Exploring Effect of Location Number on Map-Based Graphical Password Authentication

Weizhi Meng[1⋆], Wang Hao Lee[2], Man Ho Au[3], and Zhe Liu[4]

[1] Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark
[2] Infocomm Security Department, Institute for Infocomm Research, Singapore
[3] Department of Computing, The Hong Kong Polytechnic University, Hong Kong
[4] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg
{weme@dtu.dk;whlee@i2r.a-star.edu.sg}

Abstract. Graphical passwords (GPs) that authenticate users using images are considered as one potential alternative to overcome the issues of traditional textual passwords. Based on the idea of utilizing an extremely large image, map-based GPs like PassMap and GeoPass have been developed, where users can select their secrets (geographical point) on a world map. In particular, PassMap allows users to select two locations on a map, while GeoPass reduces the location number to only one. At first glance, selecting one location is more vulnerable to attacks, while increasing the location number may add burden on users. In the literature, there is no research exploring this issue. Motivated by this, our purpose in this work is to explore the effect of location number between PassMap and GeoPass in terms of users' performance and feedback. In this work, we develop a generic and open platform for realizing map-based schemes, and conduct a user study with 60 participants, which reveals that selecting two locations would not degrade the scheme performance. Our effort aims to complement exiting research studies in this area.

Keywords: User Authentication, Graphical Passwords, Map Password Authentication, Geographical Location, Security and Usability.

1 Introduction

Over the past few decades, textual passwords should be the most widely adopted method for user authentication, in which users have to recall and input the correct textual strings for authentication [26]. However, it has long been recognized that traditional textual passwords have many serious issues associated with their security and usability [26, 27]. For example, users are not good at remembering their passwords for a long

⋆ The author is previously known as Yuxin Meng.

time, especially complex and random passwords. As a result, they are very likely to choose simple strings or recycle passwords. The recent study showed that this situation might be even worse than previously believed (i.e., little variation in guessing difficulty) [1].

To improve memorability and security, graphical passwords (GPs) have been developed as a potential alternative to textual passwords. It is known that people generally have better memory and recognition for images than textual strings [16, 18]. Based on this observation, various graphical password schemes have been proposed. For example, Wiedenbeck *et al.* [25] designed PassPoints, a system that allows users to click several places on an image as their passwords. Chiasson *et al.* [2] then proposed a click-based GP scheme, named Cued Click Points (CCP), which allows users to click on one point for a sequence of images, and the next image displayed is based on the previous click-point.

To enhance password space, map-based graphical password authentication has recently attracted more attention like PassMap [22] and GeoPass [24], based on the idea of using an extremely large image. More specifically, PassMap allows users to select two sequenced locations on a large world map, while GeoPass reduces the location number to only one (but users can only choose a location at zoom level 16). A map image is believed to provide much more memorable points for users.

Motivations. We advocate that map-based GPs can be deployed as an extra authentication method, which can improve users' memorability while need more login time. Intuitively, selecting one location is more vulnerable to shoulder surfing attacks, but increasing the location numbers may add unexpected burden on users. With the development of graphical passwords, more map-based schemes have been proposed. However, there is no study to explore the effect of location number on scheme performance. In this work, our purpose is to explore this issue in terms of users' performance and feedback.

Our work aims to complement existing research results in this area and benefit the future design for map-based GPs. As PassMap and GeoPass are two typical schemes in the literature, we thus select them in our user study. The contributions can be summarized as follows.

- We develop an open and generic platform for implementing map-based GP schemes, which can realize both PassMap (i.e., selecting two locations) and GeoPass (i.e., selecting one location). This platform provides a unified environment for usability comparison. According to the observations from both schemes, a click-point is set to be valid at zoom level 16. More details can be referred to Section 3.

– We conduct a user study with 60 participants to compare the scheme performance between PassMap and GeoPass, in terms of users' performance and feedback. It is found that users could perform similarly for these two schemes. Our results reveal that increasing the location number from one to two would not degrade the performance of users' memorability.

The remaining parts of this paper are organized as follows. In Section 2, we briefly review related studies about graphical passwords and map-based GPs. Section 3 describes our platform implementation and presents study results. We make a further discussion in Section 4 and conclude our work in Section 5.

2 Related Work

2.1 GP Classification

Typically, graphical password systems can be classified into three categories [3, 21]: 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. Such schemes demand users to select one or more images from an image pool for authentication. For example, *Pass-Faces* [17] requires users to recognize a set of human faces for authentication. *Story* [5] requires users to recognize a set of sequenced images (e.g., people, food) from a large image pool.

Pure recall-based GPs. These GP schemes usually ask users to draw something on an image as their passwords. *DAS* [11] is one typical pure recall scheme, which requires users to draw on a grid. In addition, *Pass-Go* [23] allows users to select intersections on a grid as a way to input a password. Based on this idea, unlock patterns have been developed as a tuned version of *Pass-Go* on Android phones, which requires users to unlock their phones by inputting correct patterns.[5] Several similar schemes can be referred to [7, 12].

Cued recall-based GPs. This kind of GP scheme demands users to click on a sequence of points on one or multiple background images to construct their secrets. *PassPoints* [25] is an example, which requires users to recall a sequence of five selected points on a single background image. Another variant is developed by Chiasson *et al.* [4], called Persuasive Cued

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

Click-Points (PCCP), which requires users to select a point on each of a sequence of background images.

The existing GP schemes are mostly 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]

2.2 Map-based Graphical Passwords

The initial idea of using digital map in graphical password first appeared in [8], but not much details were given. Spitzer *et al.* [19] then proposed an implementation of *CCP* that combined the graphical approach with user's navigating familiarity through Google maps. In their settings, users were presented with an image of the United States and could simply click some defined key destination through identifying zooming levels.

In 2012, Georgakakis *et al.* [9] proposed *NAVI*, in which the credentials of a user are his username and a password formulated by drawing a route on a pre-defined map image. They provided an analysis about the password strength, but did not give any user study. Later, Sun *et al.* [22] proposed a map-based GP authentication system called *PassMap*, in which a password consists of a sequence of two locations on a world map. They performed a user study and showed that participants could be easy to remember *PassMap* passwords in practice. Similar to *PassMap*, Thorpe *et al.* [24] developed *GeoPass*, where a user chooses only one location as the secret. They reported that up to 97% participants 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). Meng [15] then designed *RouteMap*, which allows users to draw a route on a map as their password. Shin et al. [20] further implemented a modified version of *GeoPass* on a mobile device. These studies show that users may have a better memorability regarding map-based graphical passwords.

PassMap and *GeoPass* have been discussed more often than other map-based GPs. One big difference between them is to set location number, where *PassMap* requires users to select two locations while *GeoPass* only needs to choose one location. Intuitively, selecting one location is vulnerable to shoulder surfing attacks, while selecting two locations may add burden on users' memory. In the literature, Meng [15] previously compared the multiple password memory between *PassMap* and *GeoPass*. However, there is no study to explore the effect of location number on scheme performance, which can benefit future design of map-based GPs.

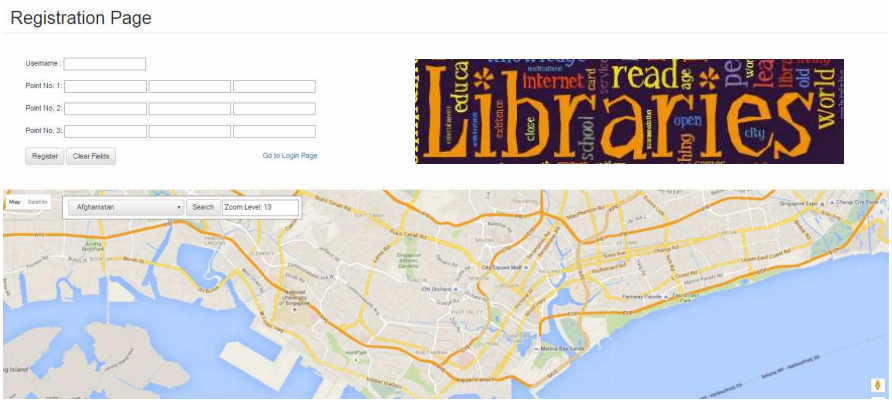

Fig. 1. The platform interface for map-based GP schemes.

3 Implementation and User Study

3.1 Platform and Scheme Implementation

As most map-based GP research did not release their source, we developed a Python-based open and generic platform to realize map-based schemes. The platform interface was deployed in our lab computers with a 17-inch screen, which can set up the required location numbers and zoom levels. In this case, our platform can realize most existing map-based GPs including *PassMap* and *GeoPass*. One interface example is shown in Fig. 1.

Platform Implementation. To develop the GP platform, we utilized the JavaScript based Google Maps API, which provides an extensive move-by-dragging, zooming and search functions. As shown in Fig. 1, when users zoom in/out on the map, our system reports and records 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 [22], 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, which is reasonable according to the results in [22, 24].

Scheme Implementation. Through applying different rules, our platform can realize various existing map-based GPs. To implement PassMap and GeoPass, we follow the same rules from [22, 24] as below.

- *GeoPass rules.* It requires users to choose only one location, which should be at zoom level 16. For authentication, users have to point out the same location at zoom level 16.
- *PassMap rules.* It allows users to select two locations at any zoom level. For authentication, users have to choose the same location in a right sequence. To avoid the effect of zoom levels, our system requires users to choose two locations at zoom level 16.

3.2 User Study

In this section, we conduct a user study with a total of 60 students to investigate users' performance between PassMap and GeoPass (approved by the Office of Academic Affairs), including 25 females and 35 males. All participants are volunteers and have no background of information security (i.e., no participant has taken any course related to information security before). The recruitment was done through emails and posters. In the study, participants were randomly divided into two groups (where each group contains 30 participants).

Methodology. Both PassMap and GeoPass are implemented on the same computer settings. Before the study, we introduced our objectives to all participants in advance. To avoid any bias, we presented a demo video and gave a detailed description to all the participants according to the same steps (i.e., how to use the prototype systems).

Before the experiment, each participant could have three trails to get familiar with the authentication system. In the study, we require all participants to create five passwords for each scheme and each password corresponds to a scenario. This study involves five scenarios 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 library account (see Fig. 1) 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 five *PassMap* passwords.
  - Step 1. Creation: creating a password for *PassMap*.
  - Step 2. Confirmation: confirming the password by drawing the same secrets in the correct place. If users incorrectly confirmed their password, they could retry the confirmation or return to Step 1.

- Step 3. Login: logging in the system with the created passwords. Users could cancel an attempt if they noticed an error.
- Step 4. Feedback: All participants were required to complete a *feedback form* about the password creation and confirmation.

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

- Step 4. Login: Logging into the prototype system with all created *PassMap* passwords. Users can cancel an attempted login if they noticed an error and try again.
- Step 5. Feedback: All participants should complete a *feedback form* about the password login.

– *Experiment2*. This experiment requires each participant to create five *GeoPass* passwords.
  - Step 1. Creation: creating a password for *GeoPass*.
  - Step 2. Confirmation: confirming the password by drawing the same secrets in the correct place. If users incorrectly confirmed their password, they could retry the confirmation or return to Step 1.
  - Step 3. Login: logging in the prototype system with the created passwords. Users could cancel an attempted login if they noticed an error.
  - Step 4. Feedback: All participants were required to complete a *feedback form* about the password creation and confirmation.

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

  - Step 4. *CD-GPS* Login: Logging into the system with all created *GeoPass* passwords. Users could cancel an attempted login if they noticed an error and try again.
  - Step 5. Feedback: All participants should complete a *feedback form* about the password login.

Ten-point Likert scales were used in each feedback question where 1-score indicates strong disagreement and 10-score indicates strong agreement. These collected questions and scores are mainly used to reflect participants' performance and explore their attitude on these two schemes. As a result, 150 real trails were recorded for *Experiment1* and *Experiment2* respectively.

Table 1. Success rate and average completion time for the step of creation, confirmation and login in *Experiment1* and *Experiment2*.

Experiment1 (PassMap)	Creation	Confirmation	Login
Success Rate (the first time)	120/150 (80.0%)	123/150 (82.0%)	127/150 (84.7%)
Completion Time (Average in seconds)	32.6	19.7	26.3
Standard Deviation (SD in seconds)	10.1	7.3	8.3
Experiment2 (GeoPass)	Creation	Confirmation	Login
Success Rate (the first time)	125/150 (83.3%)	128/150 (85.3%)	133/150 (88.7%)
Completion Time (Average in seconds)	28.2	17.1	20.6
Standard Deviation (SD in seconds)	8.7	6.5	7.2

Results. As shown in Table 1, *success rate* and *average completion time* are used for evaluating users' performance with the step of creation, confirmation and login in *Experiment1* and *Experiment2*. More specifically, *success rate* in the step of *Creation* means that participants created their passwords without restarting, *success rate* in the step of *Confirmation* means that participants confirmed their passwords without restarting and failed attempts for the first time, while *success rate* in the step of *Login* means that participants, for the first time, pressed the login button and entered into the example system successfully. *Average completion time* is an average value computed by all participants.

We also apply chi-squared (χ^2) tests for the collected data to compare non-ordered categorical or nominal data. In all cases, we regard a value of $\rho < 0.05$ as indicating that the groups being tested are different from each other, making the results statistically significant.

Success rate. In *Experiment1*, success rate is 80.0% and 82.0% for Creation and Confirmation respectively. Some participants restarted the password creation, as they changed their selected map area (i.e., from Singapore to Beijing city). On the other hand, some participants restarted or made failed attempts due to a wrong click, or incorrect zoom levels. For the Login, success rate is 84.7% where some failed attempts were due to incorrect zoom levels for the first time.

In *Experiment2*, success rate is 83.3%, 85.3% and 88.7% for Creation, Confirmation and Login, respectively. Similar to *Experiment1*, it is found that several participants restarted the creation, selected a wrong location, and made an incorrect zoom levels. The results in *Experiment2* seemed a bit better than *Experiment1*, but there are no statistically significant differences ($\chi^2 \approx 1.1,\ \rho > 0.05$; $\chi^2 \approx 1.2,\ \rho > 0.05$; $\chi^2 \approx 1.5,\ \rho > 0.05$).

Completion time. Average completion time in *Experiment1* is 32.6, 19.7 and 26.3 seconds for Creation, Confirmation and Login, respectively.

Table 2. Several main questions and relevant scores in the user study.

Questions	Score (average)
1. I could easily create *PassMap* passwords	8.5
2. I could easily create *GeoPass* passwords	8.7
3. I could easily log in *PassMap* system	7.8
4. I could easily log in *GeoPass* system	8.2
5. The time consumption in the *Experiment1* is acceptable	7.4
6. The time consumption in the *Experiment2* is acceptable	7.8
7. Are you willing to use *PassMap* passwords in practice	8.1
8. Are you willing to use *GeoPass* passwords in practice	8.3

Some participants spent much more time in Creation by considering how to choose a good location. Then, they spent less time in Confirmation. The time consumption increased a bit in Login, as participants needed to recall their locations.

In *Experiment2*, average completion time is 28.2, 17.1 and 20.6 seconds for Creation, Confirmation and Login, respectively. The situation is similar to *Experiment1*, in which participants could perform fastest in Confirmation. It is found that there are no statistically significant differences in Creation and Confirmation ($\chi^2 \approx 2.1,\ \rho > 0.05$; $\chi^2 \approx 1.8,\ \rho > 0.05$), but the results are significant for Login ($\chi^2 \approx 4.1,\ \rho < 0.05$).

Discussion. On the whole, based on the collected results, participants could perform a bit better in *Experiment2*. For example, participants in *Experiment2* could achieve higher success rate and less time consumption. However, these results are most no statistically significant differences. This indicates that participants did similar performance in both experiments, and there is no significant performance influence on selecting between one location and two locations.

Time consumption in Login is the only one significant result, which describes that participants could indeed perform a better login process in *Experiment2*. After informal interview with participants, it is found that selecting only one location is the main reason. In comparison, participants have to zoom-in/out levels and select two locations in *Experiment1*.

Feedback. To validate our collected data, we analyze the feedback from participants. Ten-point Likert scales were used in each feedback question and we present main questions and corresponding scores in Table 2. The scores are simply average values calculated by all received scores.

The scores in the first four questions indicate that most participants satisfied with the password creation and login in both passwords, while *GeoPass* received a bit higher score (8.7 and 8.2). For time consump-

tion, the scores went below 8 with 7.4 and 7.8. At last, most participants were willing to use map-based GPs in their daily lives. In our informal interview, we aimed to validate the feedback. Up to 42 (20 from *Experiment1* and 22 from *Experiment2*) participants were satisfied with the use of map-based GPs and interested in applying to their daily use. There are five participants (3 from *Experiment1*) showed no interest in daily use due to the consumption time.

Overall, most participants gave positive feedback for utilizing these map-based passwords, where they considered it is easier for them to remember than traditional textual passwords. They preferred that there were more memorable points on a map so that they could choose a secret based on their own knowledge.

4 Further Discussions

- *Security aspect.* Based on the results in [24], the most efficient attacker (i.e., has local knowledge) should have $2^{16.36}$ guessing attempts for *GeoPass* (with only one location). In the condition of two locations (like *PassMap*), the guessing attempts can be greatly increased. As stated early, selecting one location is more vulnerable to shoulder surfing attacks, in which attackers can get the secret using direct observation. Increasing location number can mitigate such attacks and increase the password entropy. Our motivation in this work thus focuses on exploring the effect of location number on scheme performance. The calculation of password space between *PassMap* and *GeoPass* can refer to [24, 22].
- *Usability aspect.* According to our study results, most participants gave positive feedback and were willing to use map-based passwords for authentication. It is found that there are no statistically significant differences between *PassMap* and *GeoPass* in the aspect of success rate and completion time, except for completion time in Login. This because selecting two locations is intuitively more time consuming than selecting only one location. The observation reveals that selecting two locations would not degrade the scheme performance.

Our study reveals that appropriately increasing location number is possible in designing map-based graphical schemes, whilst we should make a balance between security and usability (i.e., how to decide a proper number). To further investigate this issue, it is expected to have an even larger study with more diverse people.

5 Conclusion

In this paper, our main purpose is to explore the effect of location number between PassMap and GeoPass, which are two typical map-based graphical schemes. We conduct a user study with 60 participants and analyze the results in terms of users' performance (e.g., success rate, completion time) and feedback. The study results describe that participants did similar performance for both schemes, and there is no significant performance influence on selecting between one location and two locations. That is, there is a potential to increase location number in a map-based scheme. Our effort aims to complement existing studies and provide useful guidelines for designing more secure map-based graphical passwords.

Future work could include investigating the users' performance through increasing the location number to three or above, and exploring the effect of zoom levels on map-based graphical schemes.

Acknowledgments. We would like to thank all participants for their hard work and cooperation in the user study, and 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., 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. 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: Proceedings of the 14th International Conference on Information and Communications Security (ICICS), Lecture Notes in Computer Science 7618, Springer, pp. 349-356 (2012)
15. 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)
16. 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)
17. Passfaces, http://www.realuser.com/.
18. 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)
19. 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)
20. 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)
21. 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)
22. Sun, H., Chen, Y., Fang, C., Chang, S.: PassMap: A Map Based Graphical-Password Authentication System. In: Proceedings of ASIACCS, pp. 99-100, 2012.
23. 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)
24. 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)
25. 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)
26. 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)

27. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password memorability and security: Empirical results. IEEE Security and Privacy, vol. 2, pp. 25-31 (2004)