Evaluating the Effect of User Guidelines on Creating Click-Draw based Graphical Passwords

Yuxin Meng  
Department of Computer Science  
City University of Hong Kong  
Hong Kong, China  
ymeng8@student.cityu.edu.hk

Wenjuan Li  
Computer Science Division  
Zhaqing Foreign Language College  
Guangdong, China  
wenjuan.anastatia@gmail.com

ABSTRACT
Graphical passwords have become one of the possible alternatives for traditional text-based passwords in the aspect of user authentication on computers and networks. In general, this image-based authentication can be classified into three categories based on their input methods: click-based graphical passwords, choice-based graphical passwords and draw-based graphical passwords. To integrate the merits of the above three image-based authentication schemes, we have developed a prototype of click-draw based graphical password scheme (called CD-GPS) that combined current graphical password techniques and evaluated its performance with human users. In real deployment, we notice that user guidelines can affect the graphical password creation. However, the effect of user guidelines is seldom explored in the enrolment process of current graphical password schemes. In this study, we therefore aim to investigate the effect of giving user guidelines to users on the creation phase of our developed click-draw based graphical passwords. In particular, we conducted two experiments to explore the effect of user guidelines in our study with 60 participants and the experimental results indicate that by applying user guidelines into the phase of password creation, users can overall create better click-draw based graphical passwords.

Categories and Subject Descriptors
D.4.6 [Operating Systems]: Security and Protection—Authentication; H.5.2 [Information Interfaces and Presentation]: User Interfaces—Graphical user interfaces (GUI)

General Terms
Security, Human Factors

Keywords

1. INTRODUCTION

Authenticating users by means of images is one of the possible alternatives for traditional text-based passwords. Previous studies have indicated that the text-based authentication had drawbacks with regard to both usability and security [17]. For example, users have difficulty in remembering complex and random passwords which is known as long-term memory (LTM) limitations. Therefore, it is highly possible that users choose simple and short passwords for easy memorization. In such case, users who fail to select and handle passwords securely can open holes for potential attacks [2].

To overcome the drawbacks of text-based passwords, graphical passwords have been proposed to enhance the user authentication. Psychology studies (e.g., [13, 11]) have shown that human brain was better at remembering and recognizing images than text (e.g., a random digital string). Several investigations and studies (e.g., [5, 12]) have reported positive results in the aspect of recall and memorability that users were able to remember their graphical passwords accurately after long periods of time.

Generally, image-based authentication can be divided into three categories based on their input methods: namely 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).

With regard to security, the main problem with the click-based graphical password schemes is referred to as ‘hot-spot’ that users are likely to click on the same or similar point on the provided image, or click on the same area when two or more images are given [15]. Similarly, the problem with the choice-based graphical password schemes can be referred to as ‘hot-image’ that users are likely to choose preferred image associated with their genders (i.e., girls prefer to select an image with flowers or lovely object). Several security studies in graphical passwords can be found in [6], [7] and [3].

To mitigate the problems in graphical password schemes, in our previous work [10], we have proposed and developed a click-draw based graphical password scheme (called CD-GPS) which can be regarded as a combination of the above three types of graphical passwords. The scheme of CD-GPS consists of two main steps: image selection and secret drawing. In the step of image selection, users are required to choose images in a story-sequence, while in the step of se-
cret drawing, users are required to click-draw their secrets by using a series of clicks.

Motivation. Intuitively, human is the most critical factor in the authentication procedure. Therefore, users are likely to better create their graphical passwords by offering appropriate user guidelines. However, seldom studies can be found in the research literature with the purpose of exploring the effect of user guidelines on graphical password creation. In addition, in the previous user study, some participants suggested that our scheme could provide several user guidelines for them to create their graphical passwords. Our motivation is therefore to investigate the effect of user guidelines on creating their graphical passwords.

In this paper, we mainly investigate the impact of user guidelines on creating click-draw based graphical passwords. In particular, we conducted two experiments with 60 participants as follows: (1) Recording created graphical passwords from 20 participants without user guidelines, and then recording created graphical passwords from the same 20 participants by providing them with user guidelines; (2) For the remaining 40 participants, we equally divided them into two groups. One group created graphical passwords without user guidelines and the other group created graphical passwords by providing with user guidelines.

By analyzing the collected data, we found that user guidelines could enhance the creation of click-draw based graphical password scheme to some extend, especially when users are not aware of any security problems (e.g., ‘hot-spot’ problem) in creating graphical passwords.

The remaining of this paper is organized as follows: in Section 2, we introduce background information of CD-GPS and present related work; Section 3 describes the user guidelines and experimental methodology; Section 4 describes the study results and analyzes the effect of user guidelines on creating click-draw based graphical passwords; and last, Section 5 concludes our work.

2. BACKGROUND

In this section, we first describe the details of click-draw based graphical password scheme. Then, we introduce some related work with regard to graphical passwords.

2.1 Click-Draw based Graphical Password Scheme

In our previous work [10], we proposed and developed a click-draw based graphical password scheme (called CD-GPS). There are two major operational steps in the scheme of CD-GPS: image selection and secret drawing.

The first step is image selection in which users are required to select some images from an image pool and remember this order of images like a story. 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).

To facilitate the action of click-draw, the scheme partitions the selected image, which is used for click-drawing secrets, into a \( N \times N \) table.

In our developed example system, the image pool contains 10 images. Users should first select 4 images out of the image pool and organize these images in a story order. Then, users have to further select 1 image for click-drawing their secrets. The selected image in the step of secret drawing will be divided into a 16 \( \times \) 16 table with 256 clickable squares. Our previous work showed that this graphical password scheme provided suitable properties in the aspect of both usability and security. The detailed steps in the example system of click-draw based graphical password scheme are illustrated in Figure 1.

Figure 1: The specific steps in the example system of click-draw based graphical password scheme.

2.2 Related Work

In recent years, a number of graphical password schemes have been proposed aiming to enhance the user authentication [14]. Blonder [1] first designed a click-based graphical password scheme that users could generate their passwords by clicking on several pre-defined locations on an image. For authentication, users are demanded to re-click on the same locations. Then, Wiedenbeck et al. [16] extended Blonder’s idea and developed a PassPoints system that users could click on any place on an image instead of several pre-defined locations. For the choice-based graphical passwords, Davis et al. [4] proposed a Story scheme that users could choose everyday images in a story order for authentication. Users were encouraged to generate their graphical passwords like a story with the purpose of helping them remember their passwords. For the draw-based scheme, Jermy et al. [9] proposed and developed a typical DAS (Draw-a-secret) scheme that allowed users to draw their passwords on a 2D grid. During the authentication, users should re-draw their pictures in the correct ordered sequence.

However, to the best of our knowledge, there are seldom studies to investigate or introduce user guidelines as part of the enrolment process for graphical password schemes, except for the work by Jali et al. [8] in 2011. In this work, the authors introduced a set of guidelines which was referred to as Graphical Password Guidelines (GPG) to users before they began choosing their secrets. In the experiment, they implemented two different types of data collection with internal and external groups. Their experimental results indicated that the implementation of guidelines alone could not guarantee the security of graphical passwords but might give positive or negative effects on the security.

In this study, we take the click-draw based graphical password scheme as an example to explore the effect of giving user guidelines to users in graphical password creation. The
motivation here is that users were encouraged us to provide them with several guidelines before they created their graphical password schemes in our previous studies, and following Jali et al.’s work, we expect to investigate the specific conditions that user guidelines can cause positive impacts on graphical password creation.

3. USER STUDY

In this section, we begin by presenting our proposed user guidelines used in the experiments and then we describe the detailed experimental methodology.

3.1 User Guidelines

We describe the user guidelines in Table 1. Specifically, the No.1 and the No.2 guidelines indicate users how to select their graphical passwords in the step of image selection. The remaining guidelines (from the No.3 to the No.7) instruct users how to click-draw their secrets. The construction of these guidelines is referred to the work by Jali et al. [8].

For choosing images, we suggest that users should select different themes and remember the order like a story, while regarding to click-draw secrets on an image, we suggest that users can click-draw a memorable secret such as a number or a letter. To improve the security, we further advise that users should click-draw several secret points on an image. We also suggest that users should not click-draw their secrets on an obvious area or the same area on multiple images.

3.2 Experimental Methodology

We conducted an in-lab user study which consisted of two experiments with totally 60 participants those who were interested in our work. All participants are university students with diverse backgrounds and did not join our previous studies. In particular, 25 participants (10 females and 15 males) are from the computer science department (not security related major) and the other participants are from other departments and majors. All participants are regular web users and ranged in age from 20 to 32 years.

Before the experiments, we gave an in-depth description of the CD-GPS, introduced our objectives in the user study and showed how to use our example system. Each participant could complete 2 practice trials before the real trials. To investigate the effect of giving user guidelines to participants on creating their click-draw based graphical passwords, we divided the participants into two experiments as below:

- Experiment1. This experiment involved 20 participants (by randomly selection) and required each participant to create up to 5 click-draw based graphical passwords.
  - Phase1. The 20 participants created their passwords without giving the user guidelines.

- Experiment2. This experiment involved the remaining 40 participants and these participants were randomly assigned to two groups. Each group contained 20 participants and each participant was required to create 5 click-draw based graphical passwords.
  - Group1. The 20 participants created their passwords without giving the user guidelines.
  - Group2. The other 20 participants created their passwords by offering the user guidelines.

The detailed participants’ information is shown in Table 2. For the Experiment1, we aim to evaluate the effect of giving user guidelines to users on creating their graphical passwords. That is, after giving the user guidelines, how participants re-create or change their previous passwords. For the Experiment2, we attempt to explore the conditions that user guidelines can cause positive impacts for participants on creating their graphical passwords.

Finally, we presented a set of questions to all participants and collected their feedback which could help our analysis work. Ten-point Likert scales were used in each question where 1-score indicates strong disagreement and 10-score indicates strong agreement. We denoted 5-score as the statement “It is hard to say” for a participant.

4. RESULTS AND ANALYSIS

In this section, we describe the results of both experiments and analyze the results by means of users’ feedback.

4.1 Experiment1

We give relevant questions to participants when they finished relevant phases. The questions and average scores are presented in Table 3 and Table 4 respectively. The average scores are simply average values calculated by the feedback of all participants. Table 3 is related to Phase1 while Table 4 is related to Phase2.

According to Table 3, most participants satisfied with the password creation in the click-draw based graphical password scheme. In addition, most participants believed that their passwords were different from others and were secure.
Table 3: Several questions and relevant scores in the Experiment1 without user guidelines.

<table>
<thead>
<tr>
<th>Questions</th>
<th>Score (average)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. I could easily create a password in the experiment</td>
<td>8.7</td>
</tr>
<tr>
<td>2. I think my created passwords are very different than others</td>
<td>8.1</td>
</tr>
<tr>
<td>3. The created passwords are easy to remember</td>
<td>7.8</td>
</tr>
<tr>
<td>4. I believe that my passwords are secure</td>
<td>7.2</td>
</tr>
</tbody>
</table>

Table 4: Several questions and relevant scores in the Experiment1 by giving user guidelines.

<table>
<thead>
<tr>
<th>Questions</th>
<th>Score (average)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. I could more easily create a password in the experiment by providing the user guidelines</td>
<td>8.5</td>
</tr>
<tr>
<td>2. The user guidelines are no use in help create more secure passwords</td>
<td>2.3</td>
</tr>
<tr>
<td>3. I do not prefer to combine the user guidelines as part of the password enrolment</td>
<td>3.8</td>
</tr>
<tr>
<td>4. I think that my previous created passwords were secure enough without giving user guidelines</td>
<td>3.2</td>
</tr>
<tr>
<td>5. I believe that my passwords are secure by giving user guidelines</td>
<td>8.9</td>
</tr>
</tbody>
</table>

After giving user guidelines, all participants were required to re-create their passwords. They can choose to generate the same passwords or change their passwords. We evaluated the effect of user guidelines by identifying the differences of their created passwords. In Table 4, the No.1 question with the score of 8.5 showed that most participants were more easily to create their graphical passwords by offering the user guidelines. Importantly, most participants believed that the user guidelines could help them create better graphical passwords, thus, the average score of the No.2 question with the statement of “The user guidelines are no use in help create more secure passwords” is only 2.3. The main reason is that participants can better understand which kind of graphical passwords are secure by giving the user guidelines. The scores in the No.4 and the No.5 questions indicated that, without the user guidelines, most participants were not sure whether their created passwords were secure or not.

With regard to the No.3 question, most participants indicated that they preferred to combine the user guidelines as part of password enrolment. In addition, some participants pointed out that these user guidelines were very helpful since they have not created graphical passwords before, but they could know how to generate secure passwords by learning these guidelines.

To further analyze the experimental results, we calculate the trials’ information as shown in Table 5. There are totally 100 trials in each phase. In the Phase1, most participants preferred to click on 4 or 5 clickable squares in an image. No participants were chosen to click on more than 7 clickable squares. But in the Phase2, most participants preferred to increase the number of clicks. For example, 10 percent trials used 8 and 9 clicks respectively and most participants chosen 6 clicks to construct their graphical passwords. The number of 4-click graphical passwords is reduced from 38 trials (Phase1) to 5 trials (Phase2). The main reason is that, by offering the user guidelines, most participants were aware of adding some secret points to enhance their graphical passwords so that the number of clicks was increased.

Finally, we analyzed the password patterns which were created in these two phases. As illustrated above, the image pool of the click-draw based graphical password scheme contains 10 images with different themes (e.g., landscape, cartoon character, fruits, etc). Therefore, with respect to Phase1 and Phase2, we take the click-distribution map in the image of ‘snow landscape’ as an example, as shown in Figure 2 and Figure 3 respectively. In the Phase1, it is easily visible that the clicks mainly focused on the objects such as trees and mountains. In such case, these created graphical passwords are vulnerable to the ‘hot-spot’ or ‘hot-object’ attacks that attackers could use ‘hot-spot’ to launch dictionary attack.\(^1\) Whereas, by offering the user guidelines, in Figure 3, the clicks distributed more equally so that it is relatively more difficult for attackers to find the secrets compared to Figure 2. This example reflects the positive effect of giving user guidelines to users on creating CD-GPS passwords that user guidelines can help users to create more secure graphical passwords. The other created password patterns in the Experiment1 also verified this conclusion.

4.2 Experiment2

In this experiment, we also give a set of questions when the two groups finished their password creation. The major questions with their average scores are presented in Table 6 and Table 7 respectively.

Table 5: The number of clicks vs. trials in Phase1 and Phase2.

<table>
<thead>
<tr>
<th>The number of clicks</th>
<th>Trials in Phase1</th>
<th>Trials in Phase2</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 clicks</td>
<td>38</td>
<td>5</td>
</tr>
<tr>
<td>5 clicks</td>
<td>30</td>
<td>24</td>
</tr>
<tr>
<td>6 clicks</td>
<td>20</td>
<td>35</td>
</tr>
<tr>
<td>7 clicks</td>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td>8 clicks</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>9 clicks</td>
<td>0</td>
<td>10</td>
</tr>
</tbody>
</table>

\(^1\) A dictionary of graphical passwords can be built through combining these hot-spots on an image.
Table 6: Several questions and relevant scores in the Experiment 2 for Group 1.

<table>
<thead>
<tr>
<th>Questions</th>
<th>Score (average)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. I could easily create a password in the experiment</td>
<td>8.1</td>
</tr>
<tr>
<td>2. I think my created passwords are very different than others</td>
<td>7.3</td>
</tr>
<tr>
<td>3. The created passwords are easy to remember</td>
<td>9.0</td>
</tr>
<tr>
<td>4. I believe that my passwords are secure</td>
<td>7.5</td>
</tr>
<tr>
<td>5. I know how to generate a secure graphical password</td>
<td>6.8</td>
</tr>
</tbody>
</table>

Table 7: Several questions and relevant scores in the Experiment 2 for Group 2.

<table>
<thead>
<tr>
<th>Questions</th>
<th>Score (average)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. I could easily create a password in the experiment</td>
<td>8.5</td>
</tr>
<tr>
<td>2. I think my created passwords are very different than others</td>
<td>8.8</td>
</tr>
<tr>
<td>3. The created passwords are easy to remember</td>
<td>8.1</td>
</tr>
<tr>
<td>4. I believe that my passwords are secure</td>
<td>8.6</td>
</tr>
<tr>
<td>5. I know how to generate a secure graphical password</td>
<td>8.8</td>
</tr>
</tbody>
</table>

To generate a secure graphical password, the average score of 6.8 for Group 1 is significantly lower than the average score of 8.8 for Group 2. Most participants in Group 1 indicated that they have not created graphical passwords before so that they were not sure of whether their created passwords were secure or not. On the contrary, the participants in Group 2 indicated that they learned a lot from the user guidelines and could create good passwords even if they have not created such kind of passwords before.

To verify the results, we also calculate the trials’ information which is shown in Table 8. The statistical data shows that the participants in Group 1 preferred to use 5 or 6 clicks on their selected images. It is the same that the participants in Group 2 also preferred to click 5 or 6 clickable squares on an image. The main reason is due to usability that most participants feel comfortable by using these numbers of clicks. However, the statistical data in Table 8 shows that fewer participants (only 8%) in Group 2 selected 4 clicks to construct their graphical passwords than those (18%) in Group 1. We also analyzed the corresponding click-distribution map between these two groups. From the click patterns, we can also find that the clicks generated by Group 2 distributed more equally than those generated by Group 1.

Table 8: The number of clicks vs. trials in Group 1 and Group 2.

<table>
<thead>
<tr>
<th>The number of clicks</th>
<th>Trials in Group 1</th>
<th>Trials in Group 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 clicks</td>
<td>18</td>
<td>8</td>
</tr>
<tr>
<td>5 clicks</td>
<td>27</td>
<td>30</td>
</tr>
<tr>
<td>6 clicks</td>
<td>32</td>
<td>41</td>
</tr>
<tr>
<td>7 clicks</td>
<td>12</td>
<td>10</td>
</tr>
<tr>
<td>8 clicks</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>9 clicks</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

From the feedback, we can find that the participants in Group 2 were more confident with their created passwords. Whereas after analyzing the statistical data, the participants in Group 2 have not shown too much advantages in the aspect of click-numbers though they actually generated their passwords more securely. However, we find that the user guidelines are very effective for new users who did not use the graphical passwords before in terms of the participants’ feedback as well as the password-pattern analysis. Moreover, most participants indeed appreciated the effect of the user guidelines on helping create their passwords during the password creation.
Therefore, from the findings, we conclude that the user guidelines can positively impact the password creation by helping users generate more secure graphical passwords, especially for those users who do not know how to better create their graphical passwords. In addition, according to the Experiment2, we indicate that the user guidelines are also an important factor for generating a secure graphical password. Overall, the experimental results show that the user guidelines are very crucial for new graphical password users.

5. CONCLUDING REMARKS

Graphical password schemes have been regarded as a promising alternative to traditional text-based passwords. A lot of graphical password schemes have been proposed to enhance computer and network authentication. However, there is seldom work to investigate the effect of giving user guidelines to users on creating their graphical passwords.

In this study, we aim to investigate the effect of giving user guidelines to users on the creation phase of click-draw based graphical password. We conducted two experiments (Experiment1 and Experiment2) with totally 60 participants. In particular, we selected 20 participants in the Experiment1 to evaluate the effect of user guidelines. For the same participants, we find that the user guidelines give positive impacts on users when they re-create their graphical passwords. In the Experiment2, we equally divided the remaining 40 participants into two groups: Group1 and Group2. We only provided user guidelines for Group2 and compared the password patterns of these two groups. From the results, we find that the user guidelines are an important factor in generating a secure graphical password and can positively impact the password creation by helping users generate more secure graphical passwords, especially for those new users who do not know how to better create their graphical passwords.

Our work is conducted by means of the click-draw based graphical password scheme. Therefore, the future work could include a larger user study with much more participants to validate the effect of offering user guidelines to users on creating their graphical passwords. In addition, future work could also include further analysis of password patterns generated by different categories of graphical password schemes to verify our results. Moreover, we leave the construction of efficient and effective user guidelines as an open problem for our future study.

6. ACKNOWLEDGMENTS

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

7. REFERENCES