A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords

Weizhi Meng[1(✉)], Wenjuan Li[2], Wang Hao Lee[3], Lijun Jiang[2], and Jianying Zhou[4]

[1] Department of Applied Mathematics and Computer Science, Technical University of Denmark, Kongens Lyngby, Denmark
weme@dtu.dk
[2] Department of Computer Science, City University of Hong Kong, Kowloon Tong, Hong Kong
[3] Infocomm Security Department, Institute for Infocomm Research, Singapore, Singapore
[4] Singapore University of Technology and Design, Singapore, Singapore
jianying_zhou@sutd.edu.sg

Abstract. Today's computer users have to remember several passwords for each of their accounts. It is easily noticed that people may have difficulty in remembering multiple passwords, which result in a weak password selection. Previous studies have shown that recall success rates are not statistically dissimilar between textual passwords and graphical passwords. With the advent of map-based graphical passwords, this paper focuses on multiple password interference and presents a pilot study consisting of 60 participants to study the recall of multiple passwords between text passwords and map-based passwords under various account scenarios. Each participant has to create six distinct passwords for different account scenarios. It is found that participants in the map-based graphical password scheme could perform better than the textual password scheme in both short-term (one-hour session) and long term (after two weeks) password memorability tests (i.e., they made higher success rates). Our effort attempts to complement existing studies and stimulate more research on this issue.

Keywords: User authentication · Graphical passwords · Usable security · Multiple password interference · HCI

1 Introduction

Over the past few decades, text-based passwords are the most widely adopted method for user authentication. However, users may suffer from many issues when using text or pattern in the aspects of security and usability [6,35,38]. As an example, users find it difficult to remember their textual information for a long time due to the long-term memory (LTM) limitation [37]. As a result, they are likely to choose and use weak textual passwords. To mitigate these

D. Gollmann et al. (Eds.): ACNS 2017, LNCS 10355, pp. 145–162, 2017.
DOI: 10.1007/978-3-319-61204-1_8

drawbacks, graphical passwords (GPs) have been proposed as an alternative in the literature, where users are able to interact with images during the registration and authentication [29]. Generally, graphical passwords can be categorized as recognition-based, pure recall-based and cued recall passwords.

Many research studies have shown that graphical passwords can indeed help users in remembering passwords (see Sect. 2). However, nowadays users have to remember not just one password, but many, which would add a significant burden on users' memory. As a result, the concern of *multiple password interference* is raised, where for users, remembering a password for an account (e.g., email account) affects their memory of other accounts' passwords (e.g., Facebook account). In the literature, this issue has not been widely investigated, whilst one previous research had paid attention to this issue. They made a study between text-based passwords and click-based graphical passwords (*PassPoints*) [8]. In particular, the click-based GP system requires users to click on several points on an image rather than enter textual information [36]. They found that the click-based GPs were significantly less susceptible to multiple password interference in the short-term, while the results were not statistically different from textual passwords in the long-term (i.e., after two weeks).

Our current work was motivated by two observations. (1) In the literature, there have been few studies investigating this important issue of multiple password memory in the area of graphical passwords. (2) Map-based graphical passwords have been recently developed, where users can click on several locations on a world map as their secrets. A map is believed to provide better recall for users, but has not been investigated for multiple password memory. Based on this claim, our main goal of this paper is to investigate the multiple password interference between text-based passwords and map-based graphical passwords. More specifically, we develop a prototype of map-based GP in our study, which allows a sequence of three click-points on a digital world map. Furthermore, we follow the steps in the most relevant work [8], in order to facilitate the comparison and validation of the collected results.

More formally, *memory interference* can be described as "the impaired ability to remember an item when it is similar to other items stored in memory" [3]. In this work, our primary goal is to investigate the multiple password interference in text passwords and map-based GPs. The contributions of our paper are summarized below:

- A user study consisting of 60 participants was conducted to investigate the multiple password interference issue between textual passwords and map-based graphical passwords; where 50 of them successfully return after two weeks to test recall of those passwords they had created. They were assigned to use either text password system or map-based GP system. Each participant should create six distinct passwords for different account scenarios.
- It is found that participants can perform better in recalling multiple passwords using the map-based graphical passwords, not only in the short-term (e.g., a one-hour session) but also in the long-term (namely two weeks). In comparison with the results from former study (e.g., PassPoints), our results

indicate that map-based graphical passwords can offer a better and positive impact on recalling multiple passwords in both short and long term.

It is worth emphasizing that our study aims to complement existing research and reveals that recall of multiple passwords between text and map-based graphical password schemes has a statistically significant difference in both short and long term. The results also encourage research studies to develop proper map-based schemes to improve the issue of multiple password interference.

The remainder of the paper is organized as follows. Section 2 describes related work about graphical password classification, map-based graphical passwords and multiple password interference. Section 3 presents our developed map-based GP system and introduces our study methodology including procedure and steps. Section 4 analyzes the collected results. We provide a discussion in Sect. 5 and present some limitations in Sect. 6. Finally, we conclude our paper in Sect. 7.

2 Related Work

2.1 Graphical Passwords

Graphical password schemes can be classified into three broad categories [5,7]: namely, recognition-based, pure recall-based and cued recall-based.

- *Recognition-based GPs.* This kind of scheme requires users to select images from a large gallery. For example, PassFaces [10,25] lets users identify a set of human faces during the authentication phase. To create a password, the user chooses four images of human faces from a fixed portfolio of faces. The Story scheme [10] lets users identify a few images with a theme (e.g., people and food) from an image gallery.
- *Pure recall-based GPs.* Such kind of scheme lets users draw a secret on an image. An example is the DAS proposed by Jermyn et al. [17], where users draw the password on a grid. Tao and Adams [30] proposed Pass-Go that lets users select intersections within a grid as a way to enter their password. Based on Pass-Go, Android unlock patterns are developed on Android phones, which are a tuned application requiring users to unlock their phones by inputting correct patterns. Then, Dunphy and Yan [12] explored whether a background image can improve the performance of graphical passwords.
- *Cued recall-based GPs.* This kind of scheme requires users to click on a sequence of points to construct their passwords. *PassPoints* by Wiedenbeck et al. [36] belongs to this category. In *PassPoints*, users recall a sequence of five selected points by clicking on them. For authentication, users have to click close to the chosen click points within some (adjustable) tolerance distance. Later, Chiasson et al. [9] proposed *Persuasive Cued Click-Points* (*PCCP*), which lets users click a point on each of a sequence of background images.

The current graphical password schemes are designed around the actions of click, choice or draw. Combinations of these schemes have also been studied. For

instance, Meng [20] developed a click-draw based graphical password scheme (CD-GPS) with the purpose of improving the image-based authentication in both security and usability by combining the actions of clicking, selecting and drawing. Several new GP systems can be referred to [14,18,19,23]. There are many studies focusing on security aspect of graphical passwords [4,16,17,26,32,33] and relevant user behaviors [1,11,21,27,37,39].

2.2 Map-Based Graphical Passwords

Map-based GPs can be categorized as a kind of cued recall-based graphical password, in which users can recall their selected places on a world map. Despite some early research work, map-based GPs start becoming popular in recent years. In 2012, Georgakakis et al. [15] proposed a map-based graphical password scheme called *NAVI*, where the credentials of the user are his username and password formulated by drawing a route on a predefined Google map. In particular, a user selects the starting and the ending point, so that the route is calculated by the provider of the route planning service.

During the same time, Sun et al. [28] extended the above idea and suggested to use an extremely large image as the password space. They proposed a world map based graphical password authentication system called *PassMap*, in which a password consists of a sequence of two click-points on a large world map. To construct secrets, users can shift the world map to selected areas, and zoom the map to the desired zoom-level. An example of *PassMap* is shown in Fig. 1. Their collected results showed that after a week, the accuracy of login is 92.59%, and claimed that the performance was better than *PassPoints*. Later, Thorpe et al. [31] designed *GeoPass*, an interface for digital map-based authentication, where users can choose a single place as his or her password. For this scheme, users only have to remember the final location, rather than their method of navigating there. They included 35 participants in their study and found that nearly 97% of users could correctly remember their location-based-passwords over 8–9 days with very few failed login attempts. It is worth noting that *PassMap* and *GeoPass* are very similar in that secrets are constructed by clicking one or two places on a world map (e.g., Google map).

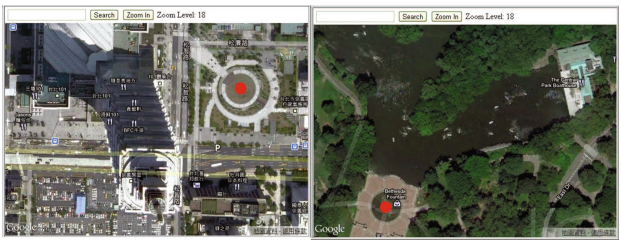

Fig. 1. An example of *PassMap*. The first click-point with red (Left) and the second click with red (Right). (Color figure online)

Recently, Meng [22] proposed *RouteMap* for better multiple password memory, which allows users to draw a route on a map as their password. They found that users could achieve better performance using *RouteMap* in terms of multiple password memory. From these studies, it is noticeable that users may have a better memorability regarding map-based graphical passwords.

2.3 Multiple Password Interference

Today, users have to remember more passwords rather than before in the course of their daily lives such as social networking accounts, personal email accounts, commercial email accounts and so on. In these cases, *multiple password interference* may become an important issue.

In the text password scheme, Vu et al. [34] had explored the memorability of multiple textual passwords for different accounts. The study discovered that users who were given five passwords have difficulty remembering them compared to those who only had to remember three. It is also revealed that users often selected passwords that have direct contextual relationship with the account(s) in question.

For the graphical password scheme, Everitt et al. [13] presented an early study on how frequency of access and interference affects recognition-based graphical passwords such as frequency of access to a graphical password. They employed *PassFaces* and discovered that many factors can noticeably impact authenticating with multiple facial graphical passwords. For example, participants who accessed four different graphical passwords per week were ten times more likely to completely fail to authenticate than participants who accessed a single password once per week.

Chiasson et al. [8] has conducted a study on comparing the recall of multiple text passwords against that of multiple click-based graphical passwords (namely *PassPoints*). Six account scenarios were simulated and they found that in the short-term, participants in the graphical password scheme performed significantly better than participants using the textual password scheme. They made fewer errors when recalling their graphical passwords. However, they found that recall success rates were not statistically different from each other after two weeks. More recently, Al-Ameen and Wright [2] showed that mental stories could be used to improve the interference issue in *GeoPass*. Meng et al. [24] presented a study on the memorability of multiple passwords between textual passwords and unlock patterns. The study also explored the difficulty of remembering those patterns for a prolonged period of time.

It is worth noting that recent research studies had showed that the performance of map-based GPs could be better than *PassPoints*; thus our current work is timely for the investigation of multiple password interference between textual passwords and map-based GPs. Our work is different from [2,24], as our used map-based scheme is not the same (i.e., *GeoPass* only allows one location to be selected). Thus, our study can complement existing research results.

3 User Study

Following the methodology in the literature [8], we conducted a lab-based user study involving two sessions: Session-1 and Session-2. All participants were students from a university who had no prior information security training, as well as no prior experience with graphical passwords.

The first session, Session-1 lasted for approximately an hour, recruiting a total of 60 participants (M = 25.6 years; SD = 3; 32 females). During the study, we randomly selected 30 participants to the text password scheme (MText), while the others were assigned to the graphical password scheme (MMP). For Session-2, after two weeks, 50 participants were successfully returned to the lab and recalled their created passwords. Also, we provide a feedback form for each session asking for users' feedback and attitude.

3.1 Implementation of Map-Based Graphical Passwords

As the source of existing map-based graphical passwords was not released, we developed a prototype of map-based graphical passwords in our lab computers with a 17-inch screen (Intel R, CPU 2.6 GHz). It is worth noting that our system provides a common platform that is able to realize several existing map-based GPs such as *PassMap* and *GeoPass*.

To obtain a world map, we utilized the JavaScript based Google Maps API, which provides an extensive move-by-dragging, zooming and search functions. When users zoom in/out on the map, our system reports the zoom-levels. The search function allows users to shift to a specific part of the map quickly and further zoom in to locate a specific area. Similar to [28], our system embedded a 640×420 pixel frame block for displaying the world map in a web page and road map instead of satellite-type map is used by default. The tolerance areas are 21×21 pixels.

We describe the registration and login phase of our developed map-based GP in Fig. 2 and Fig. 3, respectively.

- *Registration.* Figure 2 depicts that users are able to choose three locations on a world map in constructing their passwords. All the information like coordinates will be forwarded and stored in a database.
- *Login.* Figure 3 presents that users have to submit their names and three locations to the system for authentication. The system will compare the inputs with the stored information (i.e., checking whether the inputs are within tolerance). A user is successfully verified only if both credentials are correct.

It is worth noting that *PassPoints* requires users to select five points on an image as their secrets, *GeoPass* requires users to select one place while *PassMap* needs users to click two places. Intuitively, we consider the memory of one place in a map should be quite easy. To make a better comparison with *PassPoints*, our map-based GP system increases the memory burden a bit and thus demands users to choose three locations on a world map (as a study).

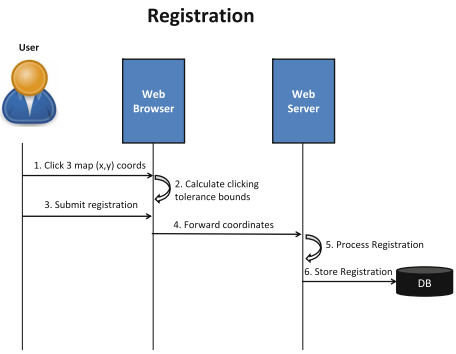

Fig. 2. Our developed system of map-based GP: registration phase.

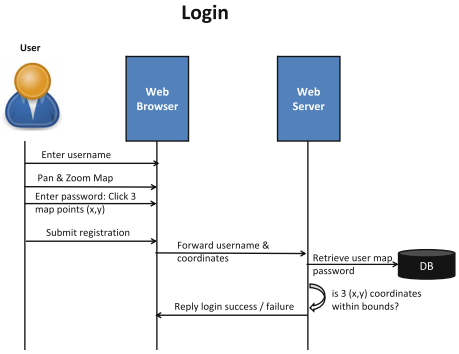

Fig. 3. Our developed system of map-based GP: login phase.

3.2 Session-1: Procedure and Steps

Session-1 consists of three phases: password practice, password creation and password retention. During the first phase, participants must complete two trials as practice to get them familiarized with the graphical password creation. In this phase, participants are not required to remember their practice passwords.

In the second phase (password generation), each participant has to complete six trials. Each password is associated with a different account scenario. A total of six account scenarios are constructed: email, bank, instant messenger, library, online dating and work (commercial). The accounts were identified by distinct banners at the top of the system interface. For map-based GP system, Fig. 4 depicts an example of registration interface with library account. It is worth noting that the banners are the same for text and map-based passwords.

In Fig. 5, we detail the process of registration, where Fig. 5(a) shows the interface that requires users to input their names and Fig. 5(b) allows users to select locations on a Google world map to create their secrets. After selecting locations, the click points including X and Y coordinates and zoom-level will be

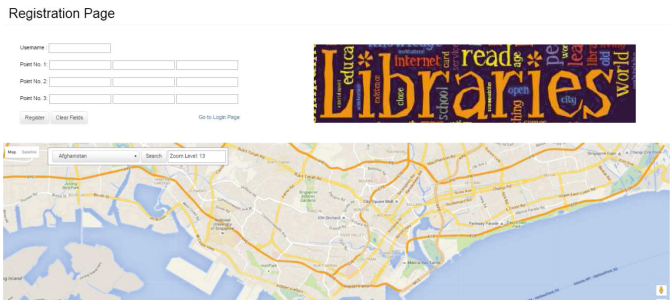

Fig. 4. The interface of map-based password creation.

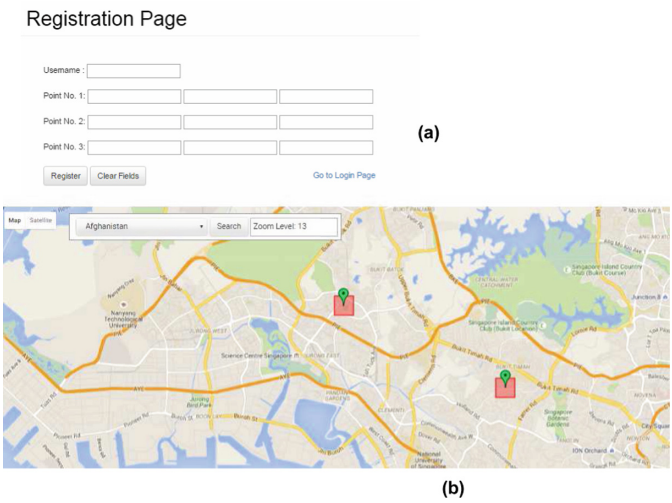

Fig. 5. Registration process: (a) inputting user name and (b) selecting locations.

shown in Fig. 5(a). To facilitate location search, our system provides a search bar in the map (see Fig. 5(b)) as well as zoom-level selection. Besides, users can switch the map between road and satellite map background.

In this stage, all accounts were presented to participants in the same order. In addition, participants were asked to construct their passwords which they could remember but would be difficult for attackers to guess. All participants were told that they would have to remember their created passwords for later use and each password was connected to a specific account scenario. Participants perform the steps below for each account:

- *Creation.* Participants have to create a password for each account. The textual password must consist of at least eight characters (this number is selected based on [8]) and entered twice. The password text was made visible during the creation process. For the graphical password, participants follow the steps in our system. This comprises choosing three different locations on a Google world map (see Fig. 4).
- *Confirmation.* In the text password scenario, participants have to enter their password (shown as asterisks), while they have to choose the same places in the graphical password scheme. If participants unexpectedly cannot remember their created password, they have the choice returning to the last step to create the password again.
- *Feedback.* Participants were invited to provide feedback to our questions (in the form of 10-point Likert-scale) about the creation and memory of the current passwords.
- *Distraction.* A 2-min interlude is given to each participant as a distraction task. First of all, participants counted backwards by 3 s from a random 4-digit number, and then participants were given a Mental Rotations Test puzzle

(MRT). Similar to [8], the purpose of these tasks was to clear participants' visual and textual working memory.
– *Login.* Participants were then invited to login with their created passwords. In the event that the password is mis-entered, they are allowed to re-enter their passwords multiple times with no pre-defined limit. If their created secrets are forgotten, they are allowed to return to the creation step.

Before the start of retention phase, participants were given a 10-min break where they were given a demographics questionnaire and could leave the experiment venue for the remaining break time. Upon returning from the break, account scenarios were presented to participants in a re-shuffled order with the help of a Latin square, where each row is connected with a participant and each column is connected with an account. All participants are required to recall each of their six textual or graphical passwords.

After this phase, participants were given another questionnaire to solicit feedback about their attitudes towards system usage and password memory.

3.3 Session-2: Procedure and Steps

Up to 50 participants returned to our lab after two weeks, among which 22 of them were previously assigned to the text password scheme. This session consists mainly of the 2-week retention phase, which follows the similar steps as per the initial retention phase during Session-1. The account scenarios were presented in the same order.

Similarly, participants are allowed to try multiple times with no limit to recall their created passwords until they gave up trying to recall. After the end of the session, a questionnaire was given to collect their feedback about password recall in these two schemes.

4 Results and Analysis

The Chi-square (χ^2) tests are mainly used to analyze data from the user studies. In all cases, we regard a value of $\rho < 0.05$ indicating that the results are statistically different between two schemes. In particular, we employ success rates as one of the major measures to evaluate participants' performance. The success rates for each step are presented in Table 1.

Table 1. The success rates of login, recall-1, recall-2 and password-confirmation. MText: multiple text passwords. MMP: multiple map-based passwords.

	Confirmation		Login		Recall-1			Recall-2		
	MText	MMP	MText	MMP	MText	MMP	χ^2	MText	MMP	χ^2
First attempt	97%	97%	94%	99%	62%	96%	$\chi^2 = 43.2,\ \rho < 0.05$	43%	72%	$\chi^2 = 30.1,\ \rho < 0.05$
Three attempts	99%	100%	98%	100%	86%	98%	$\chi^2 = 27.4,\ \rho < 0.05$	55%	79%	$\chi^2 = 23.3,\ \rho < 0.05$
More attempts	100%	100%	99%	100%	89%	99%	$\chi^2 = 17.5,\ \rho < 0.05$	64%	82%	$\chi^2 = 19.5,\ \rho < 0.05$

During password confirmation and login, it is found that there was no statistically significant difference in success rates between these two schemes. The observations are in line with the results from the previous research work [8]. In the next parts, we discuss success rates in retention and recall errors.

4.1 Recall Success Rates

Recall-1. In this phase (short term), it is found that the success-rate differences between the two password schemes are statistically significant. For correct-first-time attempts, participants in the text password scheme only achieved a success rate of 62%, but those in the map password scheme could reach a rate of 96%. With correct-on-multiple attempts, the textual password scheme yielded a success rate of up to 89%, indicating that 11% participants eventually gave up. The map password scheme in contrast yielded a rate of 99%. In other words, for 11% trials in the text password scheme, participants cannot remember their passwords, but there are only 1% unsuccessful trials for the map-based GP. These results indicated that participants in the graphical password scheme were more likely to successfully recall their created passwords than those who were under the text password scheme.

Recall-2. During this phase, we found that participants in the text password scheme had more difficulty in remembering their passwords, while those in the graphical password scheme could perform better. As an example, for the first attempt, the former could only achieve a success rate of 43%, but the latter could reach 72%. With multiple attempts, the text password scheme eventually yielded a rate of 64%, while a rate of 82% could be reached by the latter. Differing from the previous study [8], our existing results reveal that success rates have statistically significant differences between these two password schemes.

In Table 2, we present the success rates of male and female participants during Recall-2. For the graphical password scheme, 80% males can correctly enter map-based passwords within three attempts as compared to 78% female participants. Finally, male participants can reach 84% while females can reach 80%.

Table 2. Success rates of male and female for the Recall-2.

	MText: male	MText: female	χ^2
First attempt	42%	44%	$\chi^2 = 4.3,\ \rho > 0.05$
Within three attempts	53%	47%	$\chi^2 = 4.7,\ \rho > 0.05$
Multiple attempts	68%	60%	$\chi^2 = 5.4,\ \rho > 0.05$
	MMP: male	MMP: female	χ^2
First attempt	78%	76%	$\chi^2 = 4.1,\ \rho > 0.05$
Within three attempts	80%	78%	$\chi^2 = 4.5,\ \rho > 0.05$
Multiple attempts	84%	80%	$\chi^2 = 4.8,\ \rho > 0.05$

The results are similar under the text password scheme, where male participants could achieve 53% within three attempts and eventually 68% with multiple attempts. In contrast, female participants could achieve 47% and 60%, respectively. However, the results have no statistically significant differences ($\rho > 0.05$). This indicates that there is no apparent difference between male and female.

In [8], the results showed that males tend to perform better than females when using *PassPoints*, as males are good at visual-spatial tasks. By contrast, our system reduces such gap between males and females. Considering only statistics, participants in our study were performed generally better than the results reported by [8]. This implies that map-based GP can enable users to have a better memory of multiple passwords, as compared to *PassPoints*.

To understand the different observations, we further analyzed the collected data and informally interviewed the returned participants, where 90% of them gave their feedback. It is found that participants could connect their created map-based passwords with their past experience such as tours, visits, conference locations and so on. That is, when they have to input passwords in different account scenarios, they can link the account scenarios to their previous memory. For example, one participant said that "*When I have to input my map password to a work account, I can quickly remind of several locations where I have been*". During the interview, we found that such relationships can generally enhance the memory accuracy and strength in the long-term.

4.2 Recall Errors

Recall-1. As shown in Table 3, participants made 183 errors in the text password scheme, whilst they made 15 errors in the graphical password scheme. Since we allow participants to try many times for an account, the number of errors is bigger than the number of trials.

To look closer to the types of errors, participants are vulnerable to multiple password interference under the text password scheme. It is found that 21 out of 30 participants made recall errors.

- *Wrong account.* Many participants tried a wrong password for an account. For example, some of them tried a password from instant message on an online dating account. Some of them made mistakes between bank account and work account.
- *Wrong account variant.* This error means that participants entered some variant of the correct password for another account.
- *Misspelled variant.* Up to 20 errors were made because of wrong spells. For example, some participants entered "lxyy1987" instead of "Lxyy1987".
- *Unknown errors.* These errors were not belonging to any types above. Some participants reflected that they may try a password other than one they created during the study.

The errors made in the text password condition and the graphical password condition are summarized in Table 3 and Table 4, respectively. The main observations regarding the graphical password condition are discussed as below.

Table 3. Classification of recall errors for the text password scheme.

Type of error	Recall-1	Recall-2
Wrong account	90	88
Wrong account variant	42	24
Misspelled variant	20	73
Unknown	31	40
Total number of errors	183	225

Table 4. Classification of recall errors for the map-based password scheme.

Type of error	Recall-1	Recall-2
Outside tolerance	5	15
Incorrect click order	2	7
Forgotten locations	3	8
Incorrect zoom level	5	46
Total number of errors	15	76

- *Outside tolerance.* There are up to five errors made for this sake, where participants could remember the general location, but may choose a place a bit far from the correct location. For example, some participants selected a place of car park, but clicked a "house" near the car park during the recall.
- *Incorrect click order.* Not many, but still two errors were made since participants selected their locations in a wrong order.
- *Forgotten locations.* Some participants may forget their locations, or tried a location from another account. All these errors belong to this type.
- *Incorrect zoom level.* Zoom level selection is a feature of map-based graphical passwords, which can help enlarge the password space. However, we find that a few participants may make errors by selecting a wrong zoom level, or even forget the correct level.

Recall-2. Overall, participants made significantly more errors when inputting their passwords after two-weeks, under either the text password scheme, or the graphical password scheme. There are totally 225 errors made related to text passwords, while 76 errors made for map-based passwords. The recall results have statistically significant differences in these two schemes: MText: ($t = 3.73,\ \rho < 0.05$) and MMP ($t = 4.81,\ \rho < 0.05$).

For the text password scheme, most errors were made because of "wrong account" and "misspelled variant", which cover up to 67% of the total errors. Some participants may cycle through their passwords or variations of their passwords when they forget the correct secret for a specific account. These observations are in line with [8].

For the graphical password scheme, most errors were caused by tolerance and zoom level, which claim a percentage of nearly 80% total errors. It is found that participants are more likely to click a place out of the tolerance or forget to check the zoom levels. For example, some participants could choose the correct location, but ignore the zoom level, resulting in a wrong trial.

5 Discussion

5.1 User Feedback

As stated earlier, after each session, we provided each participant some questions to collect their feedback and attitude towards system usage and multiple password interference. The major questions along with the scores are shown in Table 5. In particular, 10-point Likert scales were used in each feedback question ranging from 1 to 10, where 1-score indicates strong disagreement and 10-score indicates strong agreement.

- *System usage.* According to the first two questions, most participants considered that both system interfaces are easy to use (i.e., both scores are above 9 on average).
- *Recall-1.* Regarding the third and fourth question, it can be observed that most participants can remember multiple passwords within a short time. The score in the graphical password scheme is a bit higher than that in the text password scheme (8.9 versus 8.4).
- *Recall-2.* Most participants indicated that they had difficulty in remembering multiple textual passwords after two weeks, in which the score is only 4.5. In contrast, the score in the password scheme reached 7.6, which is much better. The feedback shows that participants can have a better capability of remembering multiple map-based passwords.
- *Preference.* It is found that participants gave a positive score (8.2 on average) to the map-based GP system, presenting their interests in using map-based passwords in practice. In comparison, the text password scheme only received a score of 5.3.

Table 5. Main questions and relevant scores from users' feedback.

Questions	Score (average)
1. The text password interface is easy to use	9.1
2. The map-based password interface is easy to use	9.0
3. I easily remembered the created map passwords after one hour	8.9
4. I easily remembered the created text passwords after one hour	8.4
5. I easily remembered the created map passwords after two weeks	7.6
6. I easily remembered the created text passwords after two weeks	4.5
7. I prefer using the map-based passwords instead of text passwords in practice	8.2
8. I prefer using the text passwords instead of map-based passwords in practice	5.3
9. I am able to manage multiple map-based passwords	8.3
10. I am able to manage multiple text passwords	6.3

– *Password management.* The last two questions have a score of 8.3 and 6.3, respectively. These indicate that most participants believed that they can handle multiple passwords in the graphical password scheme. Most of them stated that map locations are more easily to recall.

It is worth noting that these scores are subjective, but they reflect participants' confidence in their password generation and management. We also interviewed up to 80% (48 out of 60) participants to explore why they provide such scores. Our interests are mainly focusing on participants' feedback in relation to Recall-1, Recall-2 and password management.

– For Recall-1, most participants (40 out of 48) stated that they could remember both types of passwords in the short term. Some of them reflected that they had some techniques in remembering text passwords, or could employ some strategies based on their own experience.
– For Recall-2, most participants (43 out of 48) supported that they can remember map-based graphical passwords much better, as the map provides many cues for them to recall their selected locations. As an example, one participant revealed an example of the created map-based secret as: 'A school', 'B park' and 'C mall'. In real life, this participant will go to 'A school', through 'B park' and 'C mall' sequentially. Thus, it is easily to recall the password as long as he can remember this route for a specific account.

For password management, most participants (38 out of 48) advocated that they could have a better memory of multiple passwords in the graphical password scheme. For instance, one participant said that he could simply use different routes to create map-based passwords. Some participants said that their map-based passwords were generated based on their past experience in tourist and conference; thus, it is very convenient for them to remember the passwords for a long time.

5.2 Comparison with Map-Based GPs and PassPoints

Both map-based GPs and *PassPoints* belong to the kind of cued recall-based graphical password, where users are able to select a set of points on an image to construct the secrets. By considering the results from [8], both graphical passwords can be easier to recall than text passwords in the short term. These results indicate that most participants can manage multiple graphical passwords with different accounts.

By contrast, after two weeks, Chiasson et al. [8] showed there was no significant difference in recalling multiple passwords between *PassPoints* and text passwords. However, our study reveals that participants can still cope with multiple map-based passwords better than text passwords in the long term (after two weeks). There are two major reasons:

– *Background selection.* For map-based GPs, users can choose their own map background, i.e., they can zoom in or zoom out the map to a particular area and choose their preferred locations. In contrast, they have limited selections in *PassPoints*, with an image pool including several pre-loaded images.

– *Map locations.* Users can choose locations on a world map in the map-based GP. In *PassPoints*, they should click several points on an image. We find that locations are more useful for users to remember, as these places are usually familiar to them. At least, they have a general understanding of the selected location. Therefore, they can link the locations to facilitate their long-term memory. In comparison, five clicks in *PassPoints* may not provide much information for users to link these clicks to a particular account. For instance, users should click some objects to improve their memory; however, there may no strong relation between clicks, causing users unable to remember their clicks after a long period.

On the whole, our discussion revealed that users are empowered with better recall capability of multiple graphical passwords with the map-based graphical passwords rather than *PassPoints*.

6 Limitations

Lab Study. Our primary goal in this study is to examine the multiple password interference between textual and map-based graphical passwords. We followed the established methodology in the literature for study steps and working memory clearance. However, we acknowledge that the lab study may not reflect password usage in real lives. For instance, participants have to construct six new passwords one after another and recall them in a short time, which seldom occur in practice. In the lab environment, we found that participants may create passwords with medium strength. For example, participants in the text password scheme may generate some weak passwords, where easy patterns could be identified. By contrast, participants in the graphical password scheme can generate better secrets. Still, our study results provide useful information and complement existing research in this area.

Participants. Current participants in our study were mainly students, but this does not dimmish the results of our work. In future work, diverse participants can be considered to validate our results. Besides, all participants did not have any prior experience in utilizing any map-based graphical password system, but they have much experience in constructing text passwords. In this case, participants should have an advantage when recalling text passwords. Interestingly, our results showed that there was a significant difference in recalling text and map-based passwords. It is found that participants could handle multiple map-based passwords better than text passwords, since map can provide cues for participants when they recalled their secrets.

User Study. In the previous work with *PassPoints*, it is found that the connection between account and clicks is not clear. Participants were likely to select click-points in simple patterns such as a straight line or C-shape [8]. These indicate that participants tried to connect their passwords with their accounts for better recall. From our existing data, we reveal that there is a potential of enhancing multiple password memory through designing graphical passwords in

an even proper way. That is, users can have a better recall capability of multiple graphical passwords when connecting passwords to their past experience. From this view, map provides many locations for users to select in terms of their own experience. Our implication could be verified in even larger studies.

Despite these limitations, our study provides interesting results to understand the effects of password interference, which can complement existing research.

7 Conclusion

Motivated by the recent development of map-based graphical password schemes, we conducted a two-phase user study with 60 participants to investigate the issue of multiple password interference between text passwords and map-based passwords. After two weeks, up to 50 participants successfully returned. In the study, each participant has to create and remember district passwords for six different account scenarios. Overall, we find that participants in the graphical password scheme can perform better than those in the text password scheme, not only in the short-term (one-hour session), but also in the long-term (after two weeks). Our current results reveal that participants can cope better with map when recalling multiple passwords. In particular, it is found that participants indeed made fewer recall errors in the map-based graphical password scheme than those in the text password scheme. Our work aims to complement existing work and stimulate more research in this area.

Acknowledgments. We would like to thank all participants for their hard work and collaboration in the user studies (e.g., data collection), and thank all anonymous reviewers for their helpful comments. This work was partially supported by SUTD start-up research grant SRG-ISTD-2017-124.

References

1. Alt, F., Schneegass, S., Shirazi, A.S., Hassib, M., Bulling, A.: Graphical passwords in the wild - understanding how users choose pictures and passwords in image-based authentication schemes. In: Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI), pp. 316–322 (2015)
2. Al-Ameen, M.N., Wright, M.: Multiple-password interference in the GeoPass user authentication scheme. In: Proceedings of NDSS Workshop on Usable Security (USEC), pp. 1–6 (2015)
3. Anderson, M.C., Neely, J.H.: Interference and inhibition in memory retrieval. In: Memory. Handbook of Perception and Cognition, chap. 8, 2nd edn, pp. 237–313. Academic Press (1996)
4. Bianchi, A., Oakley, I., Kim, H.: PassBYOP: bring your own picture for securing graphical passwords. IEEE Trans. Hum.-Mach. Syst. **46**(3), 380–389 (2015)
5. Biddle, R., Chiasson, S., Van Oorschot, P.C.: Graphical passwords: learning from the first twelve years. ACM Comput. Surv. **44**(4), 19 (2012)
6. Bonneau, J.: The science of guessing: analyzing an anonymized corpus of 70 million passwords. In: Proceedings of the 2012 IEEE Symposium on Security and Privacy, pp. 538–552 (2012)

7. 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 (2007)
8. Chiasson, S., Forget, A., Stobert, E., van Oorschot, P.C., Biddle, R.: Multiple password interference in text passwords and click-based graphical passwords. In: Proceedings of the 2009 ACM Conference on Computer and Communications Security (CCS), pp. 500–511 (2009)
9. Chiasson, S., Stobert, E., Forget, A., Biddle, R.: Persuasive cued click-points: design, implementation, and evaluation of a knowledge-based authentication mechanism. IEEE Trans. Dependable Secure Comput. **9**(2), 222–235 (2012)
10. Davis, D., Monrose, F., Reiter, M.K.: On user choice in graphical password schemes. In: Proceedings of the 13th Conference on USENIX Security Symposium, pp. 1–11. USENIX Association (2004)
11. 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 (2007)
12. Dunphy, P., Yan, J.: Do background images improve "draw a secret" graphical passwords? In: Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS), pp. 36–47 (2007)
13. Everitt, K.M., Bragin, T., Fogarty, J., Kohno, T.: A comprehensive study of frequency, interference, and training of multiple graphical passwords. In: Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI), pp. 889–898 (2009)
14. Gao, H., Liu, X.: A new graphical password scheme against spyware by using CAPTCHA. In: Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), Article No. 21 (2009)
15. Georgakakis, E., Komninos, N., Douligeris, C.: NAVI: novel authentication with visual information. In: Proceedings of the 2012 IEEE Symposium on Computers and Communications (ISCC), pp. 588–595 (2012)
16. Gołofit, K.: Click passwords under investigation. In: Biskup, J., López, J. (eds.) ESORICS 2007. LNCS, vol. 4734, pp. 343–358. Springer, Heidelberg (2007). doi:10.1007/978-3-540-74835-9_23
17. 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, pp. 1–14. USENIX Association, Berkeley (1999)
18. Liu, C.-L., Tsai, C.-J., Chang, T.-Y., Tsai, W.-J., Zhong, P.-K.: Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone. J. Netw. Comput. Appl. **53**, 128–139 (2015)
19. Lopez, N., Rodriguez, M., Fellegi, C., Long, D., Schwarz, T.: Even or odd: a simple graphical authentication system. IEEE Lat. Am. Trans. **13**(3), 804–809 (2015)
20. Meng, Y.: Designing click-draw based graphical password scheme for better authentication. In: Proceedings of the 7th IEEE International Conference on Networking, Architecture, and Storage (NAS), pp. 39–48 (2012)
21. Meng, Y., Li, W.: Evaluating the effect of tolerance on click-draw based graphical password scheme. In: Chim, T.W., Yuen, T.H. (eds.) ICICS 2012. LNCS, vol. 7618, pp. 349–356. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34129-8_32
22. Meng, W.: RouteMap: a route and map based graphical password scheme for better multiple password memory. Network and System Security. LNCS, vol. 9408, pp. 147–161. Springer, Cham (2015). doi:10.1007/978-3-319-25645-0_10

23. Meng, W., Wong, D.S., Furnell, S., Zhou, J.: Surveying the development of biometric user authentication on mobile phones. IEEE Commun. Surv. Tutor. **17**(3), 1268–1293 (2015)
24. Meng, W., Li, W., Jiang, L., Meng, L.: On multiple password interference of touch screen patterns and text passwords. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI), pp. 4818–4822 (2016)
25. Passfaces. http://www.realuser.com/
26. Pinkas, B., Sander, T.: Securing passwords against dictionary attacks. In: Proceedings of the 9th ACM Conference on Computer and communications security (CCS), pp. 161–170 (2002)
27. Shin, J., Kancharlapalli, S., Farcasin, M., Chan-Tin, E.: SmartPass: a smarter geolocation-based authentication scheme. Secur. Commun. Netw. **8**(18), 3927–3938 (2015)
28. Sun, H.-M., Chen, Y.-H., Fang, C.-C., Chang, S.-Y.: PassMap: a map based graphical-password authentication system. In: Proceedings of the 7th ACM Symposium on Information, Compuer and Communications Security (ASIACCS), pp. 99–100 (2012)
29. 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 (2005)
30. Tao, H., Adams, C.: Pass-go: a proposal to improve the usability of graphical passwords. Int. J. Netw. Secur. **2**(7), 273–292 (2008)
31. Thorpe, J., MacRae, B., Salehi-Abari, A.: Usability and security evaluation of GeoPass: a geographic location-password scheme. In: Proceedings of the 2013 Symposium on Usable Privacy and Security (SOUPS), pp. 1–14 (2013)
32. van Oorschot, P.C., Stubblebine, S.: On countering online dictionary attacks with login histories and humans-in-the-loop. ACM Trans. Inf. Syst. Secur. **9**(3), 235–258 (2006)
33. van Oorschot, P.C., Salehi-Abari, A., Thorpe, J.: Purely automated attacks on passpoints-style graphical passwords. IEEE Trans. Inf. Forensics Secur. **5**(3), 393–405 (2010)
34. Vu, K.P.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., Schultz, E.E.: Improving password security and memorability to protect personal and organizational information. Int. J. Hum. Comput. Stud. **65**(8), 744–757 (2007)
35. Weir, M., Aggarwal, S., Collins, M., Stern, H.: Testing metrics for password creation policies by attacking large sets of revealed passwords. In: Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS), pp. 162–175 (2010)
36. 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 (2005)
37. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N.: Authentication using graphical passwords: effects of tolerance and image choice. In: Proceedings of the 1st Symposium on Usable Privacy and Security (SOUPS) (2005)
38. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password memorability and security: empirical results. IEEE Secur. Priv. **2**, 25–31 (2004)
39. Zhu, B.B., Yan, J., Bao, G., Yang, M., Xu, N.: Captcha as graphical passwords - a new security primitive based on hard AI problems. IEEE Trans. Inf. Forensics Secur. **9**(6), 891–904 (2014)