Usability and Security Evaluation of GeoPass: a Geographic Location-Password Scheme

Julie Thorpe
University of Ontario
Institute of Technology
Oshawa, Canada
julie.thorpe@uoit.ca

Brent MacRae
University of Ontario
Institute of Technology
Oshawa, Canada
brent.macrae@uoit.net

Amirali Salehi-Abari
University of Toronto
Toronto, Canada
abari@cs.toronto.edu

ABSTRACT

We design, implement, and evaluate GeoPass: an interface for digital map-based authentication where a user chooses a place as his or her password (i.e., a "location-password"). We conducted a multi-session in-lab/at-home user study to evaluate the usability, memorability, and security of location-passwords created with GeoPass. The results of our user study found that 97% of users were able to remember their location-password over the span of 8-9 days and most without any failed login attempts. Users generally welcomed GeoPass; all of the users who completed the study reported that they would at least consider using GeoPass for some of their accounts. We also perform an in-depth usability and security analysis of location-passwords. Our security analysis includes the effect of information that could be gleaned from social engineering. The results of our security analysis show that location-passwords created with GeoPass can have reasonable security against online attacks, even when accounting for social engineering attacks. Based on our results, we suggest GeoPass would be most appropriate in contexts where logins occur infrequently, e.g., as an alternative to secondary authentication methods used for password resets, or for infrequently used online accounts.

Keywords

User authentication; passwords; usability; security; digital maps; map search; location-passwords.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Human Factors; Security; Design; Measurement.

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK

1. INTRODUCTION

It has long been recognized that traditional text passwords have problems relating to their memorability and vulnerability to being easily guessed by an adversary [41]. More recently, it has been demonstrated that the security problems with text-based passwords are even worse than previously believed [39, 6]. In order to ensure security requirements are met, unusable password policies are implemented that cause an increasing burden on users [21]. When passwords are forgotten, many systems rely on memorable secondary authentication methods such as challenge (or "personal knowledge") questions to prove the user's identity before resetting his or her password. Unfortunately, such methods for recovering forgotten passwords also appear to offer questionable security [32, 7]. These issues motivate new user authentication strategies that have improved memorability and security.

It is well-known that people generally have better memory for images over words [27]. The picture superiority effect has motivated many graphical password schemes that involve users remembering images (or parts of images) instead of words [4]. Cheswick [19] hypothesized that digital maps could be used in user authentication to create a strong yet memorable password. We hypothesize that location-passwords should be highly memorable under an appropriate system design that reduces the amount of user effort; after all, map locations are visual, and represent places (which may be more "concrete", and thus easier to remember [26]). A challenge that we tackle is designing a location-password interface that reduces user effort to achieve high memorability and provide reasonable security against online attacks.

We developed a map-based user authentication system using the Google Maps API that we call GeoPass, in which a user chooses a single place as their password. Similar to other map-based user authentication systems [35], GeoPass makes use of the Google Maps API's search and zoom features to enable fast zooming of a digital map. Fast zooming is critical to reduce the amount of navigation required (and thus the input time, as long as these features are used). In GeoPass the user only needs to remember the final location – but not their method of navigating there.

We performed a multi-session in-lab/at-home user study of GeoPass involving 35 users who were not in IT programs and had not previously taken a security course. Our study had three sessions to test memorability over the span of 8-9 days. 35 users completed an in-lab session on day 1, 33 completed an at-home/online session on day 2 (2 users did not return to our online system on day 2), and 30 of these users returned for a final in-lab session (three users on day 8 and 27 on day 9). The results of this study indicated that the memorability of location-passwords was quite strong. Of the 33 participants who logged in online for session 2 (one day after session 1), none of them forgot their location-password. Of the 30 participants who returned for session 3 (about one week after session 2), only one participant failed to enter their password; this participant remembered the general place they chose, but not with enough precision for successful authentication. There were very few failed login attempts throughout the entire study. Most users were able to successfully login by re-entering their location-password on their first attempts.

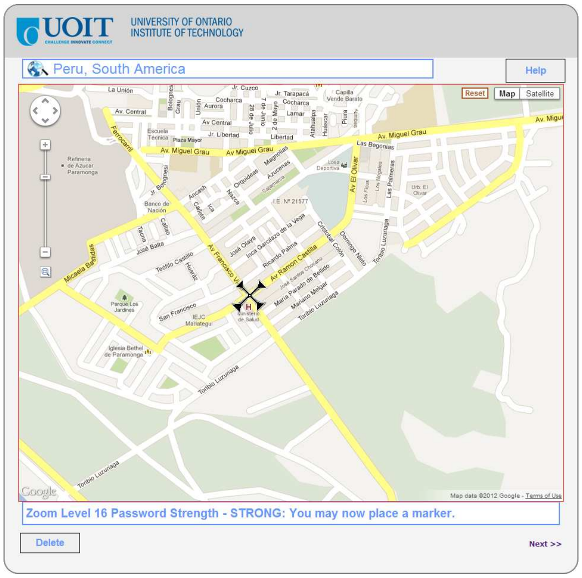
Our usability results indicate that GeoPass is likely best-suited for contexts where logins are infrequent (e.g., as a secondary authentication method in place of personal knowledge questions commonly used for password resets, or websites that users generally login to once per week). This is due to its strong memorability results and that the login times are longer than regular text passwords. Although users generally welcomed GeoPass (all of the users who completed the study reported that they would either consider using GeoPass for some of their accounts, or that they would use it for some or most of their accounts), we must be cautious about recommending its use for environments where logins are frequent. Our security results indicate that GeoPass provides enough security to protect against online attacks. GeoPass may also be useful as a building block for future user authentication systems; some possible extensions are discussed in Section 7.

Our contributions include: (1) a description of design choices for GeoPass, (2) an in-depth usability evaluation of location-passwords created with a single map location, (3) an in-depth security analysis of user choice in location-passwords, which includes evaluating the threat of social engineering or known adversaries, and (4) a discussion of possible extensions of GeoPass for stronger security.

The remainder of this paper is organized as follows. Section 2 describes our GeoPass design. Section 3 provides the methodology for our user study, Section 4 presents the user study results, and Section 5 discusses the security analysis. Related work is described in Section 6. Of course, since this is the first study towards determining the feasibility of using GeoPass for user authentication, further studies are needed; such future work and possible extensions to the system are discussed with concluding remarks in Section 7.

2. SYSTEM DESIGN

In the GeoPass system, a *location-password* is a point on a digital map that is selected by a user as his/her password. The user sets a location-password anywhere on the map simply by right-clicking on their desired location. We chose right-clicking to avoid confusion, as double left-clicking is normally associated with zooming in on Google Maps. To provide feedback to the user, we place an "X" marker at the location the user selects. To login (or authenticate), the user must be able to place the "X" marker again near his or her previously chosen location. Some error tolerance is permitted, as discussed below. GeoPass makes use of the Google Maps API in implementing its map display, zoom, search, and marker placement features[1].



Peru, South America

Zoom Level 16 Password Strength - STRONG: You may now place a marker.

Figure 1: The GeoPass system. The "X" marker represents the user's password.

2.1 User Interface Components

The user interface components of GeoPass were intended to enable and support faster navigation on the digital map. The main components are the search bar, zooming options, panning options, and zoom level indicator, which are discussed below. At any time, the user can press a "Help" button to release a menu that pops out to the right-hand side of the map that describes the components at their disposal.

2.1.1 Search Bar

The search bar component can make navigation faster by enabling the user to type the name of a place. There is some ambiguity regarding many search terms (e.g., the user could type "London" and it would not know which London the user is attempting to search for, as it could exist in the United Kingdom or Canada). To reduce this ambiguity, we decided to make use of the Google Maps API drop-down menu which suggests the locations in which the searched term appears. Then, the user needs to select a specific item from this drop down menu in order to zoom into that location.

2.1.2 Zooming and Panning Options

We enabled the zooming and panning options that are available in the Google Maps API. Zooming options included double-clicking to zoom in, the vertical zoom bar (with clickable + and - buttons), and a "drag-zoom" option that allows drawing a square on an area to zoom in upon. Panning was enabled through (1) dragging the map, and (2) using the pan control in the upper left-hand corner.

2.2 Usability/Security Design Trade-offs

Here we describe some of the trade-offs between usability and security in the design of GeoPass, the decisions for which were made based on the results of pilot studies described in Section 3. These design choices differ from those in other documented map-based user authentication systems [35].

[1] GeoPass is implemented as a web application, compatible with updated versions of Google Chrome and Firefox.

2.2.1 *Zoom Level Requirements*

In the Google Maps API, the zoom level indicates how far the user has zoomed into the map, where a higher numbered zoom level represents being zoomed in further. Higher zoom levels have more map detail, which allows for higher security as more locations are possible location-password choices. On the other hand, the further a user is required to zoom in, the more time-consuming it is to create, confirm, and login with their location-password. We determined through pilot studies that when users zoomed in further than zoom level 18, the amount of detail available on the map often decreased, and users had difficulty navigating the maps. For example, at zoom level 18, in rural areas, the streets, buildings, and landmarks would no longer be visible and would appear as an empty green area. Depending on the area, we also occasionally observed this happening at zoom level 17.

Thus, we set a minimum zoom level of 16 for setting or re-entering location-passwords, but allow users to zoom in further if desired. Zoom level 16 provides a decent amount of detail that users can choose in most locations, e.g., where streets and buildings can be seen. The user is informed of the zoom level and whether the minimum required zoom level is reached in the message bar located immediately below the map (see Figure 1). This message bar is red until the user reaches zoom level 16, after which it turns blue. Right-clicking to place a marker is only enabled once users reach zoom level 16. In the event that the user attempts to set a marker when the zoom level is less than 16, a pop-up box appears indicating that the zoom level is not high enough and the user must zoom in further to select or re-enter their password. However, we observed in our study that when users use the search bar for faster navigation they are often brought near zoom level 16, so rarely saw this message.

Once their location-password is set, users are presented with a message box telling them that they will need to remember the same location in the future to login.

2.2.2 *Initial Zoom Level*

GeoPass initially displays the map at zoom level 2 as shown in Figure 6 where most of the world is visible. Zoom level 1 was not chosen as it often showed repetition of the map in order to fill the screen. This default setting has the advantage of not influencing the user's choice in any way towards a certain subset of possible location-passwords. Another possibility would be to randomize the location at a lower (e.g., country or city) zoom level; however, this could have other usability implications that ought to be studied separately. The initial zoom level of 2 could have a usability disadvantage in that the user must zoom in from zoom level 2 to at least zoom level 16. As discussed in Section 4.3, most users appear to avoid this by using the search bar.

2.2.3 *Error Tolerance*

In order to successfully login, a user must place the marker within a 21 × 21 pixel box around the location-password they had set. The longitude/latitude of the "X" marker is converted to pixels and the error tolerance is calculated at zoom level 16. For example, if a user sets their password at zoom level 17, then upon login sets their marker at zoom level 16, the error tolerance is still a 21 × 21 pixel box. The reason for basing the error tolerance on zoom level 16 is that our pilot studies revealed that users often did not recall the exact zoom level in which they set their location-password. We chose this 21 × 21 pixel box error tolerance setting as studies in click-based graphical passwords have found a similar error tolerance to be sufficient [13, 37]. It is possible to securely store this information and allow for error tolerance using discretization methods [5, 11].

3. USER STUDY

We first conducted a preliminary pilot study to examine GeoPass's interface for usability and other issues that could affect security. We iterated our prototype/pilot testing of the system in order to eliminate obvious usability barriers in our implementation or missing instructions. This was done first with three colleagues in the security and usability fields, then a colleague in another field, and finally with four very casual computer users. This helped us refine our instructions to users for the main study, add some user interface features such as the help menu and zoom error pop-up, and decide to base the error tolerance on zoom level 16. Then, we conducted a multi-session user study to test the system's usability and security. Our user study initially had 36 participants, who were university students who have not taken any courses in computer or information security, as described in Section 3.1. One of the 36 participants chose to opt-out prior to creating a location-password for unknown reasons, thus we only report on data for 35 participants.

3.1 Sessions

We evaluated the security and usability of the GeoPass system through user studies conducted over three sessions:

- Session 1 (day 1, held in lab). Participants created and confirmed a location-password in a lab environment. If they were unable to successfully confirm, they were asked to re-create and re-confirm. After a successful confirm, the user was distracted for 10-20 minutes with a background questionnaire. At the end of the session, they were asked to login with their location-password. 35 participants completed this session.

- Session 2 (day 2, held on-line). Session two could be completed between 24-48 hours after the end of session 1. We held this session approximately one day later to model the frequency of logging on to email/messaging accounts (which a study of 20 users self-reported to be an average of 0.9 times/day [20]). Participants logged in on-line with their location-password from a convenient location of their choice. The investigators were not present to observe this session. Only 33 of our 35 participants logged on for this session and 2 did not continue with the study.

- Session 3 (day 8 or 9, held in lab). Session three was arranged seven days after session 2 (day 9) if possible; three participants could not attend session 3 seven days later so completed this session six days later (day 8). We held this session approximately one week later to model the frequency of logging on to financial accounts (which a study of 20 users self-reported to be an average of 1.3 times/week [20]). Participants logged in with their location-password and completed a feedback questionnaire in a lab environment. Only 30 of our original 35 participants returned to complete this session.

3.2 Demo Video

Each user was shown a demo video at the start of session 1 which explained that the task was to choose a place on the map as his or her password. Users were then told that they are required to choose a place that is easy for them to remember but difficult for others to guess, at a zoom level that provides enough detail for the location-password to be secure enough. The video explained that the fastest way to do this is to make use of the search bar at the top of the screen. The video walked through the other interface features as the demonstrator showed herself choosing a location-password. The demonstrator began by saying that what she will first do is to think of a place that is special to her and easy for her to remember. The participants were recommended to avoid choosing a previous home or work address; this recommendation was given for security reasons.

3.3 Environment

For each session, the participants logged in using a laptop. In most cases, the laptop used was their own personal laptop. The lab studies (sessions 1 and 3) were conducted with one participant at a time to allow the researchers to observe the user's interaction with the system while session 2 was conducted online from a location of the user's choice. The lab studies were conducted in an isolated room (to avoid distractions) on the UOIT campus.

3.4 Participants

We recruited participants from the UOIT campus by email and posters. Participants were entered into a draw for $50 to begin session one, and a guaranteed total of $10 to complete all three sessions. Our study received approval from UOIT's Research Ethics Board.

We collected information about our participant's background through the use of a questionnaire in Session 1. For all of our questions, participants were given the option to not answer. Twenty-two (62.9%) of our participants were male, thirteen (37.1%) were female. All were university students pursuing a degree but did not have formal training in Computer Security. The reason for selecting students who did not have such training was to avoid participants who are more likely to have a heightened awareness of security.

We also gathered information relating to our participant's previous experience and proficiency in using maps. When asked how often they use a map, 14% answered "daily", 28% answered "once/week", 54% answered "less than once/week", and 3% did not answer. Only 71% felt that they could find any location on an electronic map in an acceptable amount of time. Interestingly, only 54% felt that they could find any location in an acceptable amount of time on a traditional paper map. Our study population is more inclined to enjoy looking at maps than not. When asked whether they enjoy looking at maps, 71% answered yes and 29% answered no.

The participants in our study generally seemed to be concerned about passwords. 51% reported being very concerned, 37% reported being a little bit concerned, 6% reported not being concerned at all, 3% reported never considering the security of passwords, and 3% did not report their concern. We also asked the users whether they think their password(s) could be guessed by someone who knows them: 17% answered yes and 83% answered no. We asked our participants "What criteria do you use for choosing a password?", for which they could answer one, more, or none of the possible answers. The most popular answers were that they are difficult for others to guess (57%), easy for them to remember (54%), and when possible they reuse their passwords (46%). Eight of our participants (23%) reported using aids such as password managers or generators.

3.5 Limitations and Ecological Validity

We recruited UOIT students who were not in an IT program and had not taken a computer security course, to avoid participants who may have heightened awareness of what makes a good password. As the participants in this study are university students, we acknowledge that they are not fully representative of the users who would use the system. It is possible that they may have travelled to more diverse places and/or have better spatial memory than the general population. Our participants would have been aware that we were testing security of an authentication system based on the recruitment posters and emails. Thus, it is possible that they were more inclined to think about security and choose what they thought was a more secure place.

The study did not make use of a formal practice or training period. As a result, 17% of users needed to try creating their password more than once. Unfortunately, we did not account for this in the times recorded by our system, so we do not have information on the times for these failed creations. If we were to re-do this study, this is something we would change in order to measure these times. However, it seems positive that 83% of users were able to successfully create a location-password without any failed creations or practice.

Some of the questions used in our questionnaires may have been better if structured as Likert scale questions rather than yes/no questions. This is also something we would change if we were to re-do this study, in order to obtain the level of agreement users have with various statements.

This study was performed partially in the lab as it was the first study of GeoPass so we were interested in gathering qualitative data on the system's usability. As it was performed in a lab setting, we were only able to gather data from 35 participants. It is possible that there may be other patterns in user choice that we did not observe in the present study, which might become apparent in a large scale data set. Now that we have observed the performance of GeoPass in a lab setting, it seems reasonable to plan future work that evaluates GeoPass with larger and more diverse populations over longer time periods, and also evaluate the effects of interference with multiple location-passwords. Given how little research exists on location-password systems to date, and than none exists with our GeoPass design, it would have been premature to begin such studies at this point in time.

4. USER STUDY RESULTS

Here we discuss the results of the user study described in Section 3. Section 4.1 describes memorability findings and Section 4.2 describes other usability measures. Section 4.3 describes the navigation strategies used and how they relate to login times, and Section 4.4 discusses some qualitative observations.

4.1 Memorability

Our study demonstrated high memorability for GeoPass. Only two users in our study (see Figure 2 values for M3 and M5) reported any trouble remembering their location (one user in session 1 and another user in session 3); of course, we can comment on each of these two cases. The one user who reported not being able to remember his/her location-password on day one was the one participant who required a password reset in the first session. This user reported remembering the place, but had difficulty navigating back to the original location chosen, likely due to spending considerable time dragging the map before setting the marker. This is the same user who had four failed login attempts in Session 1 (see Figure 3). The other user who reported forgetting his/her location-password a week later actually remembered it, but was re-entering the marker just outside of the system's 21 × 21 pixel error tolerance. This is the same user who had six failed login attempts in Session 3 (see Figure 3). The only other user who had more than one failed login attempt was in Session 3, where the user was left-clicking on the correct location (as opposed to right-clicking) and not realizing it due to a Google Maps information box popping up. Since this was a problem with our system, as opposed to the user forgetting, we eventually let the user know that the marker is set through right-clicking, after which the user was able to login.

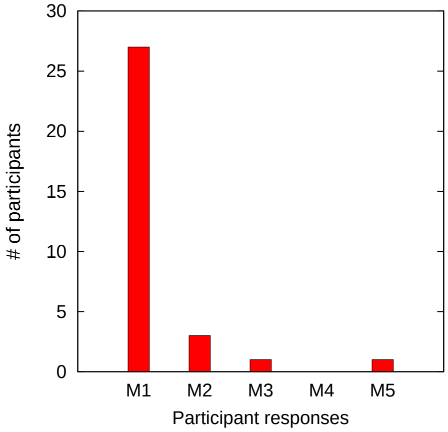


Figure 2: Post-questionnaire responses to the question "How easy was it for you to remember the location you chose?".
M1 - I had no trouble remembering it.
M2 - I think I could remember it for about a month.
M3 - I was unable to remember it on the first day.
M4 - I was unable to remember it on the second day.
M5 - I was unable to remember it the next week.

The memorability of the system can be further quantified by both the number of password resets (2.9% or $\frac{1}{35}$ in session 1, 0% in session 2, and 3.3% or $\frac{1}{30}$ in session 3) and the low number of failed login attempts in each session (see Figure 3).

Our 3% ($\frac{1}{30}$) "forgotten" location-passwords after one week compares favorably to other password schemes; studies by others [40] found that 35% ($\frac{7}{20}$) of regular text passwords and 30% ($\frac{6}{20}$) of one type of graphical passwords were forgotten after 1 week. In the case of regular text passwords, interference with the user's existing text passwords may have been an influencing factor. The performance of GeoPass also compares favorably to another location-password scheme [35] after one week, where 23.46% of users failed to login on the first attempt (compared to 10% with GeoPass), and 7.41% of users failed to login after 6 attempts (compared to 3% with GeoPass after 5 attempts).

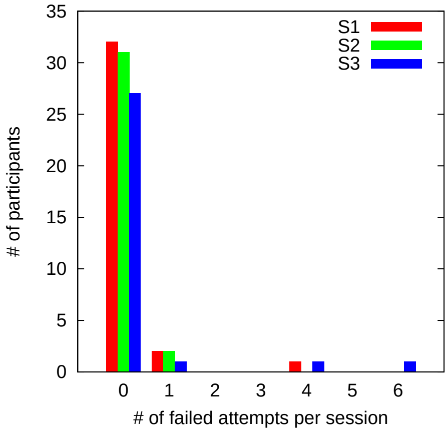


Figure 3: Number of participants (y-axis) with each possible number of failed login attempts (x-axis) for session 1 (S1), session 2 (S2), and session 3 (S3).

At present, it is not clear why GeoPass exhibits such strong memorability. One possible explanation could be that location-passwords are memorable due to a mnemonic association between a user's memory of a meaningful place and their visual memory of a specific location within it. Users' comments indicate that many think of a memory (e.g., first time seeing someone) and chose a high-level place associated with it (e.g., a specific park). Users must then select a specific location in that place (e.g., right corner of the playground), which may require visual memory. Another possible explanation could be that the navigation task (i.e., the steps the user takes to get to the destination location) act as clues to help the user recall the destination.

4.2 Usability

Most of the participants of this study were able to successfully navigate the digital map to the place they desired. Figure 4 shows the times recorded for location-password creation, confirmation, and login for each session. Some users experienced a bit of difficulty finding a memorable location in session 1; however, once they found it, most were able to quickly return to that location again. In the cases where participants spent extra time on creation, the reason was due to (a) not being able to find their search term in the search drop-down menu and/or (b) they dragged the map after zooming in, a strategy that seemed to increase the difficulty of navigating back to their chosen location.

The median times for logging in for sessions 1, 2, and 3 are 25s, 30s, and 25s respectively. These times compare favorably to another location-password system [35], which had a median login time of 33s on day one, and 52s after one week. There were some users who took quite a bit longer, as shown by the whiskers in Figure 4. Of the users whose

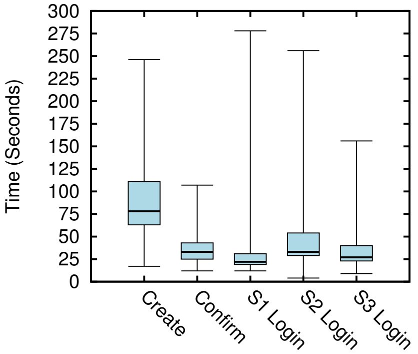


Figure 4: Box-and-whiskers plot showing times for creation, confirming, and logging in for each session.

times were long, most were due to using substantial panning within the map to navigate to their chosen location. The one participant who had forgotten their location-password in session 1 had engaged in substantial panning navigation on creation. The users who had difficulty confirming their location-password were most often attempting to navigate by panning rather than searching or repeatedly zooming in from a point of reference. As such, advanced techniques in usable map navigation such as overviews or hierarchical representations [22] may be useful future enhancements to GeoPass, to offer users better perception of the currently zoomed location.

The users who were fastest at inputting their location-password simply searched for a specific location and then placed their pointer without any further zooming or panning. Generally, when the user's intended search term appears in the drop down menu, this approach works very well. However, we observed a number of cases where the user's search term did not appear in the drop down menu, which points to one possible direction for improvement of our interface.

It is worth noting that in session 1, 83% of users were able to successfully set and confirm their location-password without any failures. However, 17% had an initial set of failed confirms when first using the system and before their first successful create, which is not included in the time to create in Figure 4. In future versions of GeoPass, it may be helpful to allow users an opportunity to create a practice location-password before moving on to create.

Response	% users
I would consider using this method for some of my accounts.	30% (9/30)
I would use this method for most of my accounts.	40% (12/30)
I would use this method for some of my accounts.	37% (11/30)
I would not use this method.	0% (0/30)

Table 1: Percentage of responses to post-questionnaire question "Would you use this method for your accounts?". Note that users could select more than one of these options.

In the end of Session 3, we asked users a few questions to understand how users perceived the usability of the system. In particular, we asked them "Would you use this method for your accounts", to determine whether they would actually use GeoPass if given the option to do so. Users were able to provide more than one answer to this question. Table 1. shows that 40% of users would use GeoPass for most of their accounts, 37% would use it for some of their accounts, and some users chose both. Eight of the participants (27%) only selected that they would consider using it for some of their accounts (one user also selected that they would use it for some of their accounts). None of the users answered that they would not use this method.

In order to better understand user's opinions about how easy the system was to use, we asked them "How easy was it for you to use this system?". Users were able to provide more than one answer to this question. Table 2 shows that 67% of the participants reported that they could easily use this method every day. All users reported that they could easily use the system either weekly, daily, and/or if it were more secure than regular passwords. No users found it too difficult, but 10% found it too time-consuming. As we discuss in Section 7, there may be ways to improve the interface to reduce login times.

Response	% users
I could easily use this method every day.	67% (20/30)
I could easily use this method every week.	30% (9/30)
I found this method too time-consuming.	10% (3/30)
I would use this system for some of my accounts if I knew it was more secure than a regular password.	37% (11/30)
I found this method difficult to use.	0% (0/30)

Table 2: Percentage of responses to post-questionnaire question "How easy was it for you to use this system?". Note that users could select more than one of these options.

In the users' comments at the end of the study, many expressed interest in the system, and positive sentiment saying e.g. that the system was "cool" or "neat", and some even inquired about using it in the future on campus systems.

4.3 Navigation Strategies

Most users followed the recommendation of using the search bar. We observed that the search bar is used during login by 28/35 (85%), 26/33 (79%), and 23/30 (77%) of total users in sessions 1, 2, and 3 respectively. The majority of the users (all users except for one) who searched in session 1 continued to use the search feature in subsequent sessions. We further observed that in the location-password creation phase, 16 users searched for a point of interest, 1 user searched for a postal code (and then panned from there to select another location), 1 user searched for a street, 11 users searched for a city/town, and 6 users did not use the search bar at all. This suggests that users can employ different types of initial information to start navigating through maps to choose their location-passwords.

We further examined the relationship between the term used in the search bar and login time. It turns out that there is no clear relationship between the time and whether the search term was more specific (e.g., a point of interest, street, or postal code) or a city/town. There does however appear to be a relationship between the number of times the user drags (or uses the pan controls) and the time to login. Given the results in Figure 5, it might be worthwhile to suggest to users once the number of drags is e.g., greater than 10 that they zoom back out to find their location.

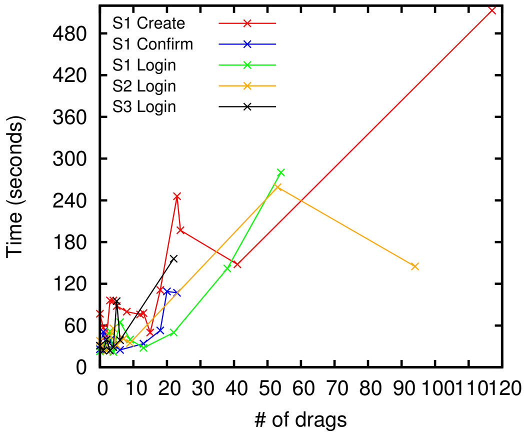


Figure 5: Average login time vs. number of drags, for each phase (create, confirm, and all three login phases). The data points shown are for all successful logins.

4.4 Qualitative Observations

Through observing the users in our study and their free-form comments provided at the end, we gained some useful insights: some users are open to suggested places offered by the search bar, e.g., they begin searching for one term and then select something that was not what they were looking for from the drop-down menu. This suggests that users may be open to suggestions or recommendations of places to choose during password creation, which could increase the effective security offered by GeoPass. We also observed that some users struggle with map navigation and might benefit from additional guidance. We observed navigation strategies (i.e., dragging and panning) that are more likely to result in failed navigation and longer login times which we explained further in Section 4.3. We can also use this information to help improve further versions of GeoPass.

The interface could likely be simplified by removing some features that were rarely used. We did not observe any participants using the "drag-zoom" feature for fast zooming, and we we only observed one user making use of satellite view rather than the default map view.

Users writing information about their location-password down and/or referring to the use of a written hint was something we specifically watched for in our user study. We did not say anything to the participants about writing their location-password down, and we wanted to see whether any naturally would use a written hint. We did not observe any users writing down information about their location-passwords. However, there was a single user who referred to a written search term in Session 3, not because the user forgot the location, but because of an unexpected side effect of one of the Google Maps API's features. This user recalled the location-password, but was left-clicking to set the "X" marker (instead of right-clicking); when left-clicking on an area that is known by Google Maps as a point of interest, an information box pops up, which the user perceived as feedback the location-password was entered. After 3 failed login attempts, the user stated they were sure this was the correct location, and that they would check with their smart phone to make sure. We allowed the user to proceed and try re-entering after consulting their written search term, observed one more failed login attempt, then we explained that the marker is set by right-clicking, after which the user was immediately able to login. Each of this user's left clicks were on the correct location. We will try to disable this Google Maps feature in future versions of GeoPass.

5. SECURITY

To analyze the security of GeoPass, we first describe the locations that users chose in Section 5.1. Next, we analyze the efficacy of different adversaries who guess location-passwords of users based on the information they know about the target user or system in Section 5.2. We discuss the user's reported perceived security of GeoPass in Section 5.3 and other security threats in Section 5.4.

5.1 Characterizing User Choice

To measure the actual security of location-passwords, we must determine whether there exist patterns in user choice that might allow an adversary (unknown to the user, or someone who the user may know) to guess the user's secret location. To determine this, we plot the locations that our participants selected to determine geographic patterns (see Figure 6), and ask the users questions in our post-questionnaire to characterize their choices.

Figure 6 indicates that location-password distribution is fairly well spread-out. No two users chose the same location. In general, the more populated areas of the Northern Hemisphere appear to be more popular. Two users chose places near New York City and eight users chose places in southern Ontario. The heatmap on Figure 6 indicates the popularity of our participants visiting, living, or working in those locations. Notice in Figure 6 that there are only a few users who chose their location-password in a place that no other user has been near before; however, there are many places that users have been that were not chosen as a location-password.

We asked participants to further characterize the locations they chose in the post-questionnaire by selecting what best described that location. We allowed participants to select none, one, or some of the responses presented in Table 3. The results indicate that all users followed our recommendation of avoiding a place they lived or worked, and the most popular category was a place the participants had visited.

To further categorize the participant's location-passwords, we asked them whether the place had any personal memory or attachment; approximately 47% ($\frac{14}{30}$) of users reported yes. Further free-form comments on the significance indicated that for most users, their location-password was a place they have been before, but not a place they have been very often. Three users indicated that the selected location is of particular importance, and two mentioned places that their ancestors had lived.

To estimate how many users may have been cued by the map itself, we asked whether it was the first place they

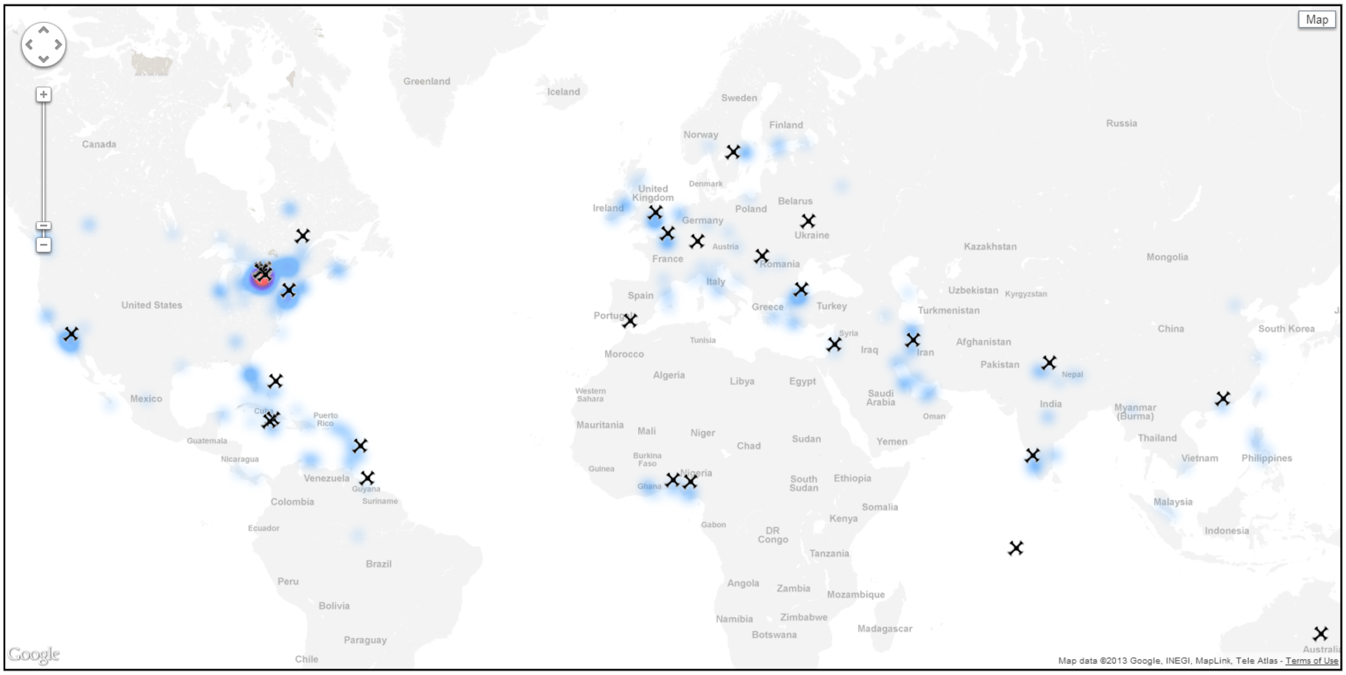


Figure 6: Visualization plotting the location-passwords that participants chose in the GeoPass system. The "X" markers indicating user-chosen location-passwords are shown at zoom level two in order to view them all simultaneously. The underlying heat map (best viewed in color) indicates places where participants self-reported they had vacationed to, worked, and/or lived.

Response	% users
A place I have visited.	47% (14/30)
A place I want to visit.	17% (5/30)
A place that might be known by someone close to me or someone who knows me very well.	27% (8/30)
My place of birth.	3% (1/30)
A historical place.	7% (2/30)
My favourite place.	7% (2/30)
My home (or a previous home).	0% (0/30)
My workplace (or a previous workplace).	0% (0/30)
Place with a great amount of significance in my life.	17% (5/30)
An unusual place that only I know the location of.	23% (7/30)
None.	0% (0/30)

Table 3: Participant's self-reported description of the location they chose (and the percentage who reported each). Note that users could select more than one of these options.

thought of when looking at the map. Approximately 40% ($\frac{12}{30}$) of users answered yes to this question.

Surprisingly, some users changed their initial choice as they interacted with the system, e.g., by using a search term that was suggested by the search bar, but was not what they intended to search for. In future research, we plan to investigate whether location-passwords that were influenced by the system are stronger and as memorable as location-passwords that were placed in user's initially intended locations.

5.2 Security Analysis

While we could simply analyze the theoretical security of GeoPass by calculating the total number of 21 × 21 pixel areas at zoom level 16 on the entire world, it would be prudent to assume that the effective security is less (as with text passwords [6]) from some regions/areas having higher probability of being chosen by users. Thus, to evaluate the security provided by GeoPass, we consider the threat model of an adversary who wishes to guess a target user's location-password in an online attack. We consider variations of this threat model based on what information the adversary has; each variation assumes the adversary will guess different regions based on different information about the target user:

1. **Unknown adversary**, i.e., the adversary does not have any information about the target user.

2. **Known adversary**, i.e., the adversary knows information about the target user (e.g., successfully gleans information through social engineering, or knows the target user).

3. **Local knowledge adversary**, i.e., the adversary knows the location of a target institution which has deployed GeoPass as its authentication scheme (e.g., the university of our study participants), and the institution has only a single location. The adversary assumes that the target system's users are likely to select the area surrounding this institution.

For each threat model, we create a high and low estimate of the security that GeoPass would offer. We assume that the adversary is aware of the 21 × 21 pixel tolerance error at zoom level 16 and can leverage this information for mounting an efficient guessing attack. The *high estimate* is based on the adversary guessing every possible 21 × 21 pixel area at zoom level 16 within a specific region (the region is based upon the threat model). The *low estimate* is based on the assumption that users may be more inclined to choose landmarks or well-known places. We estimate the number of *well-known places and landmarks* using the places (restaurants, things to do, hotels, and inns) listed for each region according to tripadvisor [38]. The results of these estimates are provided in Table 4, and further details of how these estimates were calculated for each threat model is provided in the following sections.

5.2.1 Unknown Adversary

We estimated the success of an unknown adversary by considering all land mass (i.e., no water is included) in the entire world. Thus, the high estimate represents the number of guesses for the adversary to enumerate all possible 21×21 areas (at zoom level 16) that would cover land regions. This is computed using our system to calculate the average number of 21×21 areas at zoom level 16 per square kilometer, and then multiplying that by the number of square kilometers of land in the entire world [28] (since it seems unlikely that users would choose locations in the ocean). The low estimate was obtained by collecting the well-known places/landmarks (as defined above) for each continent, summing these values, and multiplying by 10. We multiplied by 10 to estimate the number of places that a location-password could be chosen for these well-known places, since most are parks, malls, and other landmarks with many possible choices for placing a marker (e.g., if there was one possibility on each corner, one on each wall, one in the center, and another on its label, there are 10 distinct locations).

5.2.2 Known Adversary

We were able to estimate the security provided against a known adversary by asking users to list places lived and vacationed to in the background questionnaire. If the user chose his or her location-password in a city they reportedly lived or vacationed to, for the high estimate we report it as guessed and for the low estimate we report it as guessed if it is additionally on a well-known place as described further above.

The estimates for the number of attacker guesses are based on the assumption that the user has the average number of places lived and the average number of places vacationed to as determined by the questionnaires. For our participants, the average number of places lived was 3, and the average number of places vacationed to was 9. The high estimate number of attacker guesses is based on the adversary guessing all of the possible 21×21 areas (at zoom level 16) within each of the top nine vacation destinations [10], plus three regions that are approximately the size of the Greater Toronto Area (GTA) [9]. We chose to use the GTA as it represents the most popular region chosen by our participants. The low estimate for the number of attacker guesses is based on the adversary guessing all well-known places in each of the top 9 vacation destinations and all well-known places in the GTA (multiplied by 3).

5.2.3 Local Knowledge Adversary

This threat model assumes that the adversary knows that the target system is hosted in a certain location, so its users are likely familiar with the surrounding area, and thus would be more likely to choose their location-passwords nearby. For example, if the adversary were to attack UOIT, he or she may guess locations in the area of the GTA. The high estimate is thus all possible 21×21 areas (at zoom level 16) within the GTA [9], and the low estimate is all of the well-known places within the GTA.

5.2.4 Summary

Table 4 shows high and low estimates under the different threat models. The results in Table 4 show that the passwords created in GeoPass, under all threat models, would be strong enough to withstand an online attack, where the system is able to detect and stop or throttle the attack after a fixed number of failed login attempts. The most efficient attack was produced when the adversary has local knowledge. Even though this guessed 11% of location-passwords, it was in $2^{16.36}$ guessing attempts, which is still enough security to withstand an online attack.

To help put these security estimates in context, in Table 5 we compare our worst-case scenario attack on location-passwords to recent attacks against text passwords [6]. The results suggest that location-passwords might prove to have similar strength against online attacks as text passwords; however, we caution that the distribution of location-passwords must be studied further to evaluate whether there may be other unidentified security-reducing patterns. Our sample size was only 35 participants, so it is not possible to conclude with certainty.

Attacker success rate	# attacker guesses required for GeoPass	# attacker guesses required for text passwords
11%	$2^{16.36}$	2^{10} to 2^{14}*

Table 5: Security comparison between traditional text passwords and location-passwords. The number of attacker guesses required indicates the workload of an attacker to guess approximately 11% of passwords. * Depending on target population [6].

5.3 Perceived Security

The perceived security of the GeoPass system was very high; 93% of respondents reported that they believed this method would make their accounts more secure. As it is unclear how well users would distinguish the security against unknown adversaries and various types of known adversaries, we also ask them to assign a score of 1 (hard) to 10 (easy) for the following people to guess their location-password and for them to guess the location-password of those same people. The results are reported in Figures 7 and 8.

It is interesting to compare Figures 8 and 7. In general, it appears that people think that their family members and best friends are better at guessing their location-password than they would be at guessing the location-passwords of these same people. This asymmetry makes us wonder whether people might have a tendency to overestimate what others know about them and/or how well others can perceive their secrets.

5.4 Discussion of Other Security Threats

In its present form, GeoPass offers sufficient security against online guessing attacks (where the system stops or throttles the attack after a fixed number of failed login attempts), but not offline guessing attacks. There are of course other security threats besides traditional guessing attacks, which we discuss herein.

	High estimate (all possible, accounting for error tolerance)		**Low estimate (based on places of interest as per tripadvisor [38])**	
Guessing attack model	# of attacker guesses	# passwords guessed	# of attacker guesses	# passwords guessed
Unknown adversary (guesses all land surface area)	126200004576 ($2^{36.88}$)	35/35 (100%)	17658540 ($2^{24.07}$)	12/35 (34%)
Known adversary (guesses places lived and vacationed to)	21581077 ($2^{24.36}$)	23/35 (66%)	777880 ($2^{19.57}$)	6/35 (17%)
Local knowledge adversary (guesses Greater Toronto Area)	5998849 ($2^{22.52}$)	8/35 (23%)	84190 ($2^{16.36}$)	4/35 (11%)

Table 4: Security estimates based on guessing attacks under different threat models, including that of a known adversary (or social engineer) that knows where the target lives and has vacationed. We modelled the known adversary by asking users to list places lived and vacationed to in the background questionnaire.

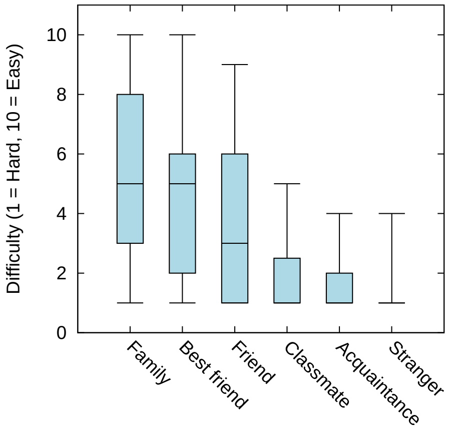


Figure 7: Users' responses to: "On a scale of 1 to 10 (1= hard, 10=easy), how easy do you think it would be for the following people to guess your location-passwords?". Some median bars and boxes do not appear for "Stranger", "Acquaintance", and "Classmate" because most users answered *1 (i.e., hard)*.

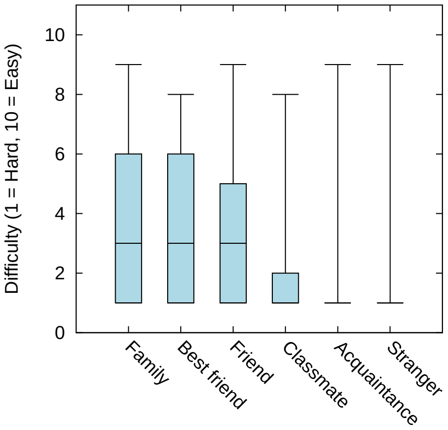


Figure 8: Users' responses to: "On a scale of 1 to 10 (1= hard, 10=easy), how easy do you think it would be for you to guess the location-passwords created by the following people?". Some median bars and boxes do not appear for "Stranger", "Acquaintance", and "Classmate" because most users answered *1 (i.e., hard)*.

5.4.1 Shoulder Surfing

As with many password schemes, shoulder surfing is a possible threat in GeoPass. Some technologies may help reduce the risk of shoulder surfing, e.g., the use of LCD screens with concurrent dual views, which show different images at different viewing angles [25] (e.g., when not positioned directly in front of the screen). Alternatively, users could interact with the system through eye gaze input (e.g., while using Google Glass [29]), which should reduce risk of shoulder surfing. Eye gaze has previously been used for inputting graphical passwords [18]. In the absence of such technologies, GeoPass seems most appropriate to use in environments where the risk of shoulder surfing is remote. For example, consider use cases in homes, single-user offices, or in mobile environments where users can reposition themselves.

5.4.2 Social Engineering

The "known adversary" threat model discussed in Section 5.2.2 models the threat of social engineering as it assumes that the adversary knows or has somehow discovered the cities the target user has lived in and travelled to. Our results in Table 4 estimate that the attack would require approximately 2^{20} guesses (if only landmarks are guessed, which is in the favor of the adversary), which offers protection against online attacks even when users choose such locations.

5.4.3 Writing Location-passwords Down

It may be easy to assume that users can more easily write their location-password down than in other forms of graphical password. For example, if users chose addresses, or very small points of interest, then it would be possible for users to completely describe their location-password in writing. However, our user study found that this is not normally the case. Normally, users use the search term to get closer to their final marker location, but we found that in session 1, 29/35 (or 82%) of users dragged or zoomed (even after searching) to navigate to their final location. Even for those users whose search terms brought them directly to the map in which their final marker was placed, they must choose a specific place on the map displayed to put their marker (of which there are many). For example, one of these users searched for a mall, but then placed the "X" marker in one particular corner of a store. Even if this user wrote his/her search term down and it were found by an adversary it would provide a hint, it would not reveal his/her entire location-password. As discussed in Section 4.2, only 46% of users searched for points of interest, but only 7/35 (or 20%) used search terms that could bring them to the same zoom level of the map where their final "X" marker is placed.

Finally, referring to a written aid was something we watched for in Sessions 1 and 3 of our user study. There was only one user who referred to a written search term (in Session 3)– although this user remembered their location, they were experiencing difficulty due to a system bug as discussed in Section 4.4.

6. RELATED WORK

The general idea of using digital map locations in passwords first appeared in news reporting a talk by Cheswick [19]. However, these articles did not describe an actual system design, nor any results from a user study. To the best of our knowledge, there are two other systems that use map locations as passwords: one by Spitzer et al. [34] and another called PassMap [35]. Spitzer et al.'s system asks users to zoom in five or seven zoom levels on a map of North America, and recall exactly where they clicked at each zoom level. Our GeoPass system design differs in the following ways: (i) GeoPass requires that users remember only one location and (ii) GeoPass allows more zooming methods than clicking on the map; it also provides a search bar and scroll wheel methods normally provided in digital map environments. Our GeoPass design differences appear to have made a positive impact on the system's usability; whereas in GeoPass 97% of users actually remembered their location-passwords after 1 week, in Spitzer et al.'s system, only 60% of users self-reported that their system was more memorable than text passwords. Also, the responses to how easy the system was to use were mixed. Unfortunately, Spitzer et al. do not report on any quantitative memorability results or other usability metrics. Although Spitzer et al.'s system [34] has stronger theoretical security (2^{40}) than GeoPass ($2^{36.9}$), due to their use of multiple locations, no studies or results are available regarding its security in practice. Thus, a comparison of its effective security vs. GeoPass's is not possible.

PassMap [35] asks users to choose two map locations as their location-password, whereas GeoPass only requires users remember one location. There are also many subtle differences relating to usability/security trade-offs between the GeoPass and PassMap designs, including: (1) GeoPass does not allow users to choose points at a zoom level lower than 16 for security reasons, whereas PassMap does not implement zoom level restrictions and thus users can choose points at lower (less secure) zoom levels (e.g., level 8). (2) GeoPass calculates the error tolerance at zoom level 16, whereas PassMap does not normalize error tolerance to a particular zoom level. We implemented this feature as we found that very few users remember their zoom level in our pilot testing. (3) GeoPass's initial screen is of the entire world to avoid influencing users to choose points in a certain geographic area (which would reduce security); PassMap's initial screen is centered on Taiwan at zoom level 8. (4) Upon a search, GeoPass zooms into the viewport assigned by the Google Maps API, whereas PassMap zooms into zoom level 18. The impact of this design choice is that when a user searches for something that has a large area (e.g., a city, or a large park), users would only see a selected portion of the entire place. This decision to influence users to choose points at zoom level 18 is theoretically good for security; however, in our pilot studies we found that if users chose rural areas, zoom level 18 did not provide enough detail, leading them to lose track of their location. Also, reported data for PassMap [35] indicates that users zoomed out (on average) 1-2 times more than they zoomed in, meaning that even if they did search and were brought to zoom level 18, many passwords could have been chosen at zoom level 16, 12, or even 8 (since the zoom function moved between zoom levels of 18, 16, 12, and 8). Although PassMap [35] has stronger theoretical security ($2^{83.1}$) than GeoPass ($2^{36.9}$), due to its use of multiple locations and assumption of both points being chosen at zoom level 18, no studies or results are available regarding its security in practice. Thus, a comparison of its effective security vs. GeoPass's is not possible.

The usability findings for PassMap showed that after one week, 23.46% of users failed to login on the first attempt (compared to 10% with GeoPass), and 7.41% of users failed to login after 6 attempts (compared to 3% with GeoPass after 5 attempts). A third recall test was performed with PassMap six weeks later, which found that 45.28% of users failed to login on the first attempt, and 18.87% of users failed to login after 6 attempts. In terms of login times, PassMap had a median login time of 33s on day one (compared to 25s for GeoPass), and 52s after one week (compared to 25s for GeoPass).

Our GeoPass study includes many more details that are not addressed by Spitzer et al. [34] nor PassMap [35], including: (1) the places that users chose, (2) the cities users lived in and/or vacationed to, (3) the resulting security impact considering (1) and (2), (4) user's perceived security, (5) user acceptance of GeoPass, (6) user's descriptions of their chosen locations, (7) the exact number of failed login attempts per session, (8) the number of password resets, and (9) the relationship between login times and navigation strategy. In general, our paper provides a much more detailed account of how map information can be useful and memorable in user authentication than other related studies.

Location-passwords can be viewed as a form of graphical passwords. In graphical passwords, the user's secret is a set of images, or parts of one or more images, instead of a word. The primary motivation of graphical passwords is earlier findings that people remember images better than words [27]. Many variations of graphical passwords exist in the literature that can be categorized by the type of memory they require from users to engage in the authentication task: pure recall, cued-recall, or recognition [4]. Here, we provide a brief summary of selected representative schemes from each of these categories, for the purpose of comparing them to location-passwords created with GeoPass. We use the graphical password categorization of Biddle et al. [4]: (pure) recall-based, recognition-based, and cued-recall. De Angeli et al. [1] called these categories by other names of drawmetric, cognometric, and locometric respectively. For a comprehensive review of graphical password schemes, see Biddle et al. [4].

6.1 Recognition-based

In Recognition-based schemes, the user is asked to recognize one or more images from a larger set. This category includes PassFaces [31, 8], which requires users to recognize a set of human faces from a larger set presented. Déjà Vu [15] requires the user to recognize a set of random art images from a larger set presented and Story [14] requires the user to recognize a set of images (of people, food, and objects) from a larger set presented. Marasim [24] is a system that involves elements of visual recognition; users must recognize images that represent tags, which the user gave to another more complex image they choose during password creation. Recognition-based schemes have been found to suffer from reduced memorability when users have multiple graphical passwords [17]; however it is worth noting that this effect has also been observed for other passwords [12], and may also exist for other schemes (including GeoPass) that have not yet been studied under multiple-password conditions.

In GeoPass, users must recognize that they have found the correct map at an acceptable zoom level (in which they must place their "X" marker). Additionally, users must recognize their search term from the drop down list, which normally involves them recalling and starting to type the search term, then before completely typing the search term, selecting the correct one from the drop-down list. Both of these tasks involve recognition, but in a different form than recognition-based graphical passwords.

6.2 Cued-recall

Cued-recall graphical passwords – occasionally called "click-based" graphical passwords – present the user with one or multiple background images, on which they click a sequence of points. One of the first such schemes was PassPoints [40], whereby the user was given a single background image and asked to recall a sequence of 5 selected points. Cued-recall graphical passwords have appeared commercially by PassLogix [30]. Other variants have been proposed such as PCCP [12], whereby the user clicks a point on each of a sequence of background images. Cued-recall graphical passwords have been found to have better resilience to multiple password interference than text passwords [12].

Location-passwords created with GeoPass can be considered a form of cued-recall graphical password, whereby the map cues the user. However, this may only happen at the final zoom level where the user selects the exact location of their "X" marker on the map. The user must first recall the general area of the map to begin the process of searching for and navigating to their marker location.

6.3 Pure Recall-based

Pure recall-based graphical password schemes generally involve the user re-creating an image by drawing; this drawing is his/her authentication secret. Thus, pure recall schemes are sometimes called drawing-based schemes. Examples of drawing-based graphical password schemes are Draw-A-Secret [23] and Pass-Go [36], which ask users to draw a password on a background grid. Another variation of this idea is Background Draw-A-Secret [16] which superimposes the grid over a background image. GridWord [3] is a related scheme which displays a grid to the user to select a few grid cells as their password (it also provides the option of entering a few text-based words if the user prefers). Other drawing-based password schemes include Android phones' password pattern [2], and a variation that has appeared as an option in Windows 8 [33], which is similar to Background Draw-A-Secret (BDAS) [16] in that it asks the user to draw on the background image. The latter two schemes also involve cued-recall, as the presentation of the background image can function as a cue to the user's memory.

Location-passwords do not involve elements of pure visual recall, but when created with GeoPass they do involve pure recall of the location the user selected (e.g., in order to begin their navigation by e.g., typing the search term in the search bar).

Overall, location-passwords created with GeoPass involve elements of recognition, cued-recall, and pure recall. Additionally, for the purpose of our study they involve a mnemonic association of a meaningful place for the user.

7. CONCLUDING REMARKS AND FUTURE WORK

We propose, implement, and evaluate an interface for map-based authentication called GeoPass that allows users to choose a place as their password (i.e., a location-password). Our evaluation was in the form of a user study with 35 participants to evaluate the usability, memorability, and security of this system. Our results demonstrate very strong memorability of location-passwords (over the span of 8-9 days). Although 67% of the users indicated that they could easily use the system every day, we must be cautious about recommending its use on frequently used accounts. Given that the login times for GeoPass are longer than traditional text passwords, we suggest that GeoPass would be most appropriate in contexts where logins occur infrequently. For example, it might be useful as an alternative to secondary authentication methods used for password resets, or for infrequently used online accounts.

Now that we have confirmed the strong memorability, reasonable usability, and security potential of GeoPass in a lab setting, we consider appropriate next steps. Future work includes evaluating GeoPass with larger and more diverse populations over longer time periods, and also evaluating the effects of interference with multiple location-passwords.

We also plan to investigate further security enhancements. We have a number of planned variations for the GeoPass system. The first variation involves a strategy that some users successfully utilized in our study to create a secure location-password: making use of a search box suggestion related to a place they remember. The second involves the user "tagging" their selected place with one or more words. We have reason to hope that these security enhancements will not have a negative impact on memorability; one graphical password study that used tagging actually found that it helped users remember their password when compared to another scheme that did not use tagging [24]. A third variation we plan to investigate involves randomization of the starting map. Usability of the system might also be enhanced by deploying recently developed and studied PolyZoom [22] to aid navigation on the digital map by allowing the user to create a hierarchy of focus regions.

8. ACKNOWLEDGMENTS

We thank the participants of our user study. We are grateful to Apu Kapadia, Stuart Schechter, and the anonymous reviewers for their insightful suggestions for improving this paper. This research was partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

9. REFERENCES

[1] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems. *International Journal of Human-Computer Studies*, 63(1-2):128–152, 2005.

[2] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive technologies*, WOOT'10, 2010.

[3] K. Bicakci and P.C. van Oorschot. A Multi-Word Password Proposal (gridWord) and Exploring Questions about Science in Security Research and Usable Security Evaluation. In *Proceedings of the New Security Paradigms Workshop (NSPW)*, 2011.

[4] R. Biddle, S. Chiasson, and P. C. Van Oorschot. Graphical Passwords: Learning from the First Twelve Years. *ACM Computing Surveys*, 44(4), 2012.

[5] J.C. Birget, D. Hong, and N. Memon. Robust Discretization, with an Application to Graphical Passwords. *IEEE Transactions on Information Forensics and Security*, 1:395–399, 2006.

[6] J. Bonneau. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *2012 IEEE Symposium on Security and Privacy*, 2012.

[7] J. Bonneau, M. Just, and G. Matthews. What's in a Name? Evaluating Statistical Attacks on Personal Knowledge Questions. In *Financial Cryptography and Data Security*. 2010.

[8] S. Brostoff and A. Sasse. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In *Proceedings of HCI 2000*, pages 405–424, 2000.

[9] Statistics Canada. Population and Dwelling Counts, For Canada, Provinces and Territories, and Census Divisions, 2006 and 2001 Censuses. `http://www12.statcan.ca/english/census06/data/popdwell/Table.cfm?T=702&PR=35&SR=1&S=3&O=D`, site accessed September 18, 2012.

[10] Travel Channel. Top 10 Vacation Spots. `http://www.travelchannel.com/interests/travel-tips/articles/top-10-vacation-spots`, site accessed March 2, 2013.

[11] S. Chiasson, J. Srinivasan, R. Biddle, and P. C. van Oorschot. Centered Discretization with Application to Graphical Passwords. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, UPSEC'08, 2008.

[12] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P.C. van Oorschot. Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism. *IEEE Transactions on Dependable and Secure Computing*, 9(2):222–235, 2011.

[13] S. Chiasson, P.C. van Oorschot, and R. Biddle. A Second Look at the Usability of Click-Based Graphical Passwords. In *SOUPS*, 2007.

[14] D. Davis, F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. In *USENIX Security*, 2004.

[15] R. Dhamija and A. Perrig. Déjà Vu: A User Study Using Images for Authentication. In *Proceedings of the 9th USENIX Security Symposium*, 2000.

[16] P. Dunphy and J. Yan. Do Background Images Improve Draw-A-Secret Graphical Passwords? In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS)*, 2007.

[17] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno. A Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, 2009.

[18] A. Forget, S. Chiasson, and R. Biddle. Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, 2010.

[19] S. Fox. Future Online Password Could be a Map, 2010. `http://www.livescience.com/8622-future-online-password-map.html`, site accessed March 2, 2013.

[20] E. Hayashi and J. Hong. A Diary Study of Password Usage in Daily Life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, 2011.

[21] P. G. Inglesant and M. A. Sasse. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, 2010.

[22] W. Javed, S. Ghani, and N. Elmqvist. Polyzoom: Multiscale and multifocus exploration in 2d visual spaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, 2012.

[23] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The Design and Analysis of Graphical Passwords. In *USENIX Security*, 1999.

[24] R. A. Khot, K. Srinathan, and P. Kumaraguru. MARASIM: A Novel Jigsaw Based Authentication Scheme Using Tagging. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, 2011.

[25] S. Kim, X. Cao, H. Zhang, and D. Tan. Enabling Concurrent Dual Views on Common LCD Screens. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, 2012.

[26] S. Madigan. Picture Memory. In J.C. Yuille, editor, *Imagery, Memory and Cognition*. Lawrence Erlbaum Assoc., 1983.

[27] D. Nelson, V. Reed, and J. Walling. Pictorial Superiority Effect. *Journal of Experimental Psychology: Human Learning and Memory*, 2(5):523–528, 1976.

[28] New World Encyclopedia contributors. List of Countries and Outlying Territories by Total Area, 2008. `http://www.newworldencyclopedia.org/p/index.php?title=List_of_countries_and_outlying_territories_by_total_area&oldid=866335`, site accessed March 2, 2013.

[29] S. Nichols. Google Patents Eye-Tracking for Google Glass, 2012. `http://www.techradar.com/news/portable-devices/google-patents-eye-tracking-for-google-glass-1091428`, site accessed March 8, 2013.

[30] Passlogix. `http://www.passlogix.com`, site accessed Feb. 2, 2007.

[31] Real User Corporation. About Passfaces. `http://www.realuser.com`, site accessed April 2012.

[32] S. Schechter, A. J. B. Brush, and S. Egelman. It's No Secret. Measuring the Security and Reliability of Authentication via "Secret" Questions. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, 2009.

[33] S. Sinofsky. Signing in With a Picture Password, 2011. `http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx`, accessed April 2012.

[34] J. Spitzer, C. Singh, and D. Schweitzer. A Security Class Project in Graphical Passwords. *Journal of Computing Sciences in Colleges*, 26(2):7–13, 2010.

[35] H. Sun, Y. Chen, C. Fang, and S. Chang. PassMap: A Map Based Graphical-Password Authentication System. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2012.

[36] H. Tao and C. Adams. Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. *International Journal of Network Security*, 2(7):273–292, 2008.

[37] J. Thorpe and P. C. van Oorschot. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. In *USENIX Security*, 2007.

[38] Tripadvisor. `http://www.tripadvisor.com`, site accessed August 22, 2012.

[39] M. Weir, S. Aggarwal, M. Collins, and H. Stern. Testing Metrics for Password Creation Policies by Attacking Large

Sets of Revealed Passwords. In *Proceedings of the 17th ACM conference on Computer and Communications Security*, CCS '10, 2010.

[40] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. *Int. J. Hum.-Comput. Stud.*, 63(1-2):102–127, 2005.

[41] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password Memorability and Security: Empirical Results. *IEEE Security and Privacy*, 2(5):25–31, 2004.