: *Defining a Password*. The participants were asked to define a password with an authentication method. Since the number of key presses was limited to 4, a user could only define a number from 0 to 15 for the pressure-based password.

Step 4: *Inputting a Password.* In this step, a participant was asked to input the password he/she defined in the previous step. A participant had three chances to complete the password. If

a participant inputted a wrong password, he/she was asked to retype it until success or all the three chances were used up. The top area in a pressure-based password interface (See Figure 1) listed all of the 16 possible passwords and their corresponding binary codes. The bottom area presented four circles that accepted a user's presses sequentially. A black circle indicated a pressed button, a red circle indicated a button currently waits for a user's press, and a gray circle indicated a button to be pressed. Colored circles provided visual feedback for a user to highlight the current step in the sequence of presses.

Step 5: *Post-study Questionnaire*. After completing step 4, participants were asked to complete a post-study questionnaire to give their subjective feedback. Then, participants repeated steps 2 to 5 with the second authentication method.

Step 6: *Shoulder Surfing*. Shoulder surfing happens when an attacker is close to a user and able to observe the typing behavior of the user. In order to evaluate shoulder surfing, we invited four volunteers (two female and two male), who were neither the researchers nor participants of this study, to make 8 videos. Specifically speaking, each volunteer shot two videos, one using the pressure-based password and one using the four-pin password. Each video recorded the details when a volunteer pressed the touchscreen. Participants were asked to watch these 8 videos with a random order. After watching a video, a participant guessed the password and wrote it down on a piece of paper.

Step 7: *False Acceptance Test*. Participants were given a predefined pressure-based password and input this password using another user's detection model.

4.5. Data Collection

Both quantitative and qualitative data were collected from the study.

4.5.1. Quantitative Data

We recorded the completion time and error rate for each authentication method. The completion time was measured as the time duration from the first touch to the last touch for the authentication, and only successful authentication attempts were recorded. The error rate was distinguished to be either a basic error or a critical error. The basic error counted the false attempts, and the critical error was the number of the completely failed authentication sessions, i.e., the participant failed to input the password three times. In addition, we collected the number of correct guesses in the shoulder surfing evaluation and the false acceptance rate.

4.5.2. Qualitative Data

For qualitative data, we gathered the subjective, self-reported data during the pre-study survey and the post-study questionnaire. Using the 5-point Likert scale (ranging from "1- strongly disagree" to "5- strongly agree"), each subject was asked to rate both authentication methods on three different characteristics, i.e., security, ease of use, ease of memorization.

4.6. Results

This subsection presents the results of both the quantitative and qualitative data.

4.6.1. Completion Time and Error Rate

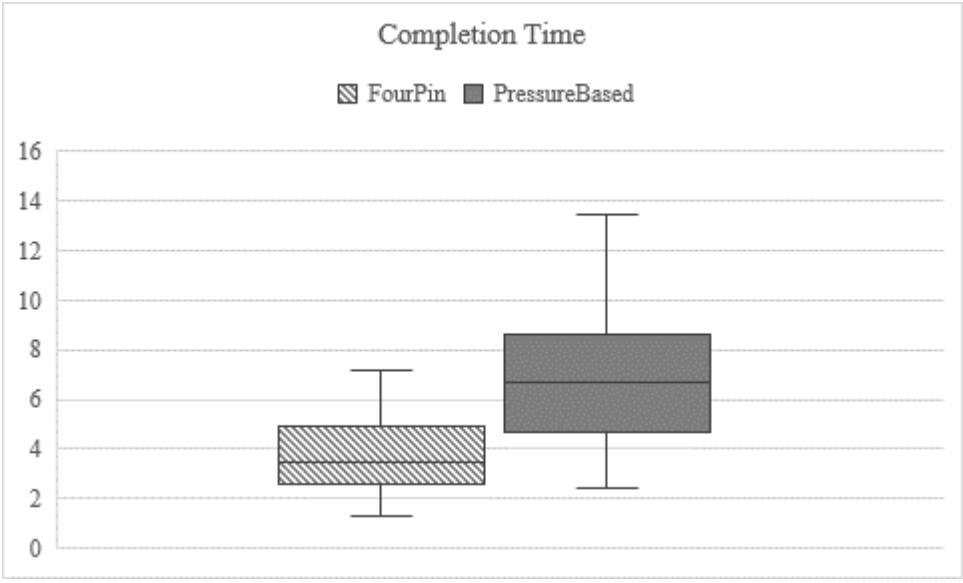

Figure 3. Box Plot of Completion Time

As presented in Figure 3, the four-pin password is significantly more efficient than the pressure-based password (4.78s vs 7.16s; p=0.002). In addition, the four-pin password has a lower error rate than the pressure-based password (3.95% vs 8.79%), but it is not significant (p=0.259). The critical errors in both treatment methods are 0.

4.6.2. User Subjective Feedback

The pressure-based password is significantly more secure than the four-pin password (4.32 vs 3.18; p<0.001). On the other hand, the four-pin password is significantly easier to memorize (4.68 vs 4.18; p=0.001) and easier to use (4.63 vs 3.87; p<0.001) than the pressure-based password.

4.6.3. Shoulder Surfing

The pressure-based password is safer than the four-pin password in the experiment of a shoulder surfing attack (46% vs 96%; p<0.001).

4.6.4. False Acceptance Rate

With a personalized detection model, even when participants knew the predefined pressure-based password, only 37.5% of the attempts were accepted by the authentication system. This low false acceptance rate indicated that a personalized detection model is effective to improve security.

5. USER STUDY 2

Though the first user study justified that the pressure-based password is more secure than the four-pin password, it is less efficient and has a lower subjective rating. However, the first study only evaluated the first time use for the pressure-based password. We expect that users' performance and subjective feedback could be significantly improved over a period of regular use. Therefore, we conducted a second user study that asked participants to use the pressure-based password for a 10-day period.

5.1. Research Hypotheses

Similar to the first user study, Goal Question Metric (GQM) [Bas94] was used to define the goals for our study.

Goal 1: Analyze pressure-based password and traditional four-pin password for the purpose of their evaluation with respect to efficiency after 10 days of use.

Hypothesis 1: There is no difference in efficiency between the two treatment methods after 10-day usage.

Goal 2: Analyze a pressure-based password and a traditional four-pin password for the purpose of their evaluation with respect to subjective feedback after 10 days of use.

Hypothesis 2: There is no difference in subjective satisfaction between the two treatment methods after 10 days of use.

5.2. Participating Subject

37 participants were recruited from a university located in the Midwestern United States for this experiment. All participants in the second experiment were new to our study, and no one from the first experiment. 81.1% of participants identified themselves as males, and 18.9% as females. 75.7% of the participants were between 18 and 24 years old, and 24.3% between 25 and

34 years old. 43.24% of participants identified themselves as iPhone users and 56.76% as Android users. 45.95% of participants described they are using a 4-digit PINs as the password of their phones, 16.22% were using 6-digit PINs, 5.4% were using FaceID, 24.32% were using Unlock Pattern, 2.7% were using Android Smartlock, 70.27% were using a fingerprint unlock, and 10.81% do not use any authentication method. Furthermore, 43.24% of participants did not know 3D Touch, and 56.76% of participants used it.

5.3. Apparatus

Participants used their personal Android smart phones to complete the study. If a participant did not have an Android phone, Google Nexus 5 was lent to the participants.

5.4. Experiment Design

The objective of this experiment was to compare the pressure-based password with the traditional four-pin password after 10 days of use. The study was conducted as a pretest-posttest, repeated-measures experiment. All participants went through each of the authentication methods each day for 10 continuous days. In order to prevent participants from memorizing passwords in a certain pattern, we randomized the order of two authentication methods each day. The experiment's operations included the following steps.

Step 1: *Pre-Study Survey*. The first step was to collect background information from the subjects.

Step 2: *Training*. Following the pre-study survey, the subjects were trained on each authentication method, by the same researcher, prior to starting the study. In the pressure-based password, a user also completed a training process to build up a personalized detection model.

Step 3: *Defining a Password*. The participants were asked to define a password for each authentication method.

Step 4: *10-day Usage Period.* In this step, each participant was asked to use each authentication method once per day for 10 continuous days. Participants could retrieve the password if they forgot the password. Each participant completed a post-study questionnaire at the end of both the first day and the last day.

5.5. Data Collection

The same types of data that were collected for the first user study were collected for the second study.

5.6. Results

5.6.1. Completion Time

Table 1. Average Completion Time of the First and Last Days

		1st day	10th day	
Completion Time	Pressure	3.25	2.3	0.00
	Four-pin	2.06	1.7	0.066
		0.00	0.00	

Table 1 shows the average completion time of both the first and the last days on two treatment methods. In the pressure-based password, the completion time of the 10th day is significantly improved over that of the 1st day, which indicates users' efficiency is significantly increased over a period of regular use. However, the four-pin is still significantly faster than the pressure-based password even after 10-day use.

For the learning curve evaluation, we were trying to find out the trend of the completion time change during the 10-day use. Therefore, we applied a fitted line plot to display the relationship between the completion time and day. The linear regression line generated from the data displayed the trend of the completion time which is decreased with the number of days increasing for both four-pin and pressure passwords. From the trend, we found the completion time of the pressure password dropped significantly from day one to day ten. Meanwhile, the

completion time of four-pin password dropped slowly from day one to day ten. Also, we generated regression equations for both four pin and pressure based password results to compare the slopes of two equations that shows the slope of pressure password line is much smaller than the slope of the four-pin line which means the completion time of press password decreased more than four-pin's as the day of use increased.

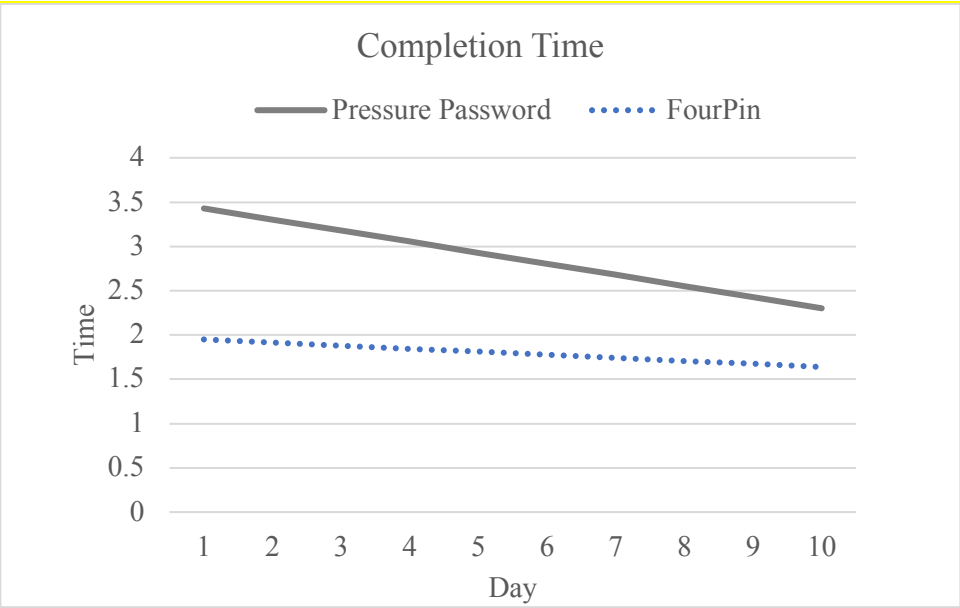

Figure 4. Fitted Line Plot of Two Methods

Figure 4 shows the fitted regression line of completion time of pressure-based method, the slope of the line is -125.29, and the constant is 3553.87. The equation of the regression line is y=-125.29*x+3553.87. Meanwhile, Figure 4 shows the regression line of the completion time of the four-pin method, the slope of the line is -34.59, and the constant is 1983.82. The equation of the regression line for the four-pin method is y=-34.59*x+1983.82. The slope of the pressure-based method is less than the four-pin method and indicates that the completion time of the pressure-based method will be less than the four-pin method when the practice time continues beyond a certain point.

5.6.2. User Subjective Feedback

Table 2. User Subjective Feedback

		1st day	10th day	
Security	Pressure	4.38	4.59	0.00
	Four-pin	3.05	3.0	0.073
		0.00	0.00	
Ease of memorization	Pressure	4.3	4.57	0.031
	Four-pin	4.75	4.49	0.058
		0.005	0.584	
Ease of use	Pressure	4.08	4.38	0.078
	Four-pin	4.54	4.43	0.524
		0.017	0.744	

User subjective feedback is measured from the perspectives of security, ease of memorization and ease of use. Being consistent with the results in the first study, the pressure-based password has a higher security rating than the four-pin password. Furthermore, the comparison between the security ratings of the first and the last days in the pressure-based password indicated that users enjoyed the security feature of pressure more after a 10-day use. In the ease of memorization, though users feel that four-pin password is easier to memorize than the pressure-based password on the first day, but there is no difference on ease of memorization after 10-day use between two treatment methods. Similar results are revealed on ease of use. Furthermore, in the pressure-based password, ease of memorization or ease of use on the 10th day is significantly or slightly significantly higher than that on the first day.

In summary, after overcoming the learning curve through regular usage, user subjective feedback is improved on the pressure-based password.

6. DISCUSSION

This section discusses the evaluation results and presents the findings from the study.

6.1. Secure

Both the subjective and objective measures justified that a pressure-based password is more secure than traditional passwords, which is consistent with previous research results [Kro16]. The improved security is mainly caused by the invisibility feature of a pressure force. Therefore, a pressure-based password is especially useful to prevent shoulder surfing for mobile authentication in a public environment. Furthermore, a pressure based password provides a cheap and secure method to replace biometric authentication on low end smartphones. The low false acceptance rate for the pressure-based password suggests that personalized detection adds additional protection. In other words, even if a pressure-based password is compromised, the attacker cannot pass the authentication if he/she has a different pressure habit from the user. In summary, the invisibility feature of pressure and personalized detection increases the security of a pressure-based password.

In addition, the pressure based authentication system is designed to defend against the smudge attack. Aviv et al. discussed the feasibility of a smudge attack on smartphone touch screens, and examined that the attacker can guess the password by analyzing the oily smudges left behind by the user's fingers when operating the device [Avi10]. Our authentication system uses different aspects to defend against the smudge attack to avoid the attacker guessing the password by using the oily smudges. From the interface design, the password input area is just below the middle of the unlock page. The input area is four horizontally listed circle buttons, every user has the same password input area so the oily smudges are left at the same place for all users. Then from our user study results, we found that even if the attacker knows the password, the personalized

pressure detection model won't predict the pressures the same as the user who defined the password. Therefore, the implicit authenticate technique helps to avoid the smudge attack.

Our study investigated a four-bit pressure-based password, which limits the password space to only 16 combinations. However, the password space can be significantly increased by either increasing the length of a pressure sequence or combining pressure with another type of password. The distinct feature of converting a pressure sequence to a decimal number makes it especially usable to define a long pressure password.

6.2. Efficiency

The first study indicated that the traditional password is more efficient than our pressure-based password. This efficiency gap is mainly caused by a difference between the cognitive models of two methods. The traditional password follows a "retrieve-press" pattern. In other words, a user first retrieves a password in his/her mind and then accordingly presses the retrieved password on a touch screen to complete the authentication. On the other hand, our pressure-based password follows a "retrieve-scan-press" pattern. After a user retrieves a predefined password, he/she has to convert the password from a decimal number to a sequence of different pressure force levels by scanning the authentication interface at the top and then pressing the touch screen with an appropriate pressure force. Therefore, the scanning time mainly slowed down the overall efficiency of the pressure-based password. The second study indicated that the efficiency of the pressure-based password can be significantly improved through regular use. Specifically speaking, regular use can help a user build up position consistency at the location of a defined sequence of pressure force. This position consistency allows a user to quickly identify a predefined password and thus avoids scanning the entire interface.

Our interface design used three enhancements, input area, status color of buttons, and status color of numbers. Our interface design enhanced the authentication process efficiency. The password input area is a small portion of the screen at the bottom of the unlock page. There are only four presses needed for the users to input the password. First, the finger travel distance of the input is shorter than the width of the screen, which is a constant because the four buttons are horizontally listed just below of the middle of the unlock page; therefore, the finger travel distance is short. In addition, the three colors that represent the status of the button also improved efficiency. The grey, black, and red colors help the user to know which button is not pressed, which is pressed, and which is ready to press, respectively the three-color status if also applied to the number list on the unlock page to help users know which binary code corresponds to the ready to press button.

In summary, the above two user studies raises a new issue that is worth future investigation, i.e., how to improve the authentication interface to improve efficiency. One straightforward solution is to reduce the number of decimal numbers and their binary codes displayed on an authentication interface. However, a smaller number will increase the risk of their password being hacked. We can also consider increasing the white space between two decimal numbers and the size of each decimal number, but this limited by the screen smartphone's size. Therefore, interface improvement is an optimization issue that is affected by several factors, such as screen size and hacking risk.

6.3. Ease of Memorization and Use

One distinct feature of our approach is to define a four-bit pressure-based password as a decimal number between 0 to 15, which is easier than a traditional four-pin password. However, the first study indicated that a traditional password is easier to memorize than our pressure-based

password. This unexpected result is caused by inconsistency. Traditional four-pin passwords are pervasive on mobile devices, and are familiar by users. On the other hand, our pressure-based password is different from traditional passwords since our approach has to convert a decimal number to a sequence of pressure forces. Users indicated a low rating on ease of memorization, which likely caused inconsistency on first time use. Fortunately, the inconsistency of pressure-based passwords can be addressed through regular usage. As shown by the second study, pressure-based passwords are as easy to memorize as traditional password after 10 days of use.

Technically, in our authentication system, the top area of the unlock page displays a set of decimal numbers, including the decimal number defined by the user, and their corresponding binary codes, so the user only need to remember the decimal number and just follow the binary codes correspond to the buttons to recall the password if the user forgot it.

6.4. Limitations

We recruited our participants of the user study at the university campus, most of the participants are the college students, faculties, or staffs. The level of education among the participants were higher than general population. Also, the technology affinity among our sample were higher than normal mobile phone users. Therefore, the results might differ from other demographics, and our results cannot stand for the entire population of smart phone users.

In addition, we conducted the shoulder surfing experiment by taping the video from the back of the volunteers, expose everything of the volunteers pressed the touchscreen when they unlock the phone. However, in the daily life, we actually unlock the phone with caution to reduce the risk of the password being leak to others. Therefore, the videos of our shoulder surfing experiment gave more information to the participants to guess the passwords. It might not simulate the real world should surfing attack.

In a word, the results of our user studies supported that the pressure based password is more secure, and as easy to remember and use as the traditional password. It has the internal validity to say the pressure based password can improve the security without increase the task overhead. Therefore, regardless of the limitations, our study design simulated the real-world mobile usage behavior, and achieved the high satisfaction.

7. CONCLUSION AND FUTURE WORK

This paper compares the authentication method with pressure sensitive data to the normal four-pin password. As we evaluated the security and usability of these methods, we figured out that the password with pressures is more secure than the digit only password. Due to the pressure is not a visible input, pressure-based password performed better than four-digit-PINs in preventing shoulder surfing attacking. In addition, by the evaluation about the personal classification models, we realized that the difference of user's sense of force presses makes the same password different in various users. Even the pressure-based password exposed to attacker, the attacker still may not unlock the device since he/she may have different sense of deep or shallow press from the password definer.

For the usability evaluation, we figured out that the pressure-based password would be as easy to remember as the four-pin password. Even though for the first-time users, the four-digit-PINs still the easier to remember and user, the more experience the user have about the pressure-based password can be more satisfied with the pressure-based password. Same as the completion time of pressure-based password, it can be decreased as the more experiences the user gain. In addition, the error rate between the methods with pressures and the digit only password has no significant difference.

In summary, our proposed pressure-based password is more secure than the traditional four PIN password, and as easy to remember as the four-pin password.

In the future, we would like to do more research on the visualization part of the unlock interface. Now we just set the pressure-based password as a number between 0-15 and use the binary representation of the 16 numbers to present four pressure input which 0 means shallow press, and 1 means deep press. Only 16 numbers probably not enough scale as a password because

of small password space. We will try to change the pressure representations by different techniques in the future to make a more secure and usable pressure only password.

REFERENCES

[Ari14] Arif, A. S., Mazalek, A., & Stuerzlinger, W. (2014). The use of pseudo pressure in authenticating smartphone users. In Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (pp. 151–160). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[Avi10] Aviv, A. J., Gibson, K. L., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge Attacks on Smartphone Touch Screens. Woot, 10, 1–7.

[Bus15] Buschek, D., De Luca, A., & Alt, F. (2015). Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 1393–1402). ACM.

[Bas94] V. R. Basili, G. Caldiera, and H. D. Rombach, "The Goal Question Metric Approach", Technical Report, Department of Computer Science, University of Maryland, 1994, ftp://ftp.cs.umd.edu/pub/sel/papers/gqm.pdf.

[Cha12] Chang, T.-Y., Tsai, C.-J., & Lin, J.-H. (2012). A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. Journal of Systems and Software, 85(5), 1157–1165.

[Cla07] Clarke, N. L., & Furnell, S. (2007). Advanced user authentication for mobile devices. Computers & Security, 26(2), 109–119.

[DeL15](1) De Luca, A., Hang, A., Von Zezschwitz, E., & Hussmann, H. (2015). I feel like I'm taking selfies all day!: towards understanding biometric authentication on smartphones. In

Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 1411–1414). ACM.

[DeL15](2) De Luca, Alexander and Harbach, Marian and von Zezschwitz, Emanuel and Maurer, Max-Emanuel and Slawik, Bernhard Ewald and Hussmann, Heinrich and Smith, Matthew. Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages

[DeL13] De Luca, A., Von Zezschwitz, E., Nguyen, N. D. H., Maurer, M.-E., Rubegni, E., Scipioni, M. P., & Langheinrich, M. (2013). Back-of-device authentication on smartphones. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2389–2398). ACM.

[Har16] Harbach, M., De Luca, A., & Egelman, S. (2016). The anatomy of smartphone unlocking: A field study of android lock screens. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 4806–4817). ACM.

[Ali09] Hasimah Ali, Wahyudi, & M. J. E. Salami. (2009). Keystroke pressure based typing biometrics authentication system by combining ANN and ANFIS-based classifiers. In 2009 5th International Colloquium on Signal Processing & Its Applications (pp. 198–203). https://doi.org/10.1109/CSPA.2009.5069216

[Kha14] Khan, H., Atwater, A., & Hengartner, U. (2014). A comparative evaluation of implicit authentication schemes. In International Workshop on Recent Advances in Intrusion Detection (pp. 255–275). Springer.

[Kim10] Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J. W., Nicholson, J., & Olivier, P. (2010). Multi-touch authentication on tabletops. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1093–1102). ACM.

[Kro16] Krombholz, K., Hupperich, T., & Holz, T. (2016). Use the force: Evaluating force-sensitive authentication for mobile devices. In Symposium on Usable Privacy and Security (SOUPS) (pp. 207–219).

[Mal06] Malek, B., Orozco, M., & El Saddik, A. (2006). Novel shoulder-surfing resistant haptic-based graphical password. In Proc. EuroHaptics (Vol. 6, pp. 1–6).

[Oro06] Orozco, M., Malek, B., Eid, M., & El Saddik, A. (2006). Haptic-based sensible graphical password. In Proceedings of Virtual Concept (Vol. 56, pp. 1–4).

[Rie13] Rieger, F. (2013). Chaos Computer Club Breaks Apple TouchID. Chaos Computer Club. https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid, last accessed 1/5/2017.

[Sae09] Saevanee, H., & Bhattarakosol, P. (2009). Authenticating user using keystroke dynamics and finger pressure. In Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE (pp. 1–2). IEEE.

[Ste10] Stewart, C., Rohs, M., Kratz, S., & Essl, G. (2010). Characteristics of pressure-based input for mobile devices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 801–810). ACM.

[Tak03] Takada, T., & Koike, H. (2003). Awase-E: Image-based authentication for mobile phones using user's favorite images. In International Conference on Mobile Human-Computer Interaction (pp. 347–351). Springer.

[Wei08] Weiss, R., & De Luca, A. (2008). PassShapes: utilizing stroke based authentication to increase password memorability. In Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges (pp. 383–392). ACM.