Enhancing Click-Draw Based Graphical Passwords Using Multi-Touch on Mobile Phones

Yuxin Meng, Wenjuan Li, Lam-For Kwok

Enhancing Click-Draw based Graphical Passwords Using Multi-Touch on Mobile Phones

Yuxin Meng,[1] Wenjuan Li,[2] and Lam-for Kwok[1]

[1] Department of Computer Science, City University of Hong Kong, Hong Kong, China
{yuxin.meng@my.cityu.edu.hk,cslfkwok@cityu.edu.hk}
[2] Computer Science Division, Zhaoqing Foreign Language College, Guangdong, China
wenjuan.anastatia@gmail.com

Abstract. Graphical password based authentication systems are now becoming one of the potential alternatives to alleviate current over-reliance on traditional text-based password authentication. With the rapid development of mobile devices (i.e., the increase of computing power), this kind of authentication systems has been implemented on mobile phones to authenticate legitimate users and detect impostors. But in real deployment, we notice that users can utilize more actions like multi-touch on a mobile phone than on a common computer. The action of multi-touch, which refers to the process of touching a touchscreen with multiple fingers at the same time, is a distinguished feature on a touchscreen mobile phone. In this paper, we therefore attempt to explore the effect of multi-touch on creating graphical passwords in the aspect of security and usability. In particular, we conduct a study of using click-draw based graphical passwords in the evaluation, which combines current input types in the area of graphical passwords, and we further develop a multi-touch enabled scheme on mobile phones. Three experiments were conducted with 60 participants and the experimental results indicate that, by integrating the action of multi-touch, graphical passwords can be generally enhanced in the aspect of both security and usability.

Keywords: Graphical Passwords, User Authentication, Multi-Touch, Human Factors, Mobile Phones, Mobile Security.

1 Introduction

User authentication on mobile phones has become more and more important with modern mobile devices being comparable to a PC (i.e., with the continuous increase of computing power). With the popularity of mobile phones, users are likely to store a lot of sensitive information (e.g., credit card numbers) on their mobile phones [11] and to use their phones for security sensitive tasks (e.g., authorizing commercial transactions) due to their fast data connection and wireless connectivity [8].

In these cases, it is crucial to develop and implement user authentication mechanisms for a mobile phone to authenticate legitimate users and detect imposters. To mitigate the limitations of traditional text-based password authentication (i.e., users have difficulty in remembering complex and random passwords which is known as long-term memory (LTM) limitations), authenticating users by means of images is one of the possible alternatives in which several studies [17, 19] have shown that human brain was

better at remembering and recognizing images than text. Along with this observation, several graphical password applications have been proposed on mobile phones like *Android unlock pattern*[3], a graphical password based Android application in which users are required to input correct unlock patterns to unlock their Android screen [5].

Generally, graphical password based authentication can be categorized into three folders based on their input methods[4]: *click-based graphical passwords*, *choice-based graphical passwords* and *draw-based graphical passwords*. In particular, the click-based schemes require users to click on the provided image(s) (i.e., choosing an object or element of the image), the choice-based schemes require users to select a series of images (i.e., selecting images in an order), and the draw-based schemes require users to draw some secrets to be authenticated (i.e., drawing a user signature). Several security studies regarding graphical passwords can be referred to [3], [7] and [9].

Motivation. In real deployment, we find that users can utilize more actions like *multi-touch* in creating graphical passwords on a mobile phone than on a common computer. The *multi-touch* refers to the process of touching a touchscreen device with multiple fingers simultaneously, which is a distinguished feature for current touchscreen mobile phones. This observation indicates that the creation of graphical passwords may be different on distinct platforms due to different types of input actions. In addition, touchscreens are becoming the leading input method on the mobile platform where 74% of all phones in the market using a touch screen [16]. Our motivation is therefore to explore the impact of *multi-touch* on creating graphical passwords.

Contributions. In this paper, we attempt to investigate the impact of multi-touch on creating graphical passwords in the aspect of security and usability and use it to enhance the creation of graphical passwords. In particular, we employ click-draw graphical password scheme (*CD-GPS*) in the evaluation which combines current inputs of creating a graphical password. Our contributions can be summarized as below.

- We give a detailed analysis of the possible impact of using multi-touch on the creation of *CD-GPS* passwords. Based on the original *CD-GPS* scheme, we develop an example system of *multi-touch enabled CD-GPS scheme* on a mobile phone that enables users to create the *CD-GPS* passwords using the action of multi-touch.
- To verify our analysis, we conducted three experiments with a total number of 60 participants. By comparing the obtained results, we find that the action of multi-touch can positively enhance the construction of graphical passwords in the aspect of both security and usability.

The remaining parts of this paper are organized as follows: in Section 2, we briefly introduce the click-draw based graphical password scheme (*CD-GPS*); Section 3 analyzes the potential impact of multi-touch on creating *CD-GPS* passwords; Section 4 presents our developed *multi-touch enabled CD-GPS scheme* and our experimental methodology; Section 5 describes the experimental results and Section 6 reviews some related work; at last, Section 7 concludes our paper and points out future work.

[3] `http://code.google.com/p/androidunlockpatternswitch/`.

[4] Another graphical password classification (e.g., [3, 20]): recognition based scheme (i.e., recognizing images), pure recall based scheme (i.e., reproducing a drawing without a hint) and cued recall based scheme (i.e., reproducing a drawing with hints).

2 Click-Draw based Graphical Password Scheme

The click-draw based graphical password scheme (shortly *CD-GPS*) [14] was developed with the purpose of enhancing traditional graphical passwords by combining existing input types from click-based, choice-based and draw-based graphical passwords. A general *CD-GPS scheme* mainly consists of two operational steps: *image selection* and *secret drawing*.

The first step is *image selection* where users are required to select several images from an image pool (i.e., the pool may contain a number of images with different themes) in an ordered sequence, and remember this order of images like a story to assist memorization. Then, users are required to further select one or more images to draw their secrets. In the step of *secret drawing*, users can freely *click-draw* their secrets (e.g., a number, a letter) on their selected image(s). The action of *click-draw* requires users to draw a secret by using a series of clicks. To facilitate the use of *click-draw*, the *CD-GPS scheme* partitions the selected image, which is used for click-drawing secrets, into a $N \times N$ table.

In [14], an example system of CD-GPS was also implemented in which the image pool contains 10 different images (i.e., themes like fruits, landscape, people, etc). In the first step, users are required to select 4 images out of the image pool and organize these images in a story order. Then, in the second step of *secret drawing*, users have to further select 1 image for click-drawing their own secrets. The selected image in the example system will be divided into a 16×16 table with 256 clickable squares. The user study with 42 participants showed that the *CD-GPS scheme* could provide suitable properties in the aspect of both usability and security. Detailed analysis about the *CD-GPS* can be referred to [14].

3 Multi-Touch

In real deployment, we notice that the way of creating graphical passwords may be different on a computer and on a touchscreen mobile phone. For instance, users can use more actions (e.g., multi-touch) on a mobile phone than on a common computer (e.g., PC). Nowadays, *multi-touch* is becoming a distinguished feature on a touchscreen mobile phone (or other touchscreen based devices) that users can touch the screen with multiple fingers at the same time. Next, we analyze the potential impact of multi-touch on creating the *CD-GPS* passwords.

Common computer. In a computer (e.g., a PC) with mouse as the input device, users can only create the *CD-GPS* passwords (i.e., drawing a secret by means of click-draw) with the action of single-click. In this scenario, the potential password space of *CD-GPS* passwords can be calculated as follows [14]:

$$\frac{N_1!}{(N_1-n)!} \times \frac{n!}{k! \times (n-k)!} \times \prod_k \frac{N_c!}{(N_c-K_i)!} (i = 1,2,3,...)$$

Where N_1 is the number of images in the image pool, n is the number of selected images in a story-sequence, k is the number of further selected images for click-drawing,

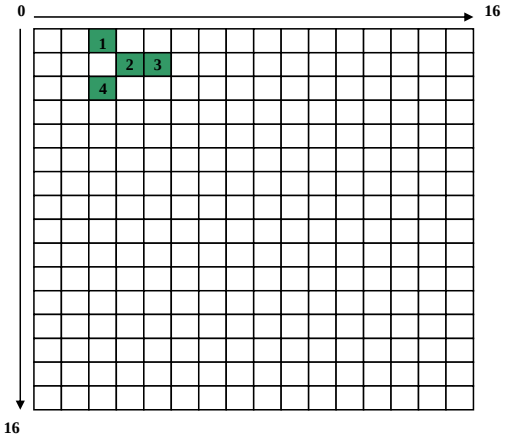

Fig. 1. An example of creating CD-GPS: drawing a symbol of arrow '>'.

N_c is the number of clickable squares and K_i means there are totally *i clicks* on a selected image. $\frac{N_1!}{(N_1-n)!}$ means that selecting n images out of N_1 images in a story sequence. $\frac{n!}{k!\times(n-k)!}$ means that choosing k images out of n images for secret drawing without considering the image sequence. Finally, $\prod_k \frac{N_c!}{(N_c-K_i)!}$ means the product of password space in selected k images.

Thus for the example system of the *CD-GPS* (where N_1=10, n=4, k=1 and N_c=256), the potential password space can be specified as below:

$$(10-4)!\times 4\times \frac{256!}{(256-K_i)!}(i=1,2,3,...)$$

Touchscreen mobile phone. On a mobile phone with touchscreen as the main input device, users can perform more actions like *multi-touch* on the screen than on a common computer. The action of *multi-touch* greatly distinguishes the creation of graphical passwords on a mobile phone from that on a computer. For example, as shown in Fig. 1, our target is to draw a symbol of arrow '>'. To better illustrate the process of creation, we further assume the ordered sequence of drawing is 1, 2, 3 and 4. On a computer with mouse as the input device, because the *CD-GPS scheme* does not consider the sequence of clicks, there is only one choice to sequentially click these 4 squares.

However, with the action of *multi-touch* (i.e., only considering two fingers), there exist other 4 choices to complete the creation: {multi-touch{1, 2}, multi-touch{3, 4}}, {1, multi-touch{2, 3}, 4}, {1, 2, multi-touch{3, 4}}, {multi-touch{1, 2}, 3, 4}. In addition, if we do not limit the click sequence to 1, 2, 3 and 4, then the number of click choices can be increased to $4\times 2=8$. This case indicates that the potential password space of *CD-GPS* can be further enlarged by integrating the action of *multi-touch* into the creation of graphical passwords.

If we only consider the multi-touch with 2 fingers (i.e., two squares can be selected at the same time), then the potential password space can be represented as below:

$$\frac{K_i!}{2!} \times \frac{N_1!}{(N_1-n)!} \times \frac{n!}{k! \times (n-k)!} \times \prod_k \frac{N_c!}{(N_c-K_i)!} (i = 1,2,3,...)$$

Correspondingly, for the example system of the *CD-GPS* in [14], its potential password space can be specified as below:

$$\frac{K_i!}{2!} \times (10-4)! \times 4 \times \frac{256!}{(256-K_i)!} (i = 1,2,3,...)$$

That is, by integrating the multi-touch with only 2 fingers, the password space can be further enlarged by $\frac{K_i!}{2!}$ times in theory. Note that the user study in [14] has showed that K_i is usually bigger than 5. Moreover, with the multi-touch, users may complete their drawings more quickly as two squares can be selected simultaneously.

4 User Study

With the above analysis of *multi-touch*, we therefore attempt to verify the impact of *multi-touch* on creating graphical passwords. In this section, we begin by describing our developed example system of *multi-touch enabled CD-GPS* on an Android phone and we then present our experimental methodology in the user study.

4.1 Multi-Touch Enabled CD-GPS

To enable the creation of *CD-GPS* passwords with the action of *multi-touch*, we design and develop an example system of *multi-touch enabled CD-GPS* that can collect multi-touch clicks. This system, as shown in Fig. 2, authenticates whether a user is legitimate by combining the click-coordinate information with multi-touch records.

Fig. 2 (a) illustrates the developed *multi-touch enabled CD-GPS scheme*. Similarly, the image pool contains 10 images (arranged in 5×2 grids) with different themes such as fruits, landscape, cartoon characters, food, sport, buildings, cars, animals, books and people. All used images have the same pixel size of 400×400. In the first step, users are required to select 4 images out of the image pool and organize these images in a story order. Then, users are required to select 1 image for drawing their secrets. Different from the *CD-GPS scheme* on a computer, users can utilize the multi-touch with two fingers to complete their drawings in the developed *multi-touch enabled CD-GPS scheme*. The *multi-touch enabled CD-GPS scheme* also divides an image into a 16×16 table with 256 clickable squares in which each square has a pixel size of 25×25.

Fig. 2 (b) shows the authentication process in our developed example system. When users finish their drawings, the authentication system collects all the inputs (e.g., clicked squares' coordinates) and multi-touch information (i.e., coordinates with multi-touch), and then constructs a signature in the phase of *signature construction*. Take the clicks in Fig. 1 as an example, if the squares with 2 and 3 are clicked with multi-touch, the relevant plaintext signature is recorded as: {(3, 1), multi-touch{(4, 2), (5, 2)}, (3, 3)}. In the phase of *signature comparison*, the authentication system can detect an imposter by comparing current collected signature with the pre-defined normal signature. The comparison process is described as follows:

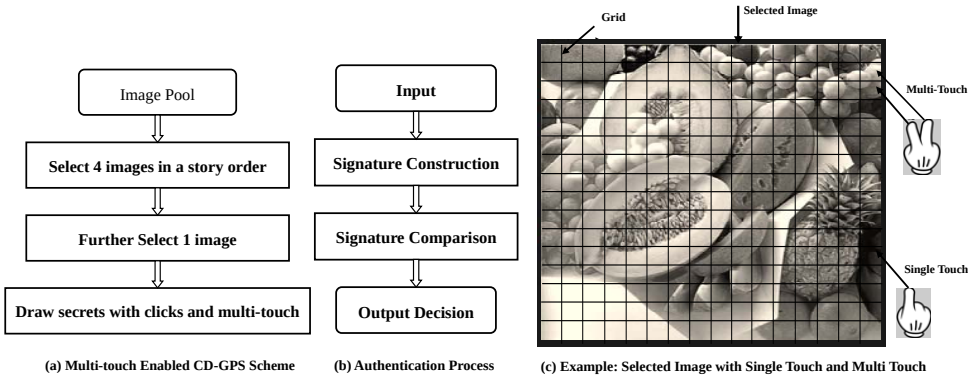

Fig. 2. An example system of *multi-touch enabled CD-GPS scheme*: (a) Multi-touch Enabled CD-GPS Scheme; (b) Authentication Process in the Example System; (c) An example of single touch and multi-touch on a selected image.

- If signature matching is successful, then the user is regarded as a legitimate user.
- If signature matching is failed, then the user is regarded as an imposter.

Finally, the authentication system outputs the decision and can require users to perform extra validation (i.e., inputting a correct PIN) if they are identified as imposters. In addition, Fig. 2 (c) illustrates an example of *single touch* and *multi-touch* on a selected image (*fruit theme*) in the example system. Users can use either *single touch* or *multi-touch* to draw their own secrets.

In the evaluation, the above example system of *multi-touch enabled CD-GPS* was implemented on an Google/HTC Nexus One Android phone (with resolution 480×800 px and CPU 1GHz). In the current smartphone market, Android OS and iOS make up the largest share with a combined 80% of smartphones [16]. In addition, the merits of using this particular phone is that its stock Android system can be replaced by a modified customized OS version. Specifically, we updated the phone with a modified Android OS version 2.2 based on CyanogenMod[5]. The modification mainly consists of changes to the application framework layer to record the multi-touch input and relevant coordinate information from the touchscreen. The implementation details are similar to our previous work [15].

4.2 Experimental Methodology

To evaluate the performance of the *multi-touch enabled CD-GPS scheme*, we conducted an in-lab user study that consisted of three major experiments with totally 60 participants those who were interested in our work. All participants are volunteer with diverse backgrounds including both students and senior people. Particularly, 30 participants (13 females and 17 males) are from the computer science department (but not security related major). All participants are regular web, mobile phone users and ranged in age from 18 to 55 years. The detailed information of participants is shown in Table 1.

[5] `http://www.cyanogenmod.com/`

Table 1. Participants information in the user study.

Age Range	Male	Female
15-25	10	10
25-35	10	8
35-45	6	6
45-55	6	4

In the user study, we mainly attempt to identify the effect of multi-touch by collecting user's feedback. To avoid any bias, we employed a *double-blind manner* in the user study that we did not uncover the name of these two schemes but we introduced our objectives in the user study and gave a detailed description of using these two example systems. Specifically, the original *CD-GPS scheme* was implemented on a computer with mouse as the input device [14] while the *multi-touch enabled CD-GPS scheme* was deployed on an Android phone with a touchscreen as the input device. To further avoid the bias of platforms, we evaluate the *multi-touch enabled CD-GPS scheme* by enabling and disabling multi-touch on the Android phone respectively.

Every participants can complete 3 practice trials for each scheme to get familiar with the platforms before they start to complete real trails. Therefore, a total of three experiments were conducted with the same 60 participants and the detailed steps in each experiment are described as below:

- *Experiment1*. This experiment was conducted on a desktop computer and each participant had to create 5 *CD-GPS* passwords.
  - Step 1. *CD-GPS* Creation: Creating a *CD-GPS* password by following the two steps in the scheme: *image selection* and *secret drawing*.
  - Step 2. *CD-GPS* Confirmation: Confirming the password by re-selecting images in the correct order and re-drawing secrets in the correct place. If users incorrectly confirm their password, they can retry the confirmation or return to Step 1.
  - Step 3. Feedback: All participants are required to complete a *feedback form* about the password creation and confirmation.

  In the second day, all participants were required to complete a login session and gave their feedback.
  - Step 4. *CD-GPS* Login: Logging in the example system with all created *CD-GPS* passwords. Users can cancel an attempted login if they noticed an error and try again.
  - Step 5. Feedback: All participants should complete a *feedback form* about the password login.
- *Experiment2*. This experiment was conducted on an Android phone by enabling the action of multi-touch, and the steps are similar to *Experiement1*.
  - Step 1. *Multi-touch enabled CD-GPS scheme* Creation: Creating 5 *CD-GPS* passwords based on the two steps in the scheme. Multi-touch is available during the creation.

- Step 2. *Multi-touch enabled CD-GPS scheme* Confirmation: This step is similar to *Experiment1*, but multi-touch is enabled.
- Step 3. Feedback collection.

In the second day, all participants were required to complete a login session and gave their feedback.

- Step 4. *Multi-touch enabled CD-GPS scheme* Login: Logging in the example system with all created passwords. The action of multi-touch is enabled.
- Step 5. Feedback collection.

– *Experiment3*. This experiment was conducted on an Android phone by disabling the action of multi-touch with the purpose of avoiding the bias regarding the platforms. The steps are similar to *Experiment2*.

- Step 1. *Multi-touch disabled CD-GPS scheme* Creation: Creating 5 *CD-GPS* passwords based on the steps in the scheme. Multi-touch is disabled during the creation.
- Step 2. *Multi-touch disabled CD-GPS scheme* Confirmation: Confirming the password with multi-touch disabled.
- Step 3. Feedback collection.

In the second day, all participants were required to complete a login session and gave their feedback.

- Step 4. *Multi-touch disabled CD-GPS scheme* Login: Logging in the example system with all created passwords. Different from *Experiment2*, the action of multi-touch is disabled.
- Step 5. Feedback collection.

Ten-point Likert scales were used in each feedback question where 1-score indicates strong disagreement and 10-score indicates strong agreement. We denoted 5-score as the meaning of "It is hard to say" for a question. In the analysis, these collected questions and scores for each experiment can be used to investigate the impact of multi-touch on creating graphical passwords. During the evaluation, 300 real trails were recorded for *Experiment1*, *Experiment2* and *Experiment3* respectively.

5 Results and Analysis

In this section, we present the results obtained in the experiments and analyze the results by means of the collected users' feedback. The *success rate* and *average completion time* regarding the step of creation, confirmation and login in *Experiment1*, *Experiment2* and *Experiment3* are shown in Table 2.

Particularly, the *success rate* in the step of *Creation* means that participants created their passwords without restarting, the *success rate* in the step of *Confirmation* means that participants confirmed their passwords without restarting and failed attempts for the first time, while the *success rate* in the step of *Login* means that participants, for the first time, pressed the login button and entered into the example system successfully. The *average completion time* is an average value computed by all participants.

Table 2. Success rate and average completion time for the step of creation, confirmation and login in *Experiment1*, *Experiment2* and *Experiment3*.

Experiment1	Creation	Confirmation	Login
Success Rate (the first time)	223/300 (74.3%)	271/300 (90.3%)	254/300 (84.7%)
Completion Time (Average in seconds)	20.2	15.7	14.3
Standard Deviation (SD in seconds)	7.6	7.5	5.3
Experiment2	Creation	Confirmation	Login
Success Rate (the first time)	270/300 (90.0%)	288/300 (96.0%)	276/300 (92.0%)
Completion Time (Average in seconds)	12.1	7.1	7.6
Standard Deviation (SD in seconds)	5.3	3.5	3.2
Experiment2	Creation	Confirmation	Login
Success Rate (the first time)	258/300 (86.0%)	276/300 (92.0%)	265/300 (88.3%)
Completion Time (Average in seconds)	16.8	11.2	9.6
Standard Deviation (SD in seconds)	5.9	6.5	4.2

Success Rate. In *Experiment1*, as shown in Table 2, the success rate is 74.3% in the *Creation step*, several participants restarted the *password creation* (i.e., click-drawing another secret) because they changed their minds in drawing the secrets. The success rate is 90.3% in the *Confirmation step*, some restarting and failed attempts were detected since these participants clicked a wrong square. In the *Login step*, most participants could enter their passwords successfully with a success rate of 84.7%, some failed attempts were identified since these participants forgot their selected images or clicked on a wrong square for the first time.

In *Experiment2*, the success rate is 90% in the *Creation step* which is higher than the corresponding results in both *Experiment1* and *Experiment3*. The success rate achieves 96% in the *Confirmation step* which is also higher than both *Experiment1* and *Experiment3*. Most participants indicated that they could create and confirm their passwords more easily by using the action of multi-touch. That is, it is easier for them to remember their passwords by reducing the number of touch gestures. In the *Login step*, the success rate again achieves a higher value of 92% compared to both *Experiment1* and *Experiment3*. Participants indicated that the action of multi-touch could facilitate their construction and memorization.

In *Experiment3*, by disabling the multi-touch, the success rate is decreased to 86%, 92% and 88.3% with regard to the *Creation step*, *Confirmation step* and *Login step* respectively. Participants indicated that they should use more touch gestures to construct a secret without multi-touch. But the results obtained in this experiment are still better than those obtained in *Experiment1*. Participants reflected that they could use a touch gesture more conveniently and accurately than a mouse-click.

Completion Time. In *Experiment1*, the average completion time is around 20 seconds in the *Creation step* since participants should spend more time in deciding the image-order and selecting the images. The average consuming time is gradually decreased to 15.7 seconds and 14.3 seconds in the *Confirmation step* and *Login step* respectively. The main reason is that participants only need to re-create their passwords without spending additional time in constructing a new one.

In *Experiment2*, the average completion time is 12.1 seconds regarding the *Creation step*, which reduces about 40.1% of the time consumption in creating the passwords compared to *Experiment1*. The same as *Experiment1*, the average time consumption in *Experiment2* continuously decreases to 7.1 seconds and 7.6 seconds for the *Confirmation step* and *Login step* respectively. Most participants indicated that they could create and confirm the passwords more quickly by utilizing the action of multi-touch. Moreover, it is visible that the standard deviation (SD) is further reduced in *Experiment2* than that in *Experiment1* (i.e., for the *Creation step*, SD 7.6 for *Experiment1* while SD 5.3 for *Experiment2*), which shows that participants can generally create their passwords more quickly in *Experiment2*.

In *Experiment3*, compared with the result in *Experiment2*, the average completion time is increased to 16.8 seconds, 11.2 seconds and 9.6 seconds for the *Creation step*, *Confirmation step* and *Login step* respectively. The reason is that participants should spend more time in single touching without the action of multi-touch. For example, selecting two clickable squares, we should use two single touches instead of a multi-touch. But similar to the situation regarding the *successes rate*, the results are still better than those in *Experiment1*, the main reason is that it is more convenient to use a touch gesture than a mouse-click for a participant.

The Number of Clicks. To further analyze the experimental results, we present the click information in Table 3. This table shows that in *Experiment1*, most participants prefer the number of 5 and 6 clicks with the percent of 32.6% and 30.7% respectively. For the number of 7 and 8 clicks, the percent of trails is 18.7% and 7.3%, and there is no participant click above 9 squares. The results in *Experiment3* is similar to the *Experiment1*, but there are 3.3% trails selecting 9 squares. The reason is that participants feel more convenient to use a touch gesture than a mouse-click.

In *Experiment2*, it is visible that most participants prefer to click 6 and 8 squares to construct their secrets with the percent of 36% and 24%. For the number of 7 clicks, the percent is 18.3%. Compared to *Experiment1*, there are about 6.7% and 3.3% of total trails in *Experiment2* clicking 9 and 10 squares whereas no participants choose to draw secrets with 4 clicks. The situation is similar when compared to *Experiment3* (i.e., there are 7% trails constructing passwords using only 4 squares and no trail selecting 10 squares in *Experiment3*). The major reason is that most participants prefer to create passwords using multi-touch on the Android phone in which a single click of multi-touch can select two squares. By means of only 4 multi-touch clicks, a participant can easily draw a secret with 8 squares.

Feedback Result. We present several questions used in the *feedback step* and corresponding scores in Table 4. The scores in the table are simply average values calculated by the recorded scores of all participants.

The scores in the No.2 and No.3 questions indicate that, on the same platform of mobile phones, two schemes are accepted by most participants while most participants feel more comfortable to create passwords using the *multi-touch enabled CD-GPS scheme*. In comparison, the No.1 question receives a lower score of 7.5 with regard to the platform of a PC. Similarly, for the No.4, No.5 and No.6 questions, the *multi-touch enabled CD-GPS scheme* obtains the highest score of 9.2. This means that most participants

Table 3. The number of selected squares in *Experiment1*, *Experiment2* and *Experiment3*.

# of selected squares	Experiment1	Experiment2	Experiment3
4 squares	32/300 (10.7%)	0	21/300 (7.0%)
5 squares	98/300 (32.6%)	35/300 (11.7%)	101/300 (33.7%)
6 squares	92/300 (30.7%)	108/300 (36.0%)	98/300 (32.7%)
7 squares	56/300 (18.7%)	55/300 (18.3%)	45/300 (15.0%)
8 squares	22/300 (7.3%)	72/300 (24.0%)	25/300 (8.3%)
9 squares	0	20/300 (6.7%)	10/300 (3.3%)
10 squares	0	10/300 (3.3%)	0

Table 4. Several questions and relevant scores in the user study.

Questions	Score (average)
1. I could easily create a password in the Experiment1	7.5
2. I could easily create a password in the Experiment2	8.9
3. I could easily create a password in the Experiment3	8.0
4. The time consumption in the Experiment1 is acceptable	6.7
5. The time consumption in the Experiment2 is acceptable	9.2
6. The time consumption in the Experiment3 is acceptable	7.9
7. I prefer to use multi-touch	9.5
8. I do not prefer to use multi-touch	2.1

feel multi-touch can reduce the time consumption since they can increase the speed of selecting squares by using several multi-touch clicks. Regarding the No.7 and No.8 questions, participants advocate to create a password by means of multi-touch with a higher score of 9.5 while the score of the opposition is only 2.1.

These results of the feedback show that utilizing the action of multi-touch can further enhance the graphical password in the aspect of usability. In addition, users can increase the password entropy by using several multi-touch clicks.

Usability and Security Discussion. For the usability, the scores regarding *Experiment2* and *Experiment3* (these two experiments were conducted on the same platform) indicate that most participants prefer the *multi-touch enabled CD-GPS scheme* in which they can use multi-touch to create passwords more quickly and comfortably. Back to Table 2, it is visible that participants indeed perform better in *Experiment2* by utilizing the multi-touch with regard to each step of creation, confirmation and login. Overall, these results show that the action of multi-touch can enhance the usability of the *CD-GPS scheme* by speeding up the password input.

For the security, as we analyzed in Section 3, by integrating the multi-touch with only 2 fingers, the password space can be enlarged by $\frac{K_i!}{2!}$ times (K_i means the number of clicked squares). As shown in Table 3, participants are likely to click more squares in *Experiment2* than *Experiment3*. For example, there are about 3.3% trails clicking 10 squares to construct passwords in *Experiment2* whereas no participant clicks 10 squares in *Experiment3*. Also, there are 24% trails clicking 8 squares in *Experiment2* but only 8.3% trails in *Experiment3*. In addition, no participant chooses 4 squares to create their

passwords in *Experiment2* while up to 7% trails clicking 4 squares in *Experiment3*. In this case, if a participant select 8 squares by means of multi-touch, the password space can be enlarged by $\frac{8!}{2!} = 20160$ times compared to the original *CD-GPS scheme*. On the whole, these results indicate that the action of multi-touch can generally enhance the security of the *CD-GPS scheme* because users are more likely to select larger number of squares to construct their passwords through remembering less number of touches on touchscreen devices such as mobile phones.

6 Related Work

In recent years, a number of graphical password schemes have been proposed aiming to enhance the user authentication [20]. Blonder [2] first designed a click-based graphical password scheme that users could generate their passwords by clicking on several predefined locations on an image. For authentication, users are demanded to re-click on the same locations. Then, graphical password based authentication systems like *PassPoints* system [22], *Story* scheme [6], *DAS* (Draw-a-secret) scheme [10], Cued Click Points (CCP) [4] and *Qualitative DAS* scheme [13] are developed on a common computer.

With the rapid development of mobile computing, more work of designing graphical passwords has been studied on a mobile device. Dunphy *et al.* [8] presented different challenges such as shoulder surfing and intersection attack in the field of graphical passwords, and investigated the deployment of recognition-based graphical password mechanisms on a mobile device. Their experiments showed that user acceptance was often driven by convenience and login durations of approximately 20 seconds were unattractive to many users. Kim *et al.* [12] evaluated a number of novel tabletop authentication schemes that exploit the features of multi-touch interaction in order to inhibit shoulder surfing. Later, Oakley and Bianchi [18] presented the feasibility of constructing a graphical password with multi-touch, but their work did not give a detailed analysis. De Luca *et al.* [5] recently presented an implicit approach to improve user authentication based on the way they perform an action on current mobile devices by means of unlock patterns. However, they have not studied the impact of multi-touch on creating passwords. Several recent work about biometrics based authentication and potential attacks on touch-enabled mobile phones can be referred to [1, 15, 21, 23].

Different from the above work, in this paper, we mainly focus on the platform of a touchscreen mobile phone and attempt to explore the impact of multi-touch on the click-draw based graphical passwords in the aspect of usability and security. In the user study with 60 participants, we find that the action of multi-touch can generally enhance the construction of graphical passwords.

7 Conclusion and Future Work

Graphical passwords have been developed as a promising alternative to traditional text-based passwords. In real-world applications, we find that the creation of graphical passwords may be different on a computer and on a touchscreen mobile phone. That is, users can use more actions like multi-touch on a mobile phone than on a common computer (e.g., desktop computer).

In this work, we therefore attempt to enhance the creation of graphical passwords by using the action of multi-touch. In particular, we conducted a study of using the click-draw based graphical passwords (*CD-GPS*) in the evaluation, which combines the current input types in the area of graphical passwords and we further developed an example system of *multi-touch enabled CD-GPS scheme* on a mobile phone. We begin by analyzing the potential impact of multi-touch on computing the password space of *CD-GPS* and we then conducted a user study that was composed of three major experiments (named *Experiment1*, *Experiment2* and *Experiment3*) with totally 60 participants. *Experiment1* was performed on a desktop computer, while *Experiment2* and *Experiment3* were conducted on an Android phone. We later give a detailed analysis of success rate, completion time, the number of clicks and users' feedback in these experiments. The experimental results show that by integrating the action of multi-touch, the construction of graphical passwords can be further improved in the aspect of both security and usability, and that users are more likely to generate more secure passwords by remembering less number of touches on a mobile phone.

Our work is an early work in discussing the impact of multi-touch on creating the *CD-GPS* graphical passwords. The future work could include performing a even larger user study with much more participants to validate the results obtained in this work (e.g., a more systematic experiment) and discussing the implications of multi-touch on shoulder-surfing and smudge attacks. In addition, future work could also include conducting a further analysis of password patterns generated by participants with different ages to explore the effect of multi-touch, and integrating and evaluating more actions (e.g., rotate, scrolling) in creating graphical passwords on a mobile device.

Acknowledgments. We would like to thank all participants for their hard work in the experiments and thank all anonymous reviewers for their helpful comments.

References

1. Angulo, J., Wästlund, E.: Exploring Touch-Screen Biometrics for User Identification on Smart Phones. In: Camenisch, J. et al. (eds.): Privacy and Identity 2011, IFIP AICT 375, pp. 130–143 (2012)
2. Blonder, G.: Graphical Passwords. United States Paten 5559961, Lucent Technologies, Inc. (1996)
3. Chiasson, S., Biddle, R., van Oorschot, P.C.: A Second Look at the Usability of Click-based Graphical Passwords. In: Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), pp. 1–12, ACM, New York, (2007)
4. Chiasson, S., van Oorschot, P.C., Biddle, R.: Graphical Password Authentication Using Cued Click-Points. In: Proceedings of the 12th European Symposium on Research in Computer Security (ESORICS), pp. 359–374, Springer, Heidelberg (2007)
5. De Luca, A., Hang, A., Brudy, F., Lindner, C., Hussmann, H.: Touch Me Once and I Know It's You!: Implicit Authentication based on Touch Screen Patterns. In: Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems (CHI), pp. 987–996, ACM, New York (2012)
6. Davis, D., Monrose, F., Reiter, M.K.: On User Choice in Graphical Password Schemes. In: Proceedings of the 13th Conference on USENIX Security Symposium (SSYM), pp. 151–164, USENIX Association, Berkeley, CA, USA (2004)

7. Dirik, A.E., Memon, N., Birget, J.-C.: Modeling User Choice in the Passpoints Graphical Password Scheme. In: Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), pp. 20–28, ACM, New York (2007)
8. Dunphy, P., Heiner, A.P., Asokan, N.: A Closer Look at Recognition-based Graphical Passwords on Mobile Devices. In: Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS), pp. 1–12, ACM, New York (2010)
9. Gołofit, K.: Click Passwords under Investigation. In: Proceedings of the 12th European symposium on Research in Computer Security (ESORICS), pp. 343–358, Springer, Heidelberg (2007)
10. Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The Design and Analysis of Graphical Passwords. In: Proceedings of the 8th Conference on USENIX Security Symposium (SSYM), pp. 1–14, USENIX Association, Berkeley, CA, USA (1999)
11. Karlson, A.K., Brush, A.B., Schechter, S.: Can I Borrow Your Phone?: Understanding Concerns when Sharing Mobile Phones. In: Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI), pp. 1647–1650, ACM, New York (2009)
12. Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J.W., Nicholson, J., Olivier, P.: Multi-Touch Authentication on Tabletops. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI), pp. 1093–1102, ACM, New York (2010)
13. Lin, D., Dunphy, P., Olivier, P., Yan, J.: Graphical Passwords & Qualitative Spatial Relations. In: Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), pp. 161–162, ACM, New York (2007)
14. Meng, Y: Designing Click-Draw based Graphical Password Scheme for Better Authentication. In: Proceedings of IEEE International Conference on Networking, Architecture, and Storage (NAS), pp. 39–48 (2012)
15. Meng, Y., Wong, D.S., Schlegel, R, Kwok, L.-F.: Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones. In: Proceedings of the 8th China International Conference on Information Security and Cryptology (INSCRYPT), pp. 331–350, Springer, Heidelberg (2012)
16. Millennial Media. Mobile mix: The mobile device index. `http://www.millennialmedia.com/research` (September, 2012)
17. Nelson, D.L., Reed, V.S., Walling, J.R.: Pictorial Superiority Effect. Journal of Experimental Psychology: Human Learning and Memory 2(5), 523–528 (September 1976)
18. Oakley, I., Bianchi, A.: Multi-Touch Passwords for Mobile Device Access. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp), pp. 611–612, ACM, New York (2012)
19. Shepard, R.N.: Recognition Memory for Words, Sentences, and Pictures. Journal of Verbal Learning and Verbal Behavior 6(1), 156–163 (1967)
20. Suo, X., Zhu, Y., Owen, G.S.: Graphical Passwords: A Survey. In: Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC), pp. 463–472, IEEE Computer Society, USA (2005)
21. Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., Ben-David, S.: Biometric Authentication on A Mobile Device: A Study of User Effort, Error and Task Disruption. In: Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC), pp. 159–168 (2012)
22. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N.: Passpoints: Design and Longitudinal Evaluation of A Graphical Password System. Int. J. Hum.-Comput. Stud. 63(1-2), 102–127 (July 2005)
23. Zhang, Y., Xia, P., Luo, J., Ling, Z., Liu, B., Fu, X.: Fingerprint Attack against Touch-enabled Devices. In: Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), pp. 57–68 (2012)