RouteMap: A Route and Map Based Graphical Password Scheme for Better Multiple Password Memory

Weizhi Meng[1,2](✉)

[1] Infocomm Security Department,
Institute for Infocomm Research, Singapore, Singapore
yuxin.meng@my.cityu.edu.hk
[2] Department of Computer Science,
City University of Hong Kong, Hong Kong, Hong Kong (SAR)

Abstract. Graphical passwords (GPs) are considered as one promising solution to replace traditional text-based passwords. Many GP schemes have been proposed in the literature such as PassPoints, DAS, Cued Click Points, GeoPass and so on. These schemes reported promising performance in their studies in the aspects of security and usability, however, we notice that these GP schemes may suffer from the issue of multiple password memory. In our first user study, it is identified that this issue has indeed become a big challenge. In real-world applications, users usually have to remember and maintain more than one password in different scenarios, thus, it is very essential to develop a better GP scheme to solve this issue. In this paper, we focus on map-based GPs and propose a scheme of RouteMap for better multiple password memory, which allows users to draw a route on a map as their secrets. In our second user study with 60 participants, it is found that users can achieve better performance using RouteMap in terms of multiple password memory, as compared with two similar schemes. Our effort attempts to complement existing studies and stimulate more research on this issue.

Keywords: User authentication · Multiple password memory · Graphical passwords · Map passwords · Security and usability

1 Introduction

For user authentication, text-based passwords should be the most commonly used method over the past few decades, where users have to input correct textual strings for registration and authentication. However, it has long been recognized that traditional text-based passwords are suffered from many issues associated with their security and usability [24,25]. For instance, users are hard to remember their passwords for a long time, especially complex and random passwords. Due to the long-term memory (LTM) limitations, users are likely to choose simple

W. Meng—The author is previously known as Yuxin Meng.

M. Qiu et al. (Eds.): NSS 2015, LNCS 9408, pp. 147–161, 2015.
DOI: 10.1007/978-3-319-25645-0_10

strings, which would significantly degrade the level of authentication security. The recent study shows that this situation would be even worse than previously believed (i.e., little variation in guessing difficulty) [1].

In this case, graphical passwords (GPs) have been proposed as a promising alternative to text-based passwords. It is known that people generally have better memory and recognition for images than textual strings [15,17]. This observation has motivated a large number of graphical password schemes, which involve users recognizing images or reproducing a drawing on images. For example, Jermyn *et al.* [11] designed *DAS*, a graphical password that allowed users to draw their own passwords on a 2D grid. Wiedenbeck *et al.* [23] then proposed *PassPoints*, a system that allowed users to click on any place on an image in creating their passwords. Later, Chiasson *et al.* [2] proposed a click-based graphical password scheme called Cued Click Points (CCP), which consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so that users could receive immediate implicit feedback and decide whether they are on the correct path.

Motivations. In real-world scenarios, people often have more than one password in hand, as they have to manage different accounts such as email accounts, commercial used accounts, social networking accounts, etc. Due to this, a good GP scheme should be easy for users to remember multiple passwords. However, we notice that multiple password memory has become an issue for current GP schemes, in which users are hard to remember all created GPs after some time. In this work, we focus on this issue and have two targets as follows.

- ***T1.*** The first target is to investigate whether users can remember multiple graphical passwords based on existing GP schemes.
- ***T2.*** The second target is to design a graphical password scheme for better multiple password memory.

Contributions. In order to achieve these two goals, we mainly conduct two user studies in this work. The first one evaluates two popular GP schemes: *DAS* and *PassPoints*. We then design a map- and route-based graphical password scheme called *RouteMap*, which allows users to draw a route on a map as their passwords. Afterwards, the second user study is conducted to investigate the performance of *RouteMap*, as compared to the state-of-the-art schemes. The contributions of this work can be summarized as follows.

- We first conduct a user study to explore whether users are able to remember multiple graphical passwords using *DAS* and *PassPoints*. These two schemes are selected due to their popularity and simplicity. It is found that multiple password memory has become an issue that cannot be ignored.
- We then focus on map-based GPs and design *RouteMap*, a map- and route-based GP scheme that allows to draw a route on a world map. This scheme aims to provide better multiple password memory and is different from previous schemes as we apply distinct rules of password creation.

- We further conduct another user study with 60 participants to investigate the performance of *RouteMap* as compared with two other similar schemes. Experimental results indicate that our scheme can achieve better performance in the aspect of multiple password memory.

The remaining parts of this paper are organized as follows. In Section 2, we review related work regarding graphical passwords, especially map-based graphical passwords. Section 3 describes our first user study relating to multiple password memory based on *DAS* and *PassPoints*. In Section 4, we introduce our proposed *RouteMap* in detail and conduct another user study to explore its performance. Finally, we conclude our work with future directions in Section 5.

2 Related Work

2.1 GP Classification

Graphical password schemes can be classified into three folders [3,19]: 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).

- *Recognition-Based GPs.* The recognition-based schemes require users to select one or more images from a large set. For instance, the application of *PassFaces* [16] requires users to recognize a set of human faces during authentication. The scheme of *Story* [5] requires users to recognize a set of images such as people and food from a large image pool.
- *Pure Recall-Based GPs.* The pure recall-based GPs usually ask users to draw something on an image as their passwords. A typical example of these GPs is *DAS* [11], which requires users to draw on a grid. Similarly, the scheme of *Pass-Go* [21] requests users to select intersections on a grid as a way to input a password. Based on *Pass-Go*, Android unlock patterns have been developed on Android phones, which are a tuned application requiring users to unlock their phones by inputting correct patterns.[1] Several similar schemes can be referred to [7,12].
- *Cued Recall-Based GPs.* This kind of graphical passwords demands users to click on a sequence of points to construct their secrets. The system of *PassPoints* belongs to this category where users have to recall a sequence of five selected points. As another example, Chiasson *et al.* [4] designed Persuasive Cued Click-Points (PCCP), which requires users to click a point on each of a sequence of background images.

The current GP schemes are mainly based on the actions of choice, click and draw, so that some combined schemes have also been developed like [13]. Several analyses and studies on GPs can be referred to [6,10,14]

[1] https://www.berkeleychurchill.com/software/android-pwgen/pwgen.php.

2.2 Map-Based Graphical Passwords

The initial idea of using digital map as a graphical password first appeared in [8], but not much details were given. Then, Spitzer *et al.* [18] developed an implementation of *CCP* that combined the graphical approach with user's familiarity with navigating through Google maps. In their work, users are presented with an image of the United States and simply click to where the key destination is located, using an approach of zooming levels. Their results with over 50 participants indicated that 60% of the users rated the system as easier to remember than text in terms of memorability.

Later, several map-based graphical passwords appeared in 2012. Georgakakis *et al.* [9] proposed a GP scheme called *NAVI*, where the credentials of a user are his username and a password formulated by drawing a route on a pre-defined map. They provided an analysis regarding the strength of the password, but no any user study was provided. Sun *et al.* [20] proposed a map-based GP authentication system called *PassMap*, in which a password consists of a sequence of 2 click-points selected on a world map. Their user study showed that *PassMap* passwords are easy to memorize in practice. Thorpe *et al.* [22] later designed *GeoPass*, a digital map-based authentication scheme, where a user chooses a place as his or her password. In the user study, they found that 97% of the users were able to remember their location password over the span of 8-9 days and most without any 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).

In this work, we focus on map-based GPs and show how to handle the issue of multiple password memory. Our designed *RouteMap* is more similar to *NAVI* [9], since both schemes require users to draw a route on a map. However, *RouteMap* is different from *NAVI*, because we apply distinct rules of password creation. More specifically, the creation of a route is different (i.e., the route in *RouteMap* is drawn using straight lines). In addition, we evaluate the performance of *RouteMap* in a user study while there are no any results reported in [9]. Our results aim to complement the existing literature regarding this topic.

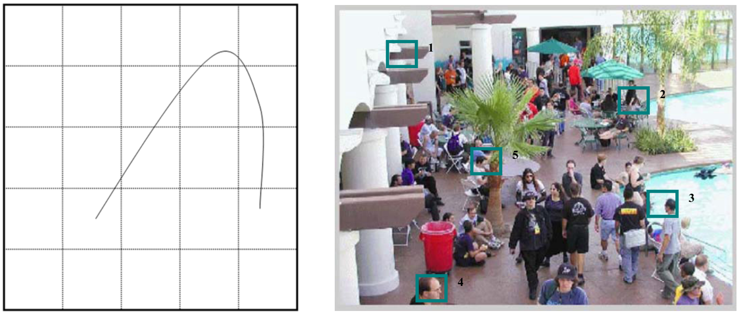
3 Multiple Graphical Password Memory

In this section, we conduct a user study with 50 participants to explore the issue of multiple password memory. According to the popularity and simplicity, we choose two existing GP schemes: *DAS* and *PassPoints*. The former is a pure recall-based GP, where users can draw their secrets on a grid. The latter is a cued recall-based GP, where users have to remember a sequence of several clicks. All participants are volunteers and have no background of information security (i.e., no participant has taken any courses related to information security before). The information of participants is shown in Table 1.

Methodology. Both schemes are implemented on the same computer settings and we introduced our objectives to all participants in advance. Two examples

Table 1. Detailed information of participants in the user study.

Age Range	Male	Female	**Occupation**	Male	Female
18-25	8	9	Senior people	3	2
25-35	8	8	Students	16	12
35-45	4	3	Researchers	3	3
45-55	2	3	Engineers	3	3
55-60	3	2	Business people	2	3



(a) DAS

(b) PassPoints

Fig. 1. Two graphical password schemes: (a) DAS and (b) PassPoints.

of these systems are depicted in Figure 1 (a) and Figure 1 (b), and the scheme details can be referred to [11,23]. To avoid bias, we set a file including all steps in the lab study and gave a detailed description to participants based on the same steps (i.e., how to use these two example systems).

Before the study, every participant can have 3 trails to get familiar with the example systems. In the study, we require all participants to create 5 passwords for each scheme and each password corresponds to a scenario as follows: the first password is created for an email account (personal use), the second one is created for a bank account, the third one is created for another email account (commercial use), the fourth one is created for a forum account and the last one is created for a social networking account. The detailed steps in each experiment are shown as below:

- *Experiment1.* This experiment requires each participant to create 5 *DAS* passwords.
  - Step 1. Creation: creating a password following the rules of *DAS*.
  - Step 2. Confirmation: confirming the password by drawing the same secrets in the correct place. If users incorrectly confirm their password, they can retry the confirmation or return to Step 1.
  - Step 3. Login: logging in the system with the created passwords. Users can cancel an attempt if they noticed an error.
  - Step 4. Feedback: All participants are required to complete a *feedback form* about the password creation and confirmation.

Table 2. Success rate for login to *DAS* and *PassPoints* after three weeks.

Experiment1 (DAS)	Successful Login	*Experiment2* (PassPoints)	Successful Login
1st time	132/250 (52.8%)	1st time	123/250 (49.2%)
2nd time	163/250 (65.2%)	2nd time	150/250 (60.0%)
3rd time	176/250 (70.4%)	3rd time	167/250 (66.8%)

DAS (Age in [18, 35])	Successful Login	*PassPoints* (Age in [18, 35])	Successful Login
1st time	98/165 (59.4%)	1st time	80/165 (48.5%)
2nd time	108/165 (65.5%)	2nd time	105/165 (63.6%)
3rd time	115/165 (69.7%)	3rd time	114/165 (69.1%)

DAS (Age in [35, 45])	Successful Login	*PassPoints* (Age in [35, 45])	Successful Login
1st time	12/35 (34.3%)	1st time	13/35 (37.1%)
2nd time	22/35 (62.9%)	2nd time	20/35 (57.1%)
3rd time	27/35 (77.1%)	3rd time	25/35 (71.4%)

DAS (Age in [45, 60])	Successful Login	*PassPoints* (Age in [45, 60])	Successful Login
1st time	21/50 (42.0%)	1st time	20/50 (40.0%)
2nd time	33/50 (66.0%)	2nd time	25/50 (50.0%)
3rd time	34/50 (68.0%)	3rd time	28/50 (56.0%)

– *Experiment2.* This experiment requires each participant to create 5 *PassPoints* passwords.

  - Step 1. Creation: creating a password following the rules of *PassPoints.*
  - Step 2. Confirmation: confirming the password by drawing the same secrets in the correct place. If users incorrectly confirm their password, they can retry the confirmation or return to Step 1.
  - Step 3. Login: logging in the example system with the created passwords. Users can cancel an attempted login if they noticed an error.
  - Step 4. Feedback: All participants are required to complete a *feedback form* about the password creation and confirmation.

Each participant will finish these two experiments in the same day. After three weeks, we require all participants to return and input all created passwords for these two schemes. Later, we provide another *feedback form* for participants about their password memory.

Results. In this user study, our main purpose is to explore whether users are able to remember and manage multiple graphical passwords. Therefore, we mainly describe and analyze users' performance after three weeks. The success rates of login to *DAS* and *PassPoints* within three attempts are described in Table 2. Three trails are determined based on the observation that most hosts or network accounts do not allow an authentication error more than three times. We have several major observations as below:

– *Overall Performance.* It is seen that participants can only achieve a success rate of 52.8% and 49.2% for *DAS* and *PassPoints* at the first attempt, respectively. After three trails, the success rate can be increased to 70.4% and 66.8%, respectively.

Table 3. Several main questions and relevant scores in the user study.

Questions	Score (average)
1. I could easily remember *DAS* passwords after one month	4.5
2. I could easily remember *PassPoints* passwords after one month	4.2
3. Are you willing to use *DAS* passwords in practice	3.2
4. Are you willing to use *PassPoints* passwords in practice	4.7
5. I can manage multiple *DAS* passwords	3.5
6. I can manage multiple *PassPoints* passwords	4.3

– *Age Impact.* In Table 2, we also presents the results according to three age groups. It is notice that participants who are aged from 35 to 45 can achieve the best performance in the experiments, while the success rate is not higher than 80% after three attempts (where the rate is 77.1% for *DAS* and 71.4% for *PassPoints*). Overall, it is found that younger participants have some advantages in multiple password memory.

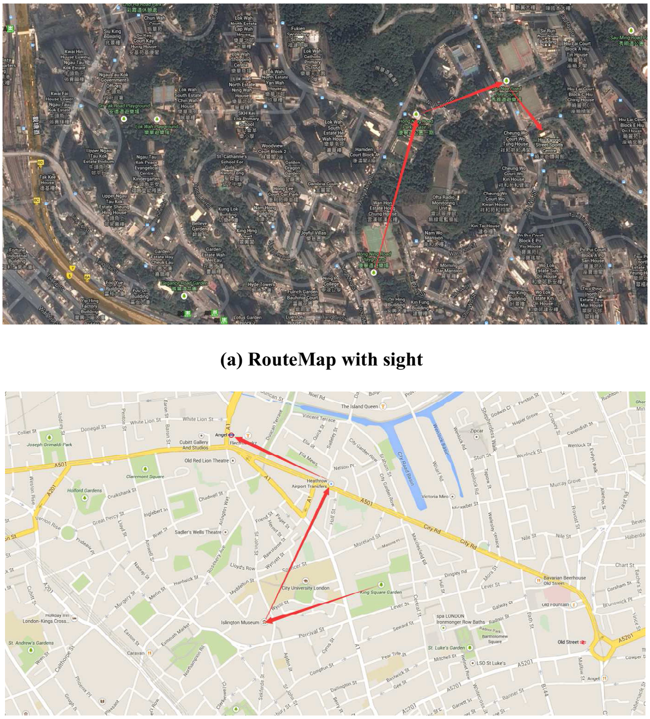
Based on the results, it is found that participants did not show satisfied capability in remembering these two GP schemes. To investigate this issue, we collect the feedback forms and present some key questions/feedback in Table 3. Ten-point Likert scales were used in each feedback question where 1-score indicates strong disagreement and 10-score indicates strong agreement.

It is seen that participants cannot remember these two GPs for a long time, where the average scores of the first and the second question are lower than 5. In addition, most participants are not willing to use these GPs in real-world applications. Similarly, most participants feel it is difficult to remember multiple GPs. We informally interviewed most participants and find two major reasons: (1) for *DAS*, it is not easy to link the graphical password to corresponding accounts and (2) for *PassPoints*, it is easily to forget the click-points when creating more than 3 passwords. Up to 80% participants reported that they have more than 5 different textual passwords in use.

Discussions. This is an initial study which can be improved in the aspects of involved users and GP numbers, while the results indeed indicate that multiple password memory has become a challenging issue for current graphical passwords. In this case, we argue that this issue should be given more attention when designing a graphical password scheme and it is crucial to develop GP schemes targeting for better multiple password memory.

4 RouteMap for Better Multiple Password Memory

Based on the study and feedback above, we have two other findings: (1) a background image can help users to remember their secrets, and (2) users should be provided with a few guidelines for creating their GPs. In this section, we describe our proposed *RouteMap* in detail and conduct a user study to investigate its performance, as compared with two similar schemes.



(a) RouteMap with sight

(b) RouteMap without sight

Fig. 2. *RouteMap*: (a) a pattern with sight and (b) a pattern without sight.

4.1 RouteMap

Our designed *RouteMap* is a kind of map-based graphical passwords, which allows users to draw a route on a map. There are three main reasons why we choose a map to build a GP scheme for better password memory.

- Map-based graphical passwords such as *PassMap* and *GeoPass* can provide large password space (e.g., $2^{36.9} for GeoPass$).
- Map can be easily zoom in or zoom out, so that users can choose a background image which they feel suitable.
- Previous studies show that map-based GPs have good usability (i.e., *GeoPass* shows that 97% participants can remember their passwords over a span of 8-9 days).

Our Scheme. As described earlier, *RouteMap* allows users to draw a route on a map (e.g., Google map). To enhance the memory, *RouteMap* allows users to choose a road-based map or a satellite map to draw their passwords. This because different people may have their own preference in background. In this work, we call it as *sight*. In Figure 2, we present two examples of *RouteMap* patterns with and without sight.

Taking Figure 2 (b) as an example, for this pattern, a user needs to click on the playground first, then move and click on a park and another playground, and finally click and stop at a sport center. Thus, a *RouteMap* pattern will include sight information, first click-point and the whole moved places. To summarize, our scheme is different from other similar schemes in the following aspects.

- *RouteMap* allows users to choose whether to use sight or not, which aims to improve users' memory by placing them in a preferred environment. This selection will be included in the final pattern stored in the system.
- *RouteMap* only allows users to draw straight lines between different places. This aims to improve the usability, as it is noted that drawing curves is not easy for authentication using mouse input (i.e., consuming more time).
- *RouteMap* provides a simple guideline for users, which recommends users to create a route based on their existing memory such as tours and visits. It is found that tour-route or visit-route is private for users, but may enhance the memory of various clicks in a pattern.

Implementation. We built a prototype system of *RouteMap* in our lab environment, which is similar to the design of *PassMap* and *GeoPass*. To fetch a real world map, we utilize Java scripts and Google Maps API, and our system can provide move (drag), zoom in, zoom out and search functions. When users zoom in or zoom out the map, *RouteMap* will report the zoom levels. For the search function, users can use it to shift to a specific area quickly and use zoom in or zoom out to locate a proper area. Afterwards, users can create a password by clicking a place and moving the mouse to click on the next places. Based on the prior work [14], we set the error tolerance to a 21 × 21 pixel box around the place they clicked. For the other similar schemes, the error tolerance of *GeoPass* was set to the same 21 × 21 pixel while *PassMap* was set to 20 × 20 pixel.

In this case, our system is able to record users' inputs and construct a pattern like {Sight, zoom level, the sequence of clicked places}. The value of *sight* is either 0 (not selected) or 1 (selected). The initial zoom level is set to 2 and the maximum level is 18. After clicking on a place, our system will record its coordinate information. It is worth noting that in order to enhance memory, a *red arrow* will be shown in *RouteMap* when users move mouse from one clicked place to another (see Figure 2).

4.2 User Study

To explore the performance of *RouteMap* in the aspect of multiple password memory, we further conduct a user study with 60 participants, among which 50 of them are from the former study. The time gap between the first study and this study is one month. The newly joined 10 participants are also volunteers and have no any background in information security. The detailed information of participants is described in Table 4.

Table 4. Detailed information of participants in the second user study.

Age Range	Male	Female	**Occupation**	Male	Female
18-25	10	11	Senior people	4	2
25-35	8	9	Students	17	15
35-45	5	4	Researchers	5	4
45-55	4	3	Engineers	3	3
55-60	4	2	Business people	4	3

In the study, we randomly divided 60 participants into two groups, named *Group1* and *Group2*, and compare *RouteMap* with *PassMap* and *GeoPass*, respectively. More specifically, *Group1* will focus on *RouteMap* and *PassMap*, while *Group2* will focus on *RouteMap* and *GeoPass*. The implementation details of *PassMap* and *GeoPass* can be referred to [20,22]. Similar to our study above, to avoid bias, we train all the participants based on the same steps on how to use these example systems.

Before the study, every participant has 3 trails to get familiar with the example systems. For example, participants in *Group1* will create passwords for *RouteMap* and *PassMap*. In the user study, we require all participants to create 5 passwords for each scheme in their group and each password corresponds to an account: the first password is created for an email account (personal use), the second one is created for a bank account, the third one is created for another email account (commercial use), the fourth one is created for a forum account and the last one is created for a social networking account. The detailed steps in each experiment are shown as below:

- *Experiment G1. Group1* conducts this experiment, in which each participant is required to firstly create 5 passwords for *PassMap* and then create 5 passwords for *RouteMap* after one hour rest.
- *Experiment G2. Group2* conducts this experiment, in which each participant is required to firstly create 5 passwords for *GeoPass* and then create 5 passwords for *RouteMap* after one hour rest.

  Both experiments follow the same steps, which are described as below:

  - Step 1. Creation: creating a password following the related rules.
  - Step 2. Confirmation: confirming the password by drawing the same secrets in the correct place. If users incorrectly confirm their password, they can retry the confirmation or return to Step 1.
  - Step 3. Login: logging in the example system with all created passwords. Users can cancel an attempted login if they noticed an error.
  - Step 4. Feedback: All participants are required to complete a *feedback form* about the password creation and confirmation.

All participants have to finish the experiments in the same day. To compare the results with the previous study, after three weeks, we later invite all participants to return and input all created passwords based on their own groups.

Table 5. Login success rate for *Group1* and *Group2* after three weeks.

Experiment G1 (PassMap)	Successful Login	*Experiment G1* (RouteMap)	Successful Login
1st time	113/150 (75.3%)	1st time	133/150 (88.7%)
2nd time	125/150 (83.3%)	2nd time	137/150 (91.3%)
3rd time	128/150 (85.3%)	3rd time	140/150 (93.3%)

Experiment G2 (GeoPass)	Successful Login	*Experiment G2* (RouteMap)	Successful Login
1st time	122/150 (81.3%)	1st time	134/150 (89.3%)
2nd time	128/150 (85.3%)	2nd time	136/150 (90.7%)
3rd time	133/150 (88.7%)	3rd time	141/150 (94.0%)

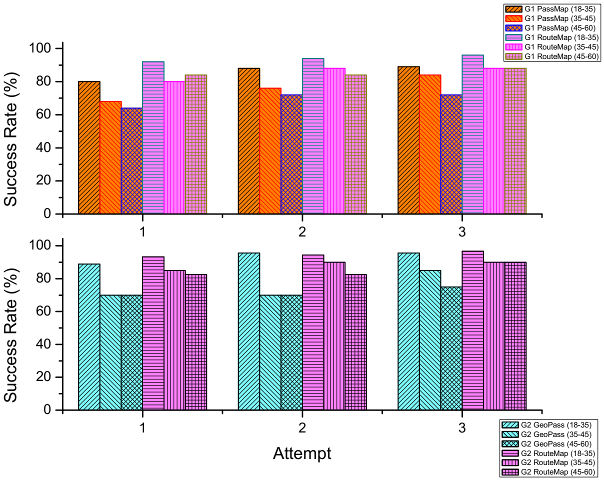


Fig. 3. Success rates for each age groups in the study.

After finishing this session, we give a *feedback form* to each participant regarding their password memory.

Results. In this study, our target is to investigate the multiple password memory of *RouteMap* by comparing it with similar schemes. The login success rates for *Group1* and *Group2* within three attempts are presented in Table 5. Our key observations are reported as below:

- *Overall Performance.* As compared with the results in Table 2, it is seen that participants perform much better in this study. *Group1* can achieve a success rate of 75.3% and 88.7% for *PassMap* and *RouteMap* at the first attempt, respectively. After three attempts, the success rate can be increased to 85.3% and 93.3%. On the other hand, *Group2* can achieve a success rate of 81.3% and 89.3% for *GeoPass* and *RouteMap* at the first attempt, respectively. Then, the success rate can be elevated to 88.7% and 94% after three attempts.
- *Age Impact.* It is easily imagine that the results for each age group would be improved, since the overall login success rate increases. Figure 3 indicates

Table 6. Several main questions and relevant scores in the user study.

Questions	Score (average)
1. I could easily remember *PassMap* passwords after one month	7.3
2. I could easily remember *GeoPass* passwords after one month	8.1
3. I could easily remember *RouteMap* passwords after one month	9.0
4. Are you willing to use *PassMap* passwords in practice	7.8
5. Are you willing to use *GeoPass* passwords in practice	8.5
6. Are you willing to use *RouteMap* passwords in practice	8.9
7. I can manage multiple *PassMap* passwords	7.1
8. I can manage multiple *GeoPass* passwords	7.8
9. I can manage multiple *RouteMap* passwords	8.7

that younger participants have advantages in memory while the success rate of senior people also increases a lot.

According to these observations, it is found that participants are able to better remember multiple passwords for these schemes, while our scheme can outperform the other two schemes with a higher success rate. The major reason is that *RouteMap* leads users to draw a route where they have experienced before. The experience actually enhances the relationship between different clicked places, so that users can have a better memory capability.

To validate the observations, the major questions and relevant scores (feedback) are presented in Table 6. Ten-point Likert scales were used in each feedback question where 1-score indicates strong disagreement and 10-score indicates strong agreement.

It is visible that most participants gave positive feedback for remembering these map-based passwords, in which *RouteMap* receives the highest score of 9.0 among them. Most participants report that the route defined in *RouteMap* can improve their memory of created passwords, due to the correlation between these clicked places. Based on this, participants are also willing to use the map-based passwords in practice such as their email accounts and social networking accounts, where *RouteMap* obtains the highest score of 8.9. Moreover, it is seen that most participants believe that they can manage multiple *RouteMap* passwords with the highest score of 8.7, as compared with the other two schemes (with a score of 7.1 and 7.8, respectively). On the whole, it is considered that *RouteMap* can provide better multiple password memory for users.

4.3 Further Discussions

This work mainly focuses on the two defined targets, so that we leave some aspects such as security analysis in our future studies. In this part, we briefly analyze *RouteMap* in the aspects of security and usability.

- *Security Aspect.* As mentioned above, *RouteMap* is a kind of map-based passwords and allows users to click several places on a map in constructing a route as passwords. Intuitively, the password space is generally not lower than *GeoPass* (one clicked place on a map), but due to the relationship between different clicked places, there is not a direct increase by clicking more places. We will provide a full security analysis in our future work.

- *Usability Aspect.* Based on our studies and participant feedback, *RouteMap* obtains higher scores than the other two schemes, so we consider it has good usability. We also informally interviewed most participants and most participants prefer *RouteMap* instead of the other schemes. It is worth noting that the other two map-based schemes also obtain good feedback, when comparing the scores between Table 3 and Table 6.
- *Multiple Password Memory.* Our study results indicate that users have better performance in multiple password memory using *RouteMap*. It is noted that users memory can be enhanced by correlating the clicked places. To explore this issue, an even larger study will be performed in our future work.

5 Conclusion

In this paper, our first purpose is to explore whether users can remember multiple graphical passwords for two existing and popular GP schemes. Based on the study results, it is identified that multiple password memory has become a big challenge. To solve this issue, we design *RouteMap*, a map- and route-based graphical password scheme, in which users can draw a route on a Google map as their secrets. To investigate its performance, we further conduct another user study with 60 participants and find that *RouteMap* can enhance multiple password memory for users, as compared with two similar schemes. Our effort aims to complement existing studies and stimulate more research in this area.

There are lots of future directions including providing a more specific analysis on password space and involving more participants in the future evaluation. Future work could also include conducting a thorough security analysis and evaluate the scheme in an adverse environment (i.e., an attacker has some knowledge about the user and build a map password dictionary).

Acknowledgments. We first would like to thank Wenjuan Li, Lijun Jiang and Ying Meng for the great support in this work and all participants for their hard work and cooperation in the user study. In addition, we would like to thank all anonymous reviewers for their helpful comments in improving the paper.

References

1. 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)
2. Chiasson, S., van Oorschot, P.C., Biddle, R.: Graphical password authentication using cued click points. In: Biskup, J., López, J. (eds.) ESORICS 2007. LNCS, vol. 4734, pp. 359–374. Springer, Heidelberg (2007)

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., Stobert, E., Forget, A., Biddle, R.: Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism. IEEE Transactions on Dependable and Secure Computing **9**(2), 222–235 (2012)
5. 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 (2004)
6. 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). ACM, New York, pp. 20–28 (2007)
7. 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)
8. Fox, S.: Future Online Password Could be a Map (2010). http://www.livescience.com/8622-future-online-password-map.html
9. 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)
10. Gołofit, K.: Click passwords under investigation. In: Biskup, J., López, J. (eds.) ESORICS 2007. LNCS, vol. 4734, pp. 343–358. Springer, Heidelberg (2007)
11. 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)
12. 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 (2007)
13. 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)
14. 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)
15. Nelson, D.L., Reed, V.S., Walling, J.R.: Pictorial superiority effect. Journal of Experimental Psychology: Human Learning and Memory **2**(5), 523–528 (1976)
16. Passfaces. http://www.realuser.com/
17. Shepard, R.N.: Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior **6**(1), 156–163 (1967)
18. Spitzer, J., Singh, C., Schweitzer, D.: A Security Class Project in Graphical Passwords. Journal of Computing Sciences in Colleges **26**(2), 7–13 (2010)
19. 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)
20. Sun, H., Chen, Y., Fang, C., Chang, S.: PassMap: a map based graphical-password authentication system. In: Proceedings of ASIACCS, pp. 99–100 (2012)
21. Tao, H., Adams, C.: Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. International Journal of Network Security **2**(7), 273–292 (2008)

22. Thorpe, J., MacRae, B., Salehi-Abari, A.: Usability and security evaluation of geopass: a geographic location-password scheme. In: Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS), pp. 1–14 (2013)
23. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N.: Passpoints: Design and Longitudinal Evaluation of A Graphical Password System. International Journal of Human-Computer Studies **63**(1–2), 102–127 (2005)
24. Weir, M., Aggarwal, S., Collins, M., Stern, H.: Testing metrics for password creation policies by attacking large sets of revealed passwords. In: Proceedings of CCS, pp. 162–175 (2010)
25. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password memorability and security: Empirical results. IEEE Security and Privacy **2**, pp. 25-31 (2004)