Multiple-Password Interference in the GeoPass User Authentication Scheme

Mahdi Nasrullah Al-Ameen and Matthew Wright
Department of Computer Science and Engineering
The University of Texas at Arlington
mahdi.al-ameen@mavs.uta.edu, mwright@cse.uta.edu

***Abstract*—Password schemes based on selecting locations in an online map are an emerging topic in user authentication research. GeoPass is the most promising such scheme, as it provides satisfactory resilience against online guessing and showed high memorability (97%) for a single location-password. No multiple-password interference study, however, has been conducted to see if GeoPass or any other location-based password scheme is suitable for real-world deployment, where users have to remember multiple passwords. In this paper, we report the results of two separate multiple-password studies on GeoPass, each conducted over the span of three weeks. In the first study, we aim to understand the effects of interference on GeoPass scheme, where we found that users remembered location-passwords in less than 70% of login sessions, with 41.5% of login failures due to interference effects. Through a detailed analysis, we identify why interferences occur for location-passwords, and based on our findings, we propose to leverage *mental stories* to address the interference issue. We then perform a second interference study on modified GeoPass scheme to test the efficacy of our approach, where we found that the login success rate was greater than 97% and 3.4% of login attempts failed because of interference effects.**

***Keywords*—User authentication; Geographic location-password; Interference study**

I. Introduction

Geographic location-password, where the user's password is a location on an online map (e.g., Google Maps), is a recent inclusion in the studies of user authentication. While both textual [1, 2] and graphical passwords [3–7] have failed to provide a viable solution to the usability-security tension in user authentication, geographic location-password presents a promising avenue to addressing this issue.

As noted by Thorpe et al. [8], the geographic location-password offers unique design features, as it involves elements of recognition, cued-recall, and pure recall, in addition to a mnemonic association of a meaningful place for the user. GeoPass [8] is the most promising geographic location-password scheme proposed to date. The short-term lab study conducted by Thorpe et al. [8] identified the potential of GeoPass by showing that it offers resilience to online guessing attacks while providing very good memorability for a single location-password (97%, found in a nine-day-long lab study).

The history of research in graphical passwords [7] makes it clear that unless the primary usability issues of a new category of passwords are identified in the initial phases of study, the later schemes in that category might fail to address the key drawbacks of the approach. Biddle et al. [7] identify multiple-password interference as a major usability concern and find in their extensive survey that only a handful of graphical password schemes have been evaluated with an interference study.

Password Interference [7, 9] occurs when users confuse the password of one account with that of another account. To the best of our knowledge, no interference study has been conducted yet on geographic location-passwords. Thus, to explore the full potential of this novel category of passwords, researchers need to examine memorability for multiple location-passwords and identify interference effects, with a goal of providing a suitable solution.

A. Research Goal

In this paper, we aim to investigate the effects of interference on geographic location-passwords, where we chose GeoPass for our study, since Thorpe et al. [8] show that GeoPass has the most potential among location-password schemes. We designed a systematic approach of exploration to achieve the goal, where we conducted *Study I* to understand the causes and effects of interference on GeoPass. In this study, we addressed the following research questions.

- **[Q1]**: How usable would GeoPass be when users would have to remember multiple location-passwords?
- **[Q2]**: How prominent will the interference effects be for multiple location-passwords?

We found that interference effects played a major role on the failure of login attempts in *Study I*, and identified the following research questions to be addressed to find a possible solution to this issue.

- **[Q3]**: Why does interference occur in GeoPass?
- **[Q4]**: How could we reduce interference effects and improve the multiple-password memorability for GeoPass authentication scheme?

Based on the analysis of *Study I*, we identified a solution to interference problem and conducted a follow-up study (*Study*

USEC '15, 8 February 2015, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2015.23004

II) to examine the efficacy of our proposed approach to reduce interference effects and thus improve the memorability for multiple location-passwords.

B. Contributions

Each of our two studies (*Study I* and *Study II*) was conducted over the span of three weeks. We used a separate group of participants for each study to prevent training effects from carrying over. Each participant had to remember four different location-passwords, one for each of four different accounts. Here, we provide a high-level overview of our contributions with references to the corresponding sections that accommodate detailed discussions.

[Q1]: In *Study I*, we found that users remembered location-passwords in less than 70% of login sessions (§III-C).

[Q2]: The results for *Study I* show that 41.5% of login attempts failed due to interference effects. We investigated both *accurate* and *non-accurate* interferences for an in-depth understanding of interference effects (§III-D).

[Q3]: As we investigated the causes of interference, we found that the interference effect between a pair of location-passwords had no correlation with the geographic distance between them (§III-E). Participants were not confused by location-passwords that were geographically close. Rather, they failed to associate their location-passwords with the corresponding accounts, and thus could not log in successfully.

[Q4]: Based on our analysis in *Study I*, we hypothesized that interference effects could be reduced if participants would be asked to make a *mental story* during registration to create a meaningful association between their location password and the corresponding account (§III-E). For example, in *Study II* that examines the efficacy of this approach, one participant chose "Bellagio Hotel" at Las Vegas as her location-password for *bank* account, while her story was: "Bank→ Money→ Las Vegas→ Bellagio."

In this way, participants could better memorize the location-password for a particular account. In *Study II*, we found 98% login success rate after one week and 99.3% success rate after two weeks of registration (§IV-A), while 3.4% of login attempts failed because of interference effects (§IV-B).

II. Background and Related Work

In this section, we first give a overview of location-password schemes proposed to date, followed by a brief discussion on multiple-password studies and an existing scheme that leverages the concept of mental story.

A. Location-password

Geographic location-passwords is a recent category in password research. In these schemes, users select one or more locations in an online map (e.g. Google Maps) as their password. To the best of our knowledge, three schemes [8, 10, 11] in this password-category have been proposed to date, where GeoPass [8], proposed by Thorpe et al. in 2013, shows most potential in terms of usability and security.

In GeoPass, the user's password is a single location on an online map (Google Maps). This secret location, known both as the *location-password* and just *geopass*[1], is selected by the user at registration by right-clicking on the map. The search bar helps to make navigation faster by enabling the user to type the name of a place. Also, typing leads to a drop-down menu suggesting locations in which the searched item may appear. Zooming and panning are also enabled via the Google Maps API. Using the convention that a higher-numbered zoom level represents being zoomed in closer, GeoPass allows the user to click on a location at a minimum zoom level of 16. A successful login requires the users to click within a 21x21 pixel box around the location-password they had set. We refer readers to Thorpe et al.'s paper [8] for in-depth discussion on the features of GeoPass.

Thorpe et al. [8] conducted a nine-day-long single-password study on GeoPass with three sessions: two in a lab-setting and one online. The login success rate was 97%, and the median login time was found to be no greater than 30 seconds [8]. The security analysis [8] showed that the theoretical password space for GeoPass is $2^{36.9}$, such that only 11% of online guessing attacks might be successful after allowing for 2^{16} guesses. In this respect, reasonable lockout rules [12] should make GeoPass sufficiently resilient against such attacks.

Other schemes. There are two other schemes that use map locations as an authentication secret: one proposed by Spitzer [11] and another one is called PassMap [10]. PassMap requires the user to choose two locations and the scheme by Spitzer [11] requires five or seven locations at different zoom levels to be selected as the location-password. Thorpe et al. [8] have shown that GeoPass is more usable than other digital-map-based schemes [10, 11] because of its requirement to click on a single location and normalized error tolerance to a given zoom level. The login success rate in GeoPass (97%) was found to be higher than that in PassMap (92.59%).

B. Multiple-password Study

Graphical password schemes can be divided into three categories, based on the kind of memory leveraged by the systems [7]: i) Cognometric (recognition-based), ii) Drawmetric (recall-based), and iii) Locimetric (cued-recall-based).

In cognometric graphical passwords, the user is asked to recognize and identify their password images from a set of distractor images. Everitt et al. [13] performed a multiple-password study on cognometric graphical passwords using facial images, which demonstrated that participants accessing four different facial passwords each week had a failure rate of 15.23% after a month, when each password was used once a week. Here, the average login time was 29.7 sec.

Locimetric graphical passwords present users with an image and have users select points on the image as their password. Chiasson et al. [9] tested the multiple-password memorability for locimetric graphical passwords, where 57% (15/26) of the participants were able to recall their graphical passwords successfully after two weeks of registration, and the average login time varied between 18 to 47 seconds. To

[1] in lowercase to avoid confusion with the system name

TABLE I. *Study I:* LOGIN PERFORMANCE OF THE PARTICIPANTS [SD: STANDARD DEVIATION]

	Success	Number of Attempts					Login Time				
Sitting	Rate (%)	Mean	Median	SD	Max	Min	Mean	Median	SD	Max	Min
login 1	58	2.8	1	4.2	26	1	59	43	47	188	9
login 2	67	3.1	1	3.7	18	1	45	35	39	203	8

the best of our knowledge, no multiple-password study was conducted on drawmetric graphical passwords, in which the user is asked to reproduce a drawing during login.

C. Mental Story

Davis et al. [5] implemented the concept of mental story to design a recognition-based graphical password. Their purpose and approach of leveraging mental story were different from ours. Their study tested the memorability for a single graphical password, where users were asked to build a story to remember a set of images in correct order. The study [5] found 85% login success rate over the span of one week, while the registration or login time was not reported. In our approach, we aim to leverage mental story in order to reduce multiple-password interference by asking users to create a meaningful association between their location-password and the account it is created for.

III. STUDY I

In this study, we explore the login performances and the corresponding interference effects when users have to remember multiple location-passwords in GeoPass [8]. All experiments received approval from our university's Institutional Review Board (IRB) for human subjects research.

A. Study Design

We conducted the study in a Computer Science (CS) class at our university that draws a broad range of majors. Out of 60 students in this class, 18 students (11 women and 7 men) participated in our study. Their mean age was 23. The subjects were compensated with extra credit in a class assignment for participating in this study, and an alternative assignment was offered for those who did not want to participate.

Haque et al. [14] classify websites into four categories: i) financial (e.g. WellsFargo.com), ii) identity (e.g. Gmail), iii) content (e.g., Netflix, Weather.com), and iv) sketchy (unfamiliar sites offering coupons and often attracting transient user relationships). We built one website from each of the above categories and refer to them in this paper as *bank*, *email*, *movie*, and *deals*, respectively. Each site was equipped with GeoPass for user authentication. The sites were designed to have the images and layouts from familiar commercial sites, with the exception of the deals site, which was designed to look less professional.

1) Procedure: The three-week-long lab-based interference study included three sessions, which we will call *sittings* (to distinguish from login sessions), each held one week apart. In the first sitting (*registration*), we gave the participants an overview of GeoPass and asked them to create a location-password for each account. To best study interference effects, the participants were asked to create a distinct geopass for each account. In the second and third sittings, users were asked to log into their four accounts from the lab computers. We refer to these latter sittings as *login 1* and *login 2*, respectively. The participants could log into the sites in any order.

If a participant failed to log into an account after five attempts, she was shown a button that she could use to view her geopass. She was also allowed to make more attempts without viewing her location-password. Once the button was clicked to view the geopass, however, the participant was no longer able to attempt to log into that account for that sitting.

B. Significance Tests

To analyze our results, we use statistical tests and consider results comparing two conditions to be significantly different when we find $p < 0.05$. When comparing two conditions where the variable is at least ordinal, we use a Wilcoxon signed-rank test for the matched pairs of subjects and a Wilcoxon-Mann-Whitney test for unpaired results. Wilcoxon tests are similar to t-tests, but make no assumption about the distributions of the compared samples, which is appropriate to the datasets in our conditions. Whether or not a participant successfully authenticated is a binary measure, and so we use either a McNemar's test (for matched pairs of subjects) or a chi-squared test (for unpaired results) to compare login success rates between two conditions.

C. Login Performance

Each of the 18 participants logged into four accounts in both *login 1* and *login 2*, making a total of 72 login sessions in each sitting. The results for login performances are shown in Table I. In this paper, *number of attempts* and *login time* respectively refer to the required attempts and time for successful logins only, unless otherwise specified.

The overall login success rates were 58% in *login 1* and 67% in *login 2* (see Table I). The mean number of attempts for successful logins were 2.8 in *login 1* and 3.1 in *login 2*, while the median was 1 in both sittings. The mean times for successful logins were 59 seconds in *login 1* and 45 seconds in *login 2*, while the medians were 43 seconds in *login 1* and 35 seconds in *login 2*.

We did not find any significant difference between *login 1* and *login 2* in terms of login success rate, number of attempts, or login time. We use a McNemar's test to compare the login success rate. We use Wilcoxon-Mann-Whitney tests while we compare *login 1* and *login 2* in terms of the login time or number of attempts for successful login, since we do not get matched pairs of subjects in this case as some participants who logged in successfully in one sitting failed in the other sitting.

TABLE II. *Study I:* SUMMARY OF THE INTERFERENCE EFFECT [TA: TOTAL ATTEMPTS, SA: SUCCESSFUL ATTEMPTS, ACC.: ACCURATE]

Sitting	TA	SA (%)	Failed Attempts (%)		
			Interference		Non-Interference
			Acc.	Non-Acc.	
login 1	282	14.9	5	39.8	40.4
login 2	309	15.5	1.9	36.3	46.3

D. Interference Effect

We now explain how we measure the interference effect and describe the corresponding results. In each sitting, every participant was asked to complete four login sessions, each for one account. We refer to the account corresponding to current login session as the *visible account* and refer to the other three accounts as *invisible accounts*. For example, when a participant attempts to log into the bank account, the bank account is visible, while email, movie, and deals accounts are considered invisible. Thus, a successful login requires the user to select the geopass of the visible account. Because of interference effects, a user may make mistakes and click on the geopass of an invisible account. Table II shows the summarized results for interference effects in our study.

1) Method of Computation: We did not restrict the number of attempts a participant can make for a successful login, and clicking at a location other than the geopass of the visible account results in an unsuccessful attempt. We figure out the impact of interference on the failure of an attempt in the following way: For each unsuccessful attempt, we measure the distances (in kilometers) between the clicked location and her geopasses for each of the four accounts. In this way, we find the account whose geopass is closest to the clicked location. If the closest account is the visible account, we assume that interference did not impact the failed attempt, and we show this as *non-interference* in Table II. If the closest account is an invisible account, we say that the attempt fails because of the interference effect. In this case, if the clicked location is a correct geopass for the invisible account, we classify it as *accurate interference*, and otherwise we call it *non-accurate interference*.

2) Results: Our results (see Table II) show that 14.9% of 282 attempts succeeded in *login 1*, while 44.8% attempts failed because of interference effects (considering both accurate and non-accurate interferences). In *login 2*, out of 309 attempts 15.5% were successful, and 38.2% attempts failed because of interference effects.

We use a Wilcoxon signed-rank test (appropriate for matched pairs of subjects) to evaluate the difference between *login 1* and *login 2* in terms of the number of failed attempts because of interference effects. We did not find any significant difference in this case, whether we consider accurate and non-accurate interferences together or separately.

E. The Causes of Interference and Possible Solution

It is possible that a user who selects two geopasses near each other may confuse them, leading to interference effects. We thus seek to determine whether the interference effect between a pair of accounts had any correlation with the distance between corresponding pairs of geopasses. However, we did not find any strong correlations in this respect either in *login 1* ($r = 0.12$) or in *login 2* ($r = 0.02$) (see [15] for details on how these correlations are measured).

Since the participants did not seem confused by geopasses that were geographically close, we speculate that they failed to associate their location-passwords with the corresponding accounts, which contributed to the interference effects while remembering multiple geopasses. So, we propose the following approach to address this interference issue. During registration, users would be asked to build a mental story to make a meaningful association between their location-password and the account it is created for. For example, in *Study II* (see §IV) that we conducted to test the efficacy of our approach, one participant chose a location for the bank account and built a story: "I had an accident here. The accident could interrupt the financial security of a family." Another participant chose for the deal account a location in Old Trafford, U.K., home to Manchester United, the famous football club that she said "make[s] good deals to get skilled players in the club."

In our approach, users are asked to type the story in a textbox, which is provided along with the Google Maps interface at registration. Users have the flexibility to build and type the story either before or after choosing the location-password. This story is not shown at login and thus is not required to be stored by the system. For the purpose of future analysis, however, we did retain the stories.

IV. STUDY II

In this section, we describe *Study II*, aimed at testing the effectiveness of our approach to address the interference issue in GeoPass.

The study design for *Study II* was same as that for *Study I*, except that participants had to come to lab only for registration in the first sitting and logged in from home in the second (after one week of registration) and third sittings (after two weeks of registration). Study II is thus, according to the terminology of Biddle et al., a hybrid study [7]. To log in from home, we sent emails to the participants with links that would redirect them to our server for logins. They had to complete the logins within 24 hours of getting the email.

The participants in *Study II* were recruited from a CS class at our university, which was a different class than that of *Study I* and drew mainly CS majors. No student participated in both *Study I* and *Study II*. Out of 60 students in this class, 38 students (mean age: 23) participated in our study. The compensation for participants was same as that in *Study I*. In both studies, participants were notified that their performances in the study would not affect the compensation. They had not taken any courses on usable security or human-computer interaction, nor had they participated in a password-related user study.

A. Login Performance

Each of the 38 participants logged into four accounts in both *login 1* and *login 2*, making a total of 152 login sessions in each sitting. The results for login performances are shown in Table III.

TABLE III. *Study II:* LOGIN PERFORMANCE OF THE PARTICIPANTS [SD: STANDARD DEVIATION]

	Success	Number of Attempts					Login Time				
Sitting	Rate (%)	Mean	Median	SD	Max	Min	Mean	Median	SD	Max	Min
login 1	98	1.6	1	0.1	11	1	43	27	2	242	8
login 2	99.3	1.8	1	0.1	29	1	39	25	3	330	8

TABLE IV. *Study II:* SUMMARY OF THE INTERFERENCE EFFECT [TA: TOTAL ATTEMPTS, SA: SUCCESSFUL ATTEMPTS, ACC.: ACCURATE]

			Failed Attempts (%)		
			Interference		Non-Interference
Sitting	TA	SA (%)	Acc.	Non-Acc.	
login 1	237	62.9	2.1	2.1	32.9
login 2	268	56.3	0	2.6	41.1

The overall login success rates were 98% in *login 1* and 99.3% in *login 2*. The mean number of attempts for successful logins were 1.6 in *login 1* and 1.8 in *login 2*, while the median was 1 in both sittings. The mean times for successful logins were found to be 43 seconds in *login 1* and 39 seconds in *login 2*, while the medians were 27 seconds in *login 1* and 25 seconds in *login 2* (see Table III). We did not find any significant difference between *login 1* and *login 2* in terms of login success rate, number of attempts, or login time.

B. Interference Effect

We measured the interference effect in the same way as described in §III-D1. Our results (see Table IV) show that 62.9% of 237 attempts succeeded in *login 1*, while 4.2% attempts failed because of interference effects (considering both accurate and non-accurate interferences). In *login 2*, out of 268 attempts 56.3% were successful, and 2.6% attempts failed because of interference effects.

The results for Wilcoxon signed-rank test show that there was no significant difference between *login 1* and *login 2* in terms of the number of failed attempts because of interference effects, whether we consider accurate and non-accurate interferences together or separately.

V. DISCUSSION

In our studies, we consider geographic distance to understand the interference effects on GeoPass. We distinguish the login attempts that failed because of confusion with other passwords (i.e. likely interference) from attempts that failed due to simply forgetting the desired password (i.e., non-interference). We investigated both accurate and non-accurate interferences for an in-depth understanding of interference effects. As noted by Biddle et al. [7], how to best evaluate multiple password interference still remains an open issue; our methodology for analyzing the interference effect should make an important contribution in this regard. In future evaluations, we would further improve our interference model by considering the interference because of confusion between two similar types of locations, such as two small islands in the ocean.

Our studies suggest that having users create a mental story contributes to reduce interference effects and gain high memorability when users have to remember multiple location-passwords. In *Study I*, users remembered location-passwords in less than 70% of login sessions, with substantial interference between different passwords. In *Study II*, the success rates were at least 98%, with very low rates of interference. While it would be inappropriate to compare the two studies statistically due to the different study populations, the success of *Study II* suggests that the mental story approach is promising and deserves further refinement and investigation.

The mental story approach offers theoretical benefits to memorization. First, the mental story works as a cue to remember new information, while an elaborative encoding (for new information) from short-term memory to long-term memory takes place when the information can be associated with something meaningful, such as cues [16]. This encoding helps people to remember and retrieve the processed information efficiently over an extended period of time [16]. Second, the mental story requires deeper processing of both the place selected and the relevant account type together. The depth of processing effect theory says that processing the meaning of the information, rather than at a more shallow level, increases the ability of the user to retain the information [17]. Typing the story may help to engage the user's mind further compared to an entirely mental-only approach.

The mental story approach also has some potential downsides that must be investigated. First, it is not clear what the effect is on security for users to pick locations related to their account in some way. We found some imaginative ways to incorporate the account information, but one might imagine many people picking Fort Knox for a banking site and the Facebook company headquarters for their Facebook passwords. In general, Geopass could have problems with common locations; blocking the most common ones could be effective much like proactive dictionary checks on textual passwords can improve password strength. Second, we cannot be sure that users will follow the requested steps in real-world deployments. Automated evaluation of the story quality, e.g. checking for minimum length and the presence of real words instead of gibberish, could help.

A. Ecological Validity

The participants in our studies were young and university educated, which may not generalize to the entire population. While lab-study is preferred to examine the primary usability issues and set performance bounds for an authentication scheme, a hybrid study could provide higher ecological validity when login sessions are performed online [7]. So, we conducted *Study I* in a lab setting to understand the causes and effects of interference, and then designed a hybrid study for *Study II* to test the efficacy of our proposed approach. It is possible that the hybrid setting in *Study II* let us have more participants than *Study I*, since participants did not need to come to lab for the login sessions in *Study II*. We had one week of interval between each session, since the one-week delay is

larger than the maximum average interval for a user between her subsequent logins to any of her important accounts [18].

In *Study I*, participants came from diverse backgrounds while the participants in *Study II* were CS majors. Since the background of the participants might have an impact on the login performances, we would further investigate this issue with larger and more diverse populations in future work.

In real-life, users may have to remember more than four passwords. The prior multiple-password studies [1, 13, 19] asked users to remember either three or four passwords. Being consistent with the prior work, we asked the participants to remember four location-passwords in our study, in which all the passwords were created in the same sitting. This registration process is in agreement with prior work [1, 19], while in real life the geopasses would likely be created over time and possibly in different contexts, e.g. in different rooms or with different computers.

VI. Conclusion and Future Work

In our first study (*Study I*), we aimed to understand the causes and effects of interferences on geographic location-passwords, and found multiple-password interference playing a major role to reduce login success rates. Based on our findings, we propose to leverage mental story in reducing interference effects, and found a high login success rate as we tested this approach in *Study II*.

In our study, we stored the stories for the purpose of future analysis. Now, we would focus on a comprehensive analysis to categorize the stories based on different types and keywords, and figure out the correlations, if any, between the predictability of a location-password and the category of corresponding story. This may enable us make useful suggestion for users to build a mental story.

Measuring the cognitive effort of building mental stories by the people from different age groups and backgrounds could be an interesting venue for future work. We plan to investigate this issue in order to design an effective mechanism that could make the mental story a successful tool for memorizing authentication secrets.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1117866 and CAREER Grant No. CNS-0954133. We are thankful to the anonymous reviewers for their thoughtful suggestions in improving the paper.

References

[1] N. Wright, A. S. Patrick, and R. Biddle, "Do you see your password? applying recognition to textual passwords," in *SOUPS*, 2012.

[2] A. Forget, "A world with many authentication schemes," Ph.D. dissertation, Carleton University, 2012.

[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *USENIX*, 1999.

[4] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *SOUPS*, 2005.

[5] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical password schemes," in *USENIX*, 2004.

[6] "Passfaces corporation," The science behind Passfaces. White paper, http://www.passfaces.com/enterprise/resources/white_papers.htm.

[7] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys*, vol. 44(4), 2012.

[8] J. Thorpe, B. MacRae, and A. Salehi-Abari, "Usability and security evaluation of geopass: a geographic location-password scheme," in *SOUPS*, 2013.

[9] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text and click-based graphical passwords," in *CCS*, 2009.

[10] H. Sun, Y. Chen, C. Fang, and S. Chang, "A map based graphical-password authentication scheme," in *ASIACCS*, 2012.

[11] J. Spitzer, C. Shingh, and D. Schweitzer, "A security class project in graphical passwords," *Journal of Computing Sciences in Colleges*, vol. 26 (2), p. 7, 2010.

[12] D. Florencio, C. Herley, and B. Coskun, "Do strong web passwords accomplish anything?" in *HotSec*, 2007.

[13] K. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in *CHI*, 2009.

[14] S. M. T. Haque, M. Wright, and S. Scielzo, "A study of user password strategy for multiple accounts," in *CODASPY*, 2013.

[15] M. N. Al-Ameen and M. Wright, "A comprehensive study of the GeoPass user authentication scheme," arXiv:1408.2852 [cs.HC], Tech. Rep., 2014.

[16] C. R. Atinkson and M. R. Shiffrin, "Human memory: A proposed system and its control processes," *K.W. Spence and J.T. Spence (eds), Advances in the psychology of learning and motivation, New York academic press*, 1968.

[17] F. I. Craik and E. Tulving, "Depth of processing and the retention of words in episodic memory." *Journal of experimental Psychology: general*, vol. 104, no. 3, p. 268, 1975.

[18] E. Hayashi and J. I. Hong, "A diary study of password usage in daily life," in *CHI*, 2011.

[19] M. Hlywa, R. Biddle, and A. S. Patrick, "Facing the facts about image type in recognition-based graphical passwords," in *ACSAC*, 2011.