CPMap: Design of Click-Points Map-Based Graphical Password Authentication

Weizhi Meng, Fei Fei, Lijun Jiang, Zhe Liu, Chunhua Su, Jinguang Han

HAL Id: hal-02023732
https://inria.hal.science/hal-02023732

Submitted on 21 Feb 2019

CPMap: Design of Click-Points Map-based Graphical Password Authentication

Weizhi Meng[1], Fei Fei[2], Lijun Jiang[2], Zhe Liu[3], Chunhua Su[4], and Jinguang Han[5]

[1] Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark
[2] Department of Computer Science, City University of Hong Kong, Hong Kong SAR
[3] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg
[4] Division of Computer Science, University of Aizu, Japan
[5] Department of Computer Science, University of Surrey, UK
`weme@dtu.dk`

Abstract. As traditional textual passwords suffer from many known limitations, graphical passwords (GPs) are proposed as one promising alternative to complement the existing authentication systems. To obtain a large password space, map-based GPs (geographical passwords) have been developed that allow users to choose one or more places on a map for authentication. For example, PassMap requires users to choose two places as their credentials, and GeoPass enables users to click only one place for authentication. Some research studies have reported that choosing only one place as a password may be not secure enough, whereas selecting two places may decrease the system usability. In this work, we first conducted a study to learn how users would choose two places under PassMap, and found that users may choose two similar locations due to time consideration. Motivated by this observation, we then design CPMap, a click-points map-based GP scheme that allows users to choose one place on a world map at first and then click a point or an object on an image relating to the previously selected location. To investigate the performance of CPMap, we conducted another user study with up to 50 participants. It is found that users could achieve promising results with our scheme in the aspects of both security and usability.

Keywords: User Authentication, Graphical Passwords, Map-based Passwords, Geographic Authentication, Security and Usability.

1 Introduction

Nowadays, traditional textual passwords are still the most widely deployed user authentication method across many organizations, but they have well-known limitations in the aspects of both security and usability [35]. For instance, users are difficult to remember a complicated password for a long period of time; thus, users may select weak passwords for better recall. Generally, a weak password

can be easily guessed by attackers, which would greatly degrade the security of authentication. In practice, this situation would be even worse than we previously believed (i.e., most created passwords only provided fewer than 10 bits of security against an online trawling attack) [1, 34].

In some early studies, people were found to generally remember and recognize images better than textual passwords [24, 26]. Based on this observation, graphical passwords (GPs) are developed as a promising alternative to complement textual password-based authentication, which typically require users to create their credentials on images, i.e., DAS, PassPoints and CCP are some well-known schemes. In particular, DAS was proposed by Jermyn *et al.* [11], which allows users to draw their passwords on a 2D grid. Wiedenbeck *et al.* [33] developed *PassPoints* that demands users to generate passwords by clicking on any place on an image. Chiasson *et al.* [2] proposed Cued Click Points (CCP), in which the next image displayed can be varied with the previous click-point and users have to select five points in a sequence of images.

In order to obtain a large password space, map-based GP schemes are developed that can provide more potential places for users by adopting a world image. PassMap [30] and GeoPass [32] are two typical examples: PassMap asks users to choose two places in a sequence at any zoom-level on a world map, while GeoPass only needs users to select one location on a world map at zoom level of 16. Intuitively, the selection of one location is more vulnerable to shoulder surfing attacks, while increasing the number of locations may cause more additional burden on users (i.e., selecting two places). Previous study [23] investigated this issue and found that increasing the number of locations from one to two would not much degrade the performance of users' memorability, but would indeed consume more authentication time.

Contributions. In this work, we first conduct a user study to investigate the password patterns of PassMap, i.e., measuring the distance between the selected locations. Then, we design a new type of map-based passwords by combining existing geographical authentication with click points. We further conduct another user study to explore its performance as compared to PassMap and GeoPass. The contributions of this work can be summarized as follows.

- In the first study, we investigate how users would select the two locations on a world map under PassMap. The selection of *PassMap* is due to its scheme design and popularity. It is identified that common users are likely to create two locations that are very close to each other for the sake of time consumption during authentication (i.e., two locations are within the same community, which may greatly reduce the effective password space).
- To enhance the existing map-based GPs, we develop a click-points map-based password scheme, named *CPMap*. Users have to firstly select one location on a world map and then click one point or an object on an image that is relevant to the previously selected location. This scheme can be regarded as a combination of geographical passwords and *CCP*.
- To explore the performance of *CPMap*, we conducted another user study with 50 participants and compared our scheme with PassMap and GeoPass. Ex-

perimental results indicate that our scheme can achieve better performance in terms of both security and usability.

Road map. The remaining parts of this paper are organized as follows. In Section 2, we introduce related studies regarding existing GP schemes, especially map-based authentication schemes. Section 3 describes our first user study on *PassMap* with 30 participants. In Section 4, we detail our proposed *CPMap* and analyze the results obtained from another user study with 50 participants. Finally, we conclude our work with future directions in Section 5.

2 Related Work

This section introduces the classification of graphical passwords and related research on map-based authentication schemes.

GP Classification. Generally, a GP scheme can be categorized into three types [3, 23, 29]: namely, recognition-based (i.e., remembering and recognizing images), pure recall-based (i.e., recreating a pattern without a hint) and cued recall-based scheme (i.e., recreating a pattern with hints).

- *Recognition-based scheme.* This kind of schemes asks users to select one or more images from an image pool. *PassFaces* [25] is one particular recognition-based scheme, which needs users to identify several human faces for authentication. Another scheme, called *Story* [5], requires users to pick out some assigned images from an image pool such as people, food, fruit, etc.
- *Pure recall-based scheme.* This type of schemes requires users to create a pattern on an image as their secret. For example, Jermyn *et al.* [11] proposed a scheme of *DAS* ('draw-a-secret') that allows users to create their secrets on a grid. Tao *et al.* [31] introduced *Pass-Go* that asks users to create a password by selecting intersections on a grid. Based on the idea of *Pass-Go*, Android unlock patterns have been widely adopted on Android phones, allowing users to unlock the phone if they can input a correct pattern.[6] Several other relevant schemes can be referred to [7, 12].
- *Cued recall-based scheme.* This kind of schemes needs users to select a sequence of points on an image or multiple images to construct their passwords. A typical system of *PassPoints* was proposed by Wiedenbeck *et al.* [33], which requires users to remember a sequence of five points on different images. To improve the memorability of *PassPoints*, Chiasson *et al.* [4] then proposed Persuasive Cued Click-Points (PCCP), which requires users to select a point on each of a sequence of background images.

To further enlarge the password space, a set of hybrid GP schemes were also developed in the literature, like click-draw based GP scheme [14] that combined the main input types of current GPs including clicking, selecting and drawing. Some other relevant studies on GP improvement can be referred but not limited to [6, 10, 15–17, 19–21, 36].

---

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

Map-based Graphical Password Schemes. To the best of our knowledge, Fox in 2010 [8] first presented the idea of using a digital map to create a password. After that, Spitzer *et al.* [27] developed a scheme called Cued Click Points (*CCP*), which could combine the graphical approach with user's familiarity with navigating through Google maps. For implementation, users were presented with an image of the United States and simply click to where the key destination is located. Their results with around 50 participants indicated that around 60% users rated the system as easier to remember than traditional textual passwords in terms of memorability.

Map-based GP schemes become more popular from the year of 2012. Georgakakis *et al.* [9] proposed a scheme called *NAVI*, which allows users to draw a route on a pre-loaded map image. They initially analyzed the strength of the password, but did not give any user study for the real performance. Then, Sun *et al.* [30] proposed a map-based authentication system called *PassMap*, which allows users to select two sequenced places on a world map. In the evaluation, users found that *PassMap* passwords are easier to remember than textual strings. Similarly, Thorpe *et al.* [32] proposed *GeoPass*, a digital map-based GP scheme, which allows users to choose only one place on a world map as the credentials. Then, MacRae *et al.* [13] proposed GeoPassNotes, asking users to further select a note associated with their chosen location in the second step. Shin et al. [28] further implemented a modified version of *GeoPass* on a mobile device. The major difference between *PassMap* and *GeoPass* is the number of locations allowed by the system, i.e., clicking one or two places on a world map. Focused on this issue, Meng *et al.* [23] conducted a study with 60 participants and found that participants could perform very closely for both schemes. In other words, there is no significant difference between the selection of one or two locations.

To enhance the performance of multiple password memory, Meng [18] proposed *RouteMap*, a map- and route-based graphical password scheme, allowing users to draw a route on a world map as their secrets. In the user study with 60 participants, it is found that *RouteMap* can outperform similar schemes. Then, Meng *et al.* [22] conducted a study with 60 participants to investigate the recall of multiple passwords between text passwords and map-based passwords under various account scenarios. In particular, 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.

3   A Study on PassMap

In this section, we conduct a user study with 30 participants to investigate the password patterns of *PassMap*. The selection is due to its scheme design and popularity. As introduced earlier, this scheme requires users to select two places on a world map at any zoom level. For authentication, users have to select the same location in the correct sequence and zoom level.
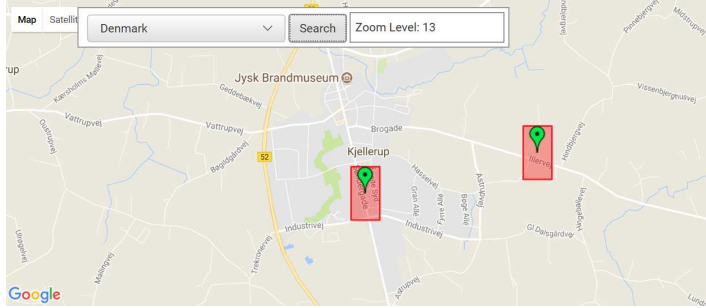
Fig. 1. The implementation of PassMap: (a) registration page with user name, and (b) an example of selected locations.

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

Age Range	Male	Female	Occupation	Male	Female
17-35	9	8	Students	10	8
36-45	5	4	Researchers	4	4
Above 45	2	2	Business people	2	2

PassMap Implementation. In this work, we adopted an open-source GP platform from the previous study [23]. It enables an extensive move-by-dragging, zooming and search functions by leveraging the JavaScript from Google Maps API. The search function allows users to shift to a specific part of the map quickly and further locate a specific area. As shown in Fig. 1 (a) and Fig. 1 (b), users can input their usernames, and zoom in or zoom out on the map to find a place with zoom levels. According to PassMap [30], our system embedded a 640×420 pixel frame block for displaying the world map in a web page and road/map view was implemented by default with a tolerance of 21×21 pixels.

User Study. To investigate the password patterns of PassMap, we performed a study with 30 participants, who are volunteers and have not attended any courses in relation to security. The information of participants is shown in Table 1.

Before the study, we introduced our objectives to all participants and provided a guideline including all steps in the lab study. Each participant has 3 trails to get familiar with PassMap system. In particular, every participant was
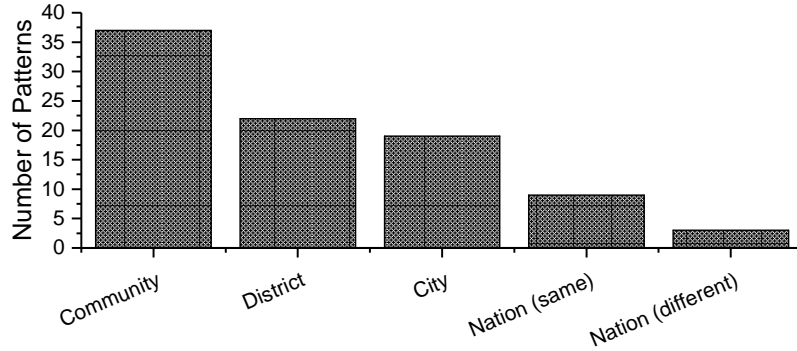
Fig. 2. The distribution of in-between distance for PassMap passwords in the study.

required to create three passwords in the same day. The detailed steps can be summarized as below:

- Step 1. Creation: creating a password according to the rules of PassMap.
- Step 2. Confirmation: confirming the password by choosing the same locations in the correct place. If users incorrectly confirm their password, they can either retry this step or return to the last step.
- Step 3. Login: entering the system with the created passwords. Users can cancel an attempt if they notice an error.
- Step 4. Feedback: all participants are required to complete a *feedback form* about the password creation and confirmation.

Result analysis. In the study, our major purpose is to investigate the password patterns created by participants, especially the distance between two selected locations. This is because two similar points may greatly reduce the effectiveness of PassMap (i.e., resulting in a weak password). To facilitate the illustration, we classify the patterns into different categories based on the in-between distance: community, district, city, nation (same continent), nation (different continents). In total, we collected 90 PassMap passwords in the study. The distribution of in-between distance is depicted in Fig 2.

It is known that GeoPass is vulnerable to offline guessing attacks due to the selection of only one location. Intuitively, selecting two locations would double the password space of PassMap as compared to GeoPass. However, it is found that up to 37 and 22 PassMap passwords (65.6%) dropped into the first two categories. The close locations could cause PassMap to offer weak security against online guessing attacks, if the attacker had some effectively prioritizing guesses. In other words, choosing two close points would greatly lower the effective password space and increase the cracking probability.

To find the reason, we informally interview the participants and identified that most of them would choose two close locations to reduce the time consumption. Table 2 computes the success rate and average completion time, which indicates that participants required around 36 seconds, 22 seconds, and 27 seconds

Table 2. Success rate and average completion time for the step of creation, confirmation and login in the study.

PassMap	Creation	Confirmation	Login
Success Rate (the first time)	68/90 (75.6%)	76/90 (84.4%)	79/90 (87.8%)
Completion Time (Average in seconds)	35.6	21.3	26.6
Standard Deviation (SD in seconds)	9.5	8.6	10.3

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

Questions	Score (average)
1. I could easily create a *PassMap* password	8.2
2. I could easily log in *PassMap* system	7.2
3. The time consumption by *PassMap* is acceptable	4.9
4. Are you willing to use *PassMap* passwords in practice	5.3

for password creation, confirmation and login, respectively. In the interview, most participants reflected that it is very time-consuming to complete a successful authentication under PassMap; thus, they decided to select two close locations to reduce the time in zooming the map.

Feedback and Discussion. According to the results obtained in the study, it is found that most participants did not create a strong PassMap password. Table 3 further analyzed the feedback forms collected in the study. 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 still gave positive feedback on password creation (with a score of 8.2), but they believed the login phase should be improved, especially the time consumption was unacceptable. By considering the usability, most of them believed that current PassMap was not mature enough for real-world usage.

As users have to find two locations on a world map, PassMap can be considered as a two-step scheme. For such kind of schemes, there is a need to enhance the password design, especially to reduce the time consumption for better authentication in practical applications.

4   CPMap and Evaluation

To design an appropriate two-step geographical password scheme, a balance should be made between location number and time consumption. For instance, *PassMap* requires users to choose two locations on a world map, which may consume a lot of time during authentication. Focused on this issue, we design *CPMap*, a click-points map-based GP by combining the geographical passwords with click-point schemes. We then conduct a user study to investigate its performance as compared with *PassMap* and *GeoPass*.

Fig. 3. (a) The steps on how to create a CPMap password, and (b) an example: selection of one location on a world map in the first step and selection of one point on an image in the second step.

4.1   Design of CPMap

To improve the performance of *GeoPass*, MacRae *et al.* [13] proposed GeoPassNotes, which requires users to choose a note to be associated with their chosen location in the second step. They actually combined the location password with a note, where users are authenticated by correctly entering both a location and an annotation. However, we notice that writing a note may increase the time consumption and be less convenient on some mobile devices with a small touch-screen. In this work, we design *CPMap*, which is a combination of map-based password and click-points. More specifically, it needs users to select one location on a world map at first, and then click one point or an object on an image that is extracted from the surroundings related to the selected location.

Our scheme. Fig. 3 (a) details the steps on how to construct a *CPMap* password, and Fig. 3 (b) shows a concrete example of password creation. Firstly, similar to most map-based schemes, users have to select one location on a world map, e.g., the central station in Copenhagen. Then, *CPMap* shows up an image that is related to the selected location, e.g., a construction work environment in the central station. Similar to click-based GPs, users have to click one point (or an object) to create their password, i.e., selecting a tower (upper right corner). For authentication, users have to locate the right place on the world map and select the correct object. In short, *CPMap* is believed to have several advantages over *PassMap* and *GeoPass*.

- *CPMap* allows users to select only one location on a world map, which aims to reduce the time for zooming out / zooming in on the map to find another

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

Age Range	Male	Female	Occupation	Male	Female
18-30	13	11	Business people	4	3
31-40	7	6	Students	15	12
41-50	4	4	Researchers	5	6
Above 50	3	2	Senior people	3	2

location, as compared to *PassMap*. In our first study, *PassMap* was found to cost too much time for password creation and login.
- The password space of *PassMap* is expected to reach around $2^{36.9 \times 2}$ with two map locations, whereas users are likely to create a weak password, resulting in a similar password space to *GeoPass* ($2^{36.9}$). By contrast, *CPMap* is also a two-step scheme: it requires users to decide a location at first while selecting an object on an image in the second step. As a result, *CPMap* can offer a larger password space than *GeoPass*.
- Based on the previous studies on map-based password schemes [13, 23, 32], users were often advised to choose a familiar location where they have travelled or visited before. As *CPMap* provides an image that is related to the selected location, it can facilitate users to remember the created location.

CPMap Implementation. A prototype system of *CPMap* was implemented in our lab environment. Similar to *PassMap*, we use Java scripts and Google Maps API to fetch a real world map, in which users can perform a set of actions such as move (drag), zoom in, zoom out and search. Based on the Google Maps API, a particular surrounding image could be extracted, which can vary with the selected locations. We set the error tolerance to a 21×21 pixel box around the place. As a comparison, it is worth noting that *GeoPass* and *PassMap* has an error tolerance of 21×21 pixel and 20×20 pixel, respectively. Users can create their passwords according to the steps as shown in Fig. 3 (a). In addition, our system requires users to choose a location at zoom level of 16 due to the usability (similar to *GeoPass*).

4.2   User Study

To explore the performance of *CPMap*, we conducted another user study with a total of 50 participants, who did not attend the first study (in order to avoid any bias). Similarly, all participants are volunteers and have no any background in security. We gave an introduction about the tasks to each participant and asked them to sign a consent form before they started their work. The participants' background is detailed in Table 4.

In order to compare our scheme of *CPMap* with *PassMap* and *GeoPass*, we randomly divided the participants into two groups with 25 individuates each, named *Group-A* and *Group-B*. In particular, *Group-A* targets on a comparison between *CPMap* and *PassMap*, while *Group-B* focuses on *CPMap* and *GeoPass*. More implementation details of *PassMap* and *GeoPass* can refer to the former

studies [30, 32]. To avoid any bias, we offered a guideline and trained all partic-
ipants based on the same steps, ensuring that they understood the study steps
and how to use these example systems.

Similar to our first study, each participant has 3 trials to get familiar with
the assigned example systems. In the user study, every participant was asked to
create 5 passwords for each scheme in their group. All participants should finish
the experiments in the same day. In this case, a total of 250 trials were collected
from each group during the whole study. The detailed steps in each experiment
are summarized as follows:

- *Group-A*. Participants in this group were required to create 5 passwords for
  each *PassMap* and *CPMap*, with a half hour rest in-between. The start from
  which scheme was selected by random.
- *Group-B*. Participants in this group needed to create 5 passwords for *GeoPass*,
  and 5 passwords for *CPMap* after a half hour rest. The start from which
  scheme was selected by random.

  Participants from both groups should follow the same steps shown as below:
  - Step 1. Creation: creating a password following the related rules.
  - Step 2. Confirmation: confirming the password by inputting the same
    secrets in the correct place. If users incorrectly confirm their password,
    they can either retry this step or return to Step 1.
  - Step 3. Distributed memory: participants were provided with two finding
    tasks (paper-based) in order to distract them for 15 minutes.
  - Step 4. Login: logging into the example system with all created pass-
    words. Users can cancel an attempt if they found an error.
  - Step 5. Feedback: participants are required to complete a *feedback form*
    about the scheme usage.

Result analysis. Table 5 summarizes the success rate and average comple-
tion time regarding creation, confirmation and login for two groups. The main
observations are discussed as below.

- In *Group-A*, it is found that participants in *CPMap* could perform better
  than those in *PassMap* in the aspects of both login success and time con-
  sumption. For example, participants achieved a success rate of 78.4%, 80.8%
  and 82.4% for creation, confirmation and login in *PassMap*, but could in-
  crease the success rate to 86.4%, 88.0% and 89.6% in *CPMap*, respectively.
  Regarding time consumption, participants spent much less time in *CPMap*
  than those in *PassMap*, i.e., they spent 24.1 seconds for *PassMap* login, but
  only needed 11.6 seconds for *CPMap* login.
- In *Group-B*, it is found that participants in *CPMap* could achieve a slightly
  better performance than those in *GeoPass*. For instance, participants reached
  a success rate of 84.0%, 87.2%, 89.6%, and 84.8%, 88.8%, 92.0% for *GeoPass*
  and *CPMap*, respectively. Regarding time consumption, these two schemes
  could achieve a similar result as well, i.e., they spent 14.4 seconds and 13.9
  seconds for *GeoPass* and *CPMap* login.

Table 5. Success rate and average completion time for the step of creation, confirmation and login for two groups in the second study .

PassMap (Group-A)	Creation	Confirmation	Login
Success Rate (the first time)	98/125 (78.4%)	101/125 (80.8%)	103/125 (82.4%)
Completion Time (Average in seconds)	31.2	23.5	24.1
Standard Deviation (SD in seconds)	10.3	9.3	9.7
CPMap (Group-A)	Creation	Confirmation	Login
Success Rate (the first time)	108/125 (86.4%)	110/125 (88.0%)	112/125 (89.6%)
Completion Time (Average in seconds)	21.3	13.3	11.6
Standard Deviation (SD in seconds)	8.8	8.2	7.4
GeoMap (Group-B)	Creation	Confirmation	Login
Success Rate (the first time)	105/125 (84.0%)	109/125 (87.2%)	112/125 (89.6%)
Completion Time (Average in seconds)	20.6	16.2	14.4
Standard Deviation (SD in seconds)	9.8	9.5	8.3
CPMap (Group-B)	Creation	Confirmation	Login
Success Rate (the first time)	106/125 (84.8%)	111/125 (88.8%)	115/125 (92.0%)
Completion Time (Average in seconds)	20.1	14.2	13.9
Standard Deviation (SD in seconds)	8.5	8.3	6.6

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

Questions	Score (average)
1. I could easily create PassMap passwords	7.5
2. I could easily create GeoPass passwords	8.7
3. I could easily create CPMap passwords	8.8
4. I could easily log into PassMap system	6.9
5. I could easily log into GeoPass system	8.0
6. I could easily log into CPMap system	8.1
7. I think PassMap passwords are more secure	8.7
8. I think GeoPass passwords are more secure	7.3
9. I think CPMap passwords are more secure	8.7

User feedback. Regarding users' attitude, Table 6 summarizes the major questions and relevant scores (feedback) collected during this study. The first three questions attempt to investigate the creation experience regarding the different schemes, it is found that *CPMap* and *GeoPass* got a higher score than *PassMap*, i.e., 7.5 for *PassMap* but 8.8 for *CPMap*. The following three questions indicated that participants believed *CPMap* and *GeoPass* could provide better login experience (usability). For the last three questions, most participants believed *PassMap* and *CPMap* were more secure than *GeoPass*. In our informal interview, participants believed that two-step authentication could enhance the scheme security and increase the cracking difficulty for cyber-attackers, hence they considered *CPMap* to be more secure than *GeoPass*. Overall, most participants supported *CPMap* in terms of both security and usability.

4.3   Discussion and Limitations

- *Security aspect.* As mentioned earlier, *CPMap* is a two-step password scheme, which requires users to firstly choose a location on a world map and further click an object on an image. This aims to provide a better password space over *GeoPass* (with one clicked place on a map). In theory, *PassMap* should provide an even larger password space, but its security level would not be that high due to the weak password creation (refer to our first user study). To provide a formal security analysis is one of our future work.
- *Usability aspect.* Our study found that participants required much less time consumption in *CPMap* than that in *PassMap*. Actually, the time required by our scheme is quite close and even less than *GeoPass* (refer to Table 5). By analyzing the feedback collected from the participants, most participants considered both *CPMap* and *GeoPass* to be more usable than *PassMap*. As there are many GPs available in literature, one of our future work is to compare our scheme with other similar schemes like *GeoPassNotes*.

5   Conclusion

Map-based password authentication generally requires users to create their passwords by means of a (world) map. In this work, we firstly investigated how users would select two locations on a world map under the scheme of *PassMap*. It is found that common users may pick up two places that are very close to each other due to time considerations, which may greatly lower the security level. Motivated by the observation, we design *CPMap*, a click-points map-based GP scheme that allows users to choose one place on a world map at first and then click an object on an associated image relating to the selected location. We then conducted another user study with 50 participants to explore the scheme performance. Participants were found to perform better under our scheme as compared to *PassMap* and *GeoPass* in the aspects of both security and usability. Future work could include providing a thorough security analysis of password space and comparing our scheme with other similar schemes.

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., Lopez, 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), pp. 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), New York, NY, USA: ACM, 2007, pp. 20-28 (2007)
7. P. Dunphy, J. Yan, 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. S. Fox. 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. Golofit, K.: Click passwords under investigation. In: Proceedings of the 12th European Symposium on Research in Computer Security (ESORICS). Berlin, Heidelberg: Springer-Verlag, pp. 343-358 (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. D. Lin, P. Dunphy, P. Olivier, J. Yan. Graphical passwords & qualitative spatial relations. In: Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), pp. 161-162 (2007)
13. MacRae, B., Salehi-Abari, A., Thorpe, J.: An Exploration of Geographic Authentication Schemes. IEEE Transactions on Information Forensics and Security 11(9), pp. 1997-2012 (2016)
14. 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)
15. Meng, Y., Li, W.: Evaluating the Effect of Tolerance on Click-Draw Based Graphical Password Scheme. In: Proceedings of the 14th International Conference on Information and Communications Security (ICICS), Lecture Notes in Computer Science 7618, Springer, pp. 349-356 (2012)
16. Meng, Y., Li, W.: Evaluating the effect of user guidelines on creating click-draw based graphical passwords. In: Proceedings of the 2012 ACM Research in Applied Computation Symposium (RACS), pp. 322-327 (2012)
17. Meng, Y., Li, W., Kwok, L.-F.: Enhancing Click-Draw based Graphical Passwords Using Multi-Touch on Mobile Phones. In: Proceedings of the 28th IFIP TC 11 International Information Security and Privacy Conference (IFIP SEC), IFIP Advances in Information and Communication Technology 405, pp. 55-68 (2013)
18. Meng, W.: RouteMap: A Route and Map Based Graphical Password Scheme for Better Multiple Password Memory. In: Proceedings of the 9th International Conference on Network and System Security (NSS), pp. 147-161 (2015)

19. Meng, W.: Evaluating the Effect of Multi-Touch Behaviours on Android Unlock Patterns. Information and Computer Security, vol. 24, no. 3, pp. 277-287, Emerald (2016)
20. Meng, W., Li, W., Wong, D.S., Zhou, J.: TMGuard: A Touch Movement-based Security Mechanism for Screen Unlock Patterns on Smartphones. In: Proceedings of the 14th International Conference on Applied Cryptography and Network Security (ACNS), pp. 629-647 (2016)
21. Meng, W., Li, W., Kwok, L.-F., Choo, K.-K.R.: Towards Enhancing Click-Draw Based Graphical Passwords Using Multi-Touch Behaviours on Smartphones. Computers & Security, vol. 65, pp. 213-229 (2017)
22. Meng, W., Li, W., Lee, W., Jiang, L., Zhou, J.: A Pilot Study of Multiple Password Interference between Text and Map-based Passwords. In: Proceedings of the 15th International Conference on Applied Cryptography and Network Security (ACNS), pp. 145-162 (2017)
23. Meng, W., Lee, W., Au, M.H., Liu, Z.: Exploring Effect of Location Number on Map-Based Graphical Password Authentication. In: Proceedings of the 22nd Australasian Conference on Information Security and Privacy (ACISP), pp. 301-313 (2017)
24. Nelson, D.L., Reed, V.S., Walling, J.R.: Pictorial superiority effect. Journal of Experimental Psychology: Human Learning and Memory, vol. 2, no. 5, pp. 523-528 (1976)
25. Passfaces, `http://www.realuser.com/`.
26. Shepard, R.N.: Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior, vol. 6, no. 1, pp. 156-163 (1967)
27. Spitzer, J., Singh, C., Schweitzer, D.: A Security Class Project in Graphical Passwords. Journal of Computing Sciences in Colleges 26(2), pp. 7-13 (2010)
28. Shin, J., Kancharlapalli, S., Farcasin, M., Chan-Tin, E.: SmartPass: a smarter geolocation-based authentication scheme. Security and Communication Networks 8, pp. 3927-3938 (2015)
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. IEEE Computer Society, USA (2005)
30. Sun, H., Chen, Y., Fang, C., Chang, S.: PassMap: A Map Based Graphical-Password Authentication System. In: Proceedings of AsiaCCS, pp. 99-100, 2012.
31. Tao, H., Adams, C.: Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. International Journal of Network Security 2(7), pp. 273-292 (2008)
32. 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)
33. 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)
34. 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)
35. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password memorability and security: Empirical results. IEEE Security and Privacy, vol. 2, pp. 25-31 (2004)
36. Yu, X., Wang, Z., Li, Y., Li, L., Zhu, W.T., Song, L.: EvoPass: Evolvable graphical password against shoulder-surfing attacks. Computers & Security 70, pp. 179-198 (2017)