An Exploration of Geographic Authentication Schemes

Brent MacRae, Amirali Salehi-Abari, and Julie Thorpe

***Abstract*—We design and explore the usability and security of two geographic authentication schemes: GeoPass and GeoPassNotes. GeoPass requires users to choose a place on a digital map to authenticate with (a *location password*). GeoPassNotes—an extension of GeoPass—requires users to annotate their location password with a sequence of words that they can associate with the location (an *annotated location password*). In GeoPassNotes, users are authenticated by correctly entering both a location and an annotation. We conducted user studies to test the usability and assess the security of location passwords and annotated location passwords. The results indicate that both variants are highly memorable, and that annotated location passwords may be more advantageous than location passwords alone due to their increased security and the minimal usability impact introduced by the annotation.**

***Index Terms*—Security, Authentication, Usability, Passwords, Location passwords, Digital maps.**

I. Introduction

PASSWORDS have well-known problems relating to their memorability and vulnerability to being easily guessed by an adversary [1]. The security problems with passwords appear to be even worse than previously believed [2], [3]. To ensure security requirements are met, unusable password policies are implemented that cause an increasing burden on users [4]. When passwords are forgotten, many systems rely on secondary authentication such as challenge (or "personal knowledge") questions for resetting his or her password. Unfortunately, such methods also appear to offer questionable security [5], [6]. These issues motivate new user authentication strategies that have improved memorability and security.

People generally have better memory for images over words [7]; this has motivated many graphical password schemes that involve users remembering images (or parts of images) instead of words [8]. We hypothesize that location passwords should be highly memorable under an appropriate system design; after all, map locations are visual, and represent places (which may be more "concrete", and easier to remember [9]). A challenge that we tackle is designing location password interfaces that are memorable and provide security against guessing attacks.

We design and explore the usability and security of two geographic authentication schemes: GeoPass—first proposed and analyzed in the preliminary version [10] of this work—and GeoPassNotes, which is proposed and analyzed for the first time in this paper. We first develop a map-based user authentication system we call GeoPass [10], in which a user chooses a single place on a digital map as their password. We perform a multi-session in-lab/at-home user study of GeoPass involving 35 users over 8-9 days. Our results suggest that GeoPass is highly memorable: none of the returning participants forgot their location passwords after one day. Of the 30 participants who returned to login one week later, only one participant failed to enter their password. There were very few failed login attempts throughout the entire study. Our security results suggest that GeoPass provides enough security to protect against online attacks under simple system-enforced policies. GeoPass may also be useful as a building block for future geographic authentication systems.

However, GeoPass is certainly vulnerable to offline guessing attacks. Additionally, GeoPass may offer weak security against online guessing attacks in some circumstances (e.g., if it is deployed in a small city or if the adversary had a method of effectively prioritizing guesses). Thus, prudent implementations of GeoPass should find another way to increase security.

Through our GeoPass user study, we found that many users chose places where they participated in a special event or had a memorable experience (e.g., where they kissed their significant other for the first time). This lead us to hypothesize that a natural extension may be to incorporate other event-related information with the location password. Event-specific information, such as the "what" and "who" of events (which tend to be recalled along with the "where" [11]), could be expressed in the form of a *note* or *annotation* (i.e., a word or sequence of words). The annotation was chosen as it is an easily associable piece of information to the location password. It can be viewed differently than a password, since it is a text string without limits on length or character types as a traditional password typically is.

Therefore, we aim to enhance the security of location passwords by asking users to choose a note they can associate with their chosen location; we call this combination of the location password and its note an *annotated location password*. Users are authenticated by correctly entering both a location and an annotation. In essence, an annotated location password is using the location component to cue a user's memory for text information; however, both components (location and text) are used together for stronger authentication. GeoPassNotes is our implementation of an annotated location password system.

The addition of the annotation is simple but purposeful; it should increase resistance to both online and offline attacks,

B. MacRae and J. Thorpe are with the Faculty of Business and IT, University of Ontario Institute of Technology, Oshawa, Ontario, Canada e-mail:brent.macrae@uoit.ca, julie.thorpe@uoit.ca

A. Salehi Abari is with the Department of Computer Science, University of Toronto, Toronto, Ontario, Canada. email: abari@cs.toronto.edu

observation attacks (shoulder surfing), and attacks by third party map providers. However, without a study and analysis, it is not clear that GeoPassNotes would remain memorable and actually offer stronger security; for example, users may choose annotations that have an easily guessable relationship to their locations, or users might have difficulty recalling their annotations. Thus, in the present work, we study annotations to evaluate the security and usability impact of adding this easily associable piece of information to the location password.

We evaluate the security and usability of GeoPassNotes through a user study with 30 participants over 8-9 days to allow comparison to GeoPass. Our analyses suggest that annotated location passwords are more secure than and as memorable as regular location passwords (100% recall after one week). Our security analyses suggest that GeoPassNotes is resistant to online attacks (even without any system-enforced policies) and to offline attack (with system-enforced policies). Also, our security analysis for GeoPassNotes suggests it may offer stronger protection than text passwords against offline attacks. However, these security results should only be viewed as indications of promise for these systems, rather than definitive security results, as our study sample sizes are 35 and 30 for GeoPass and GeoPassNotes respectively.

Given that we found the median login times for GeoPass and GeoPassNotes are 25-30 and 33-36 seconds respectively, we suggest these schemes are most appropriate for accounts with infrequent logins (e.g., once per week). It may also be useful for fallback authentication as discussed in Section VII-D.

Our contributions are as follows: (1) We propose two novel user authentication schemes called GeoPass and GeoPassNotes. (2) We design, implement, and pilot test these systems to refine their interfaces. (3) We measure their usability through two separate user studies. (4) We design adversary models and attacker strategies to allow estimation of the security these systems offer when considering patterns in user choice. (5) We compute the first, and to our knowledge only to date, estimates of the effective security provided by geographic authentication systems, using our adversary models and the user study data collected. (6) We perform the first analysis of user's navigation patterns to better understand how they may be used to improve future geographic authentication schemes.

Based on our analyses, we recommend security policies and use cases for these geographic authentication systems. Our results suggest that map-based authentication schemes are a highly memorable way to authenticate, and that GeoPassNotes might be more desirable for higher-security environments as the annotation increases resistance to guessing attacks, observation attacks, and attacks by third party map providers.

II. Related Work

The idea of authenticating using a digital map was first introduced by Cheswick [12]. Since then, a few digital map-based authentication schemes have been developed and tested.

Spitzer et al.'s [13] system first asks a user to select one box of a grid placed over a digital map. Once the user selects a box, the map is automatically zoomed into it. The user then repeats this process using this new view 5 or 7 times to form a password. Users must remember every box clicked in order to successfully login. The system's initial view starts at a zoomed in map of the USA. A survey was reported of 50 students who used the system for an undisclosed period of time. No security analysis of user choice on the system was reported, nor usability metrics such as resets, failed logins, or login time.

PassMap [14] is a location password system that GeoPass differs from in various ways. First, PassMap asks users to login using two locations chosen on a digital map as opposed to one location in GeoPass. Second, PassMap's initial view starts at an already zoomed in map of Taiwan whereas GeoPass's starts at a view of the entire world to avoid influencing the user. Third, PassMap does not appear to enforce any particular zoom level requirements or compute error tolerance at a specific level; GeoPass enforces that locations be set at (minimum) zoom level 16 and error tolerance is calculated at that level to avoid usability problems. A user study of 27 participants was reported for PassMap, indicating that after one week, 77% were able to login on the first attempt (93% within 6). No security analysis of user choice on the system was reported.

In a preliminary version of the present work, Thorpe et al. [10] report on the GeoPass system, which asks users to zoom in to a digital map and select a single location to be used as their password. GeoPass enforces certain zoom levels and error tolerances to balance security and usability. It also does not require that users zoom in the same way every time to get to their location, unlike Spitzer et al.'s system. Finally, to avoid bias towards a specific map region, GeoPass starts with a zoomed out view of the whole world.

SmartPass [15] is a location password system with a similar design to GeoPass that was implemented for mobile phones. In a study with 20 users, and login tests on days 1, 2, 3, 4, 7, and 31, they found that in all sessions, all users were able to recall their location password within 3 login attempts. Login times were however still high, with an average of 30-35 seconds depending on the day.

Al-Ameen et al. [16], [17] recently ran a 66-day long field study [16] with GeoPass, finding a 96.1% login success rate and that 100% of participants logged in successfully within five attempts on average. They also conducted two separate three week long studies [17] to test the interference of multiple location passwords (4 per user) for both the GeoPass scheme and GeoPass with modified instructions. The modified instructions were to ask users to make a meaningful association between their location password and corresponding account. Their results indicate that in the absence of mental associations, GeoPass suffers from interference effects of multiple location passwords; however, by leveraging mental associations, the login success rates were 98% after one week.

RouteMap [18] is a system that requires a user to click a sequence of locations on a map, which displays a "route". This sequence of locations becomes the users password. The multiple password memorability of RouteMap was compared to GeoPass by asking 30 participants to create passwords for 5 accounts on each system (i.e., each user had 10 passwords total). After 3 weeks, the participants were invited to login again; after 3 attempts, 88.7% and 94% of participants successfully

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2570681, IEEE Transactions on Information Forensics and Security

logged into GeoPass and RouteMap respectively. Login times and security analyses were not reported for RouteMap.

Fallback authentication using location-based security questions has recently been studied [19], where a user is asked a security question to which a location is the answer. The map input interface studied had some design choices inspired by GeoPass. The method was found to have good accuracy: 95% after 4 weeks and 92% after 6 months. The information leaked by the security questions was measured through asking both strangers and known adversaries to guess users' locations given the corresponding question.

Renaud et al. [20] compare how users responded to traditional text challenge questions and picture-based challenges for both name-based and location-based questions. The location-based questions were often answered incorrectly in both cases, apparently due to the fact that users were required to enter a text city and country name, which lead to inexact inputs by users (the example the authors give is "Glasgow, Scotland" vs. "Glasgow, UK"). In GeoPass, users may input text in the search bar, but if the text is incorrect, they will receive instant feedback as the map they are shown would be different than what they intended to search for. Also, when users input text into the search bar, they are presented with a drop-down list from which they select their intended search term. While entering a location password in GeoPass is more time consuming than typing a text name, its design aids the usability of correctly entering accurate locations.

Authentication through a digital map can be seen as a type of graphical password. An overview of graphical passwords is out of the scope of this paper; see a survey [8] for a comprehensive overview. As GeoPassNotes can also be seen as a hybrid graphical-text scheme, we review related literature on such hybrids below.

Marasim [21] is a graphical-text hybrid authentication scheme. During enrollment, the user creates tags for a personal image of their choice. Using the tags created, four random images are found on Google. The four random tag-related images are then mixed with 4 decoy images and the user is asked to correctly identify the four images related to their tags.

GridWord [22] is a hybrid scheme as well. During enrollment, the user selects a set of three words. The system stores a one-to-one mapping of words to cells on a 2D grid. The user can then enter their password by selecting the three grid cells or selecting the three words from drop-down menus.

Inkblot authentication [23] is another hybrid scheme that is based on cueing users with a set of inkblot images. During enrollment, the user is asked to create a tag for each inkblot, and then type the first and last letters of the tag. For example, a set of 10 inkblot cues produces a 20-character password.

Video-passwords [24] are a class of user authentication schemes that involve the user watching and remembering parts of a given video as his/her password. Some variants involve the user pausing the video at a certain time and inputting text.

These hybrid schemes, like GeoPassNotes, involve a graphical and associated text element. To the best of our knowledge, GeoPassNotes is the first hybrid system that uses digital maps for text-location associations.

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

III. System Design of GeoPass and GeoPassNotes

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 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 (see Figure 1). To login, the user must be able to place the "X" marker again near his/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.

A. User Interface Components

The user interface components of GeoPass support faster navigation on the digital map. The main components are the search bar, zooming options, panning options, and zoom level indicator (discussed below). At any time, the user can press a "Help" button for further instructions.

Search Bar: The search bar 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", which 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.

Zooming and Panning Options: We enabled the zooming and panning options of 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. Panning was enabled through (1) dragging the map, and (2) using the pan control in the upper left-hand corner.

Zoom Level Indicator: 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. 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2570681, IEEE Transactions on Information Forensics and Security

message bar is red until the user reaches zoom level 16, after which it turns blue. Right-clicking to place a marker is enabled once users reach zoom level 16. If 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.

B. 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 IV. These design choices differ from those in other documented map-based user authentication systems [14].

1) Zoom Level Requirements: Higher zoom levels have more map detail, which allows for higher security as more locations can be chosen as location passwords. On the other hand, the further a user is required to zoom in, the more time-consuming it is to create and login with their location password. We determined through pilot studies that when users zoom in further than zoom level 18, the amount of detail available on the map often decreases, and users have difficulty navigating the maps. 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 enough detail that users can choose a location password in most places, e.g., where streets and buildings can be seen. The zoom level indicator lets users know when they have reached zoom level 16.

2) Initial Zoom Level: GeoPass initially displays the map at zoom level 2 as shown in Figure 3 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. 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 VI-D, most users appear to avoid this by using the search bar.

3) Error Tolerance: For a successful login, a user must place the marker within a 21×21 pixel box centered 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. The 21×21 pixel box error tolerance setting is chosen from studies in click-based graphical passwords [8], [25]. It is possible to securely store this information and allow for error tolerance using discretization methods [26].

C. GeoPassNotes User Interface

GeoPassNotes is an extension of the GeoPass system. Users login by first selecting a location on the map as in GeoPass and then creating an annotation. For a login to be successful, both the same location (errors within 10 pixels at zoom level 16 are tolerated) and the same annotation must be re-entered. There are a few design differences from GeoPass due to the introduction of the annotations:

Fig. 2. Snapshot of the GeoPassNotes interface during note entry.

- *Note pop-up.* Once a user sets their 'X' marker, a box pops up to allow entering their annotation (see Figure 2). Users were instructed to "choose a word or sequence of words that they can associate with this place", and to avoid using the place's name. After typing the annotation, the user can press the "Enter" key or "Login" button to login. Like a regular password, the typed characters appear as circles. There are no restrictions on the annotation (e.g., it can be any length or use any character set).
- *Clickable 'X' marker.* To enable users to change the location entered before logging in, they can close the annotation popup and then move the 'X' marker by right-clicking elsewhere on the map. If they chose to keep the chosen location after closing the annotation pop-up, they could re-open the annotation pop-up by left-clicking on the 'X' marker.

IV. User Studies

We conduct preliminary pilot studies to examine GeoPass and GeoPassNotes for usability and other issues that could affect security. We iterated our prototype/pilot testing of the systems in order to eliminate obvious usability barriers in our implementation or missing instructions. For GeoPass, this was done with 3 colleagues and 4 casual computer users. This helped us refine our instructions, add user interface features such as the help menu and zoom error pop-up, and base the error tolerance on zoom level 16. GeoPassNotes was pilot tested with 3 experienced and 4 casual computer users.

Next we evaluated the security and usability of the systems by conducting two multi-session user studies. These studies involved university students who have not taken any courses in computer security or IT. Our participants were a diverse group, including majors in Nursing, Health Sciences, Engineering, Education, and Criminology. GeoPass's study had 35 subjects and GeoPassNotes's study had a different 30 subjects.

A. Sessions

The user studies were conducted over three sessions. In the GeoPassNotes study, all participants completed all sessions. In the GeoPass study, 33 and 30 participants returned to complete

sessions 2 and 3 respectively. For both studies, the sessions are arranged as follows:

- Session 1 (day 1, held in lab). Participants created and confirmed their passwords in a lab environment. After a successful confirmation, the user was distracted for 10-20 minutes with a background questionnaire. At the end of the session, they were asked to login.
- 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 [27].
- Session 3 (day 8 or 9, held in lab). Session three was arranged seven days after session two (day 9) if possible; for the GeoPass study, 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 [27]. Participants logged in with their password and completed a feedback questionnaire in a lab environment.

B. Participant Instructions

Each user was shown a demo video at the start of session 1 which explains the task of location password creation. 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 to be secure enough. The video hints 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 (and annotation for GeoPassNotes). The participants were recommended to avoid choosing a previous home or work address; this recommendation was given for security reasons. For GeoPassNotes, participants were instructed to "choose a word or sequence of words that they can associate with this place", and to avoid using the place's name.

C. Environment

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

D. Participants

We recruited two separate groups of participants from the UOIT campus by email and posters: 35 for GeoPass and 30 for GeoPassNotes. 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 was approved by UOIT's Research Ethics Board. All were university students pursuing a degree but did not have formal training in Computer Security to avoid participants who are more likely to have a heightened awareness of security. We collected information about our participants' background through the use of a questionnaire in Session 1. For all of our questions, participants were given the option to not answer.

1) GeoPass Study Demographics: Twenty-two (62.9%) of our participants were male, thirteen (37.1%) were female. 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. 71% felt that they could find any location on an electronic map in an acceptable amount of time. When asked whether they enjoy looking at maps, 71% answered yes and 29% answered no.

The participants in our study seemed to be quite 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.

2) GeoPassNotes Study Demographics: Nineteen (63.3%) of our participants were male, eleven (36.7%) were female. When asked how often they use a map, 50% answered "daily", 7% answered "once/week", 40% answered "less than once/week", and 3% did not answer. Only 47% felt that they could find any location on an electronic map in an acceptable amount of time. When asked whether they enjoy looking at maps, 60% answered positively and 7% answered negatively.

The participants generally seemed to be concerned about passwords: 20% reported being very concerned, 27% reported being concerned, 20% reported being a little bit concerned, 20% reported being indifferent, and 20% reported being not concerned, and 3% did not report their concern.

V. Security

The patterns found in user choice impact the security of GeoPass and GeoPassNotes. In Sections V-A and V-B we analyze the security of GeoPass and GeoPassNotes respectively. Section V-C discusses other security threats such as shoulder surfing and writing location passwords down. Finally, we compare the security of GeoPass and GeoPassNotes in Section V-E.

A. Security of Location Passwords

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 [3]) since some regions/areas have higher probability of being chosen by users. To inform our security analysis, we begin by characterizing user choices.

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. We first plot the locations that our participants selected to determine geographic patterns (see Figures 3 and 4).

Figure 3 and 4 indicate that the distribution of locations chosen is fairly well spread-out. No two users chose the same

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2570681, IEEE Transactions on Information Forensics and Security

Fig. 3. Heat map of the location passwords chosen for GeoPass.

Fig. 4. Heat map of the locations chosen for GeoPassNotes.

location. Even until zoom level 9, no two locations fell within the same 21×21 error tolerance of each other (and thus would not be considered the same location password at higher zoom levels). At zoom level 9 there is some overlap between the error tolerance boxes of one set of two location passwords. At zoom level 8, two sets of two location passwords overlap. In general, the more populated areas of the Northern Hemisphere appear to be more popular. The most popular area was Southern Ontario, where our participants' university is located.

In the questionnaire, we asked participants to characterize the locations they chose by selecting what best described it. We allowed participants to select none, one, or some of the responses presented in Table V-A1. The results indicate that 59/60 users from the studies 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; 47% (14/30) of users reported yes for the GeoPass study, and 43% (13/30) reported yes for GeoPassNotes. Further free-form comments indicated that for most of these users, their location password was a place they have been before, but not a place they have been very often.

2) Security Analysis: To evaluate the security provided by location passwords, we consider the threat model of an adversary who wishes to guess a target user's location password. 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:

Question	% GeoPass	% GeoPassNotes
A place I have visited.	47% (14/30)	50% (15/30)
A place I want to visit.	17% (5/30)	37% (11/30)
A place that might be known by someone close (or knows me well)	27% (8/30)	43%(13/30)
My place of birth.	3% (1/30)	3% (1/30)
A historical place.	7% (2/30)	7% (2/30)
My favourite place.	7% (2/30)	7% (2/30)
My home (or a previous home).	0% (0/30)	3% (1/30)
My workplace (or a previous workplace).	0% (0/30)	0% (0/30)
Place with a great amount of significance in my life.	17% (5/30)	27% (8/30)
An unusual place that only I know the location of.	23% (7/30)	23% (7/30)
A random location I chose*.	N/A	23% (7/30)
Other*.	N/A	17% (5/30)

TABLE I
PARTICIPANT'S DESCRIPTION OF CHOSEN LOCATIONS. USERS COULD SELECT MORE THAN ONE OPTION. *ONLY ASKED FOR GEOPASSNOTES

1) **Unknown adversary**, i.e., the adversary does not have any information about the target user or institution deploying the system.
2) **Known adversary**, i.e., the adversary knows information about the target user (through social engineering, or knows the target user).
3) **Local knowledge adversary**, i.e., the adversary knows the single location of a target institution which has deployed the system (e.g., our participant's university).

For each threat model, we create a high and low estimate of the security that location passwords 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). Thus, the high estimate is guessing all land mass for a given 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 *points of interest (POI)*, e.g., restaurants, things to do, hotels, and inns using those listed for each region according to tripadvisor [28]. The results of these estimates are provided in Table II, and further details of how these estimates were calculated for each threat model is provided in the following sections.

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 all land regions. This is computed by calculating 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 [29] (since it seems unlikely that users would choose locations in the ocean). The low estimate was obtained by summing up the number of POI (as defined above) for all continents and multiplying by 10. We multiplied by 10 to estimate the number of places that a location password could be chosen for each POI, since most are parks, malls, and other landmarks with many possible choices for placing

	All Land (High Estimate)			Points of Interest (Low Estimate)		
Guessing attack model	# of attacker guesses	# guessed (GeoPass)	# guessed (GeoPassNotes locations)	# of attacker guesses	# guessed (GeoPass)	# guessed (GeoPassNotes locations)
Unknown adversary	$2^{36.88}$	35/35 (100%)	30/30 (100%)	$2^{24.07}$	12/35 (34%)	4/30 (13.33%)
Known adversary	$2^{29.17}$	23/35 (66%)	17/30 (56.67%)	$2^{19.69}$	6/35 (17%)	3/30 (10%)
Local knowledge adversary	$2^{22.52}$	8/35 (23%)	7/30 (23.33%)	$2^{16.75}$	4/35 (11%)	2/30 (7%)

TABLE II
SECURITY ESTIMATES BASED ON GUESSING ATTACKS UNDER DIFFERENT THREAT MODELS.

a marker. More specifically, we consider one possibility on each corner, each wall, the center, and another on its label, thus resulting in 10 distinct locations.

Known Adversary: For the GeoPass study participants, we estimated 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 POI. For GeoPassNotes, this was estimated based on the users' responses to a question in the background questionnaire asking what the significance of their chosen location was. If their answer indicated they had been there before, we categorized the location as vulnerable to a known adversary.

To estimate the number of attacker guesses, the average number of places lived and vacationed to by participants were employed. For our GeoPass study 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 [30], plus three regions that are approximately the size of the Greater Toronto Area (GTA) [31]. 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 POI in each of the top 9 vacation destinations and all POI in the GTA (multiplied by 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 a GeoPass system at 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 [31], and the low estimate is all of the POI within the GTA.

3) Summary: Table II provides our all land and POI estimates under the different threat models. We include the results for the location component of GeoPassNotes in a separate column, to analyze whether the location component's security changes with the annotation extension. The only notable difference between locations chosen in each system is that points of interest were less popular in GeoPassNotes (see POI estimate, Unknown adversary). The results in Table II show that the location passwords created in GeoPass, under all threat models except the local knowledge adversary with POIs, would be strong enough to withstand an online attack [32], 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 (guessed 11% in $2^{16.75}$ guessing attempts). This attack could however be mitigated with a proactive check as discussed in Section VII-B.

To put GeoPass's security in context, we compare it with recent results from semantic guessing attacks on leaked passwords from Myspace and LinkedIn [2], which are also reported in Figure 5. GeoPass location passwords have similar guessing resistance to MySpace passwords; after approximately 2^{16}, 2^{20}, and 2^{29} attempts, approximately 11%, 22%, and 55%, of passwords were guessed respectively. However, LinkedIn passwords have stronger resistance to guessing than GeoPass location passwords; after approximately 2^{16}, 2^{20}, and 2^{29} attempts, approximately 1%, 3%, and 21% of passwords were guessed respectively.

B. Security of Annotated Location Passwords

The main motivation for the addition of notes to location passwords is to increase security. GeoPassNotes has at least the security of GeoPass since in an online attack, the attacker needs to first guess the location and then the associated note. In addition to user choice patterns for location passwords, annotated location passwords might exhibit some patterns between locations and notes, and among notes themselves, that can be exploited for mounting an efficient attack.

Our analysis primarily focuses on resistance to guessing attacks, a common threat model (distinct from shoulder surfing as discussed in Section V-C). It is natural to assume that there might be some association between the note and location components of the annotated location passwords. Thus, we begin our analysis by categorizing the notes collected from our study to observe their relationship to the location in Section V-B1. It also seems likely that there will be patterns in the notes users choose, thus we categorize the notes to determine common patterns in Section V-B2. As there were many notes that were "password-like" in that they contained special characters, numbers, etc., we ran popular password cracking programs against the notes to estimate their security and report their results in Section V-B3. We discuss attacker strategy in Section V-B4 and combine the security of the location component and the note component to get an overall estimated security of GeoPassNotes in Section V-B5.

1) Note-Location Relationship: We first analyze the relationships between notes and locations. Through a questionnaire, we asked participants why they chose their notes. Out of our 30 users, 24 users claimed their notes held significance to the location. Interestingly, even though the users saw a

relationship, it was difficult in most cases for us to see this relationship. We manually analyzed each location and note pair; the only relationship we could find was in 2 of the user's notes where they directly labelled their location. Direct location labels cause a strong correlation between notes and locations, which arguably provides the worst case for GeoPassNotes security. When a user labels a location, and the location is compromised, the note can easily be guessed by compiling a small dictionary of location-specific terms. When we noticed the first user of our study labelling the location, we decided to implement the "no labelling" recommendation for future users. In Section VII-B, we discuss how proactive checking by the system can be used to prevent direct labels.

2) Categorization of Patterns in Notes: To gain a better understanding of the types of notes users choose, we manually categorize them. We noticed that a few notes appeared to be names, and a significant number were simple words. Surprisingly, a fairly large number looked like a text password (containing mixed case, numbers, special characters, etc.). Based on these observations, we categorize notes based on whether they appear in the following lists:

- *COCA (all).* The Contemporary Corpus of American English (COCA) [33] contains 497,186 words and covers 12/30 (40%) of notes.
- *COCA (frequent).* This dictionary should capture the most common nouns, adjectives, and verbs in COCA [33]. As a vocabulary of 15851 words was found to cover 97.8% of the Brown Corpus [34], we consider this as a likely vocabulary size. We first select the 15851 most frequent words from COCA. Then we filter out the words that are neither nouns, adjectives, or verbs. This produces a list of 14674 words, covering 5/30 (17%) of notes.
- *Names.* Unique names of 82,386 babies born in the USA since 1960 [35], covering 3/30 (10%) of notes.
- *Low # characters.* All combinations of three or fewer lower-case characters, which covers 1/30 (3%) of notes.

In total, only 14/30 notes could be categorized (some fall in multiple categories). Manual analysis revealed that the other notes contained phrases, sequences of words, mangled words (containing digits), and even one user chose a random string. We used the categories above to guess notes, finding that this method was not as efficient as the password crackers in Section V-B3. Thus, we focus on the password cracking method to guess notes in the remainder of this paper.

3) Note Security: We estimate the security that annotations alone offer, under the assumption that an adversary cannot exploit a user's associations between an annotation and location. We later use these results in our analysis of the overall security of GeoPassNotes. We first found that most of the annotations had a password-like appearance, containing numbers, special characters, and sometimes multiple words. They had lengths similar to passwords (average length was 8.84 characters, and only 5/30 were longer than 12 characters). This motivates us to analyze the security gained by annotations by simulating a password cracking attack against them. We used three popular password crackers in our analysis:

- John the Ripper (JtR [36]), an open-source password cracker. JtR was configured to use a large dictionary [37].
- Probabilistic Context-Free Grammars (PCFG) [38], which generates a guessing order that JtR can use.
- Semantic Guesser [2], which generates guesses based on the semantic and grammar patterns of passwords.

JtR was configured to operate in wordlist mode using default word mangling rules. Once the wordlist had been exhausted we configured JtR to continue in incremental mode until 3 billion guesses. We trained PCFG on the RockYou dataset [39]. We configured PCFG to use the DIC-0294 wordlist and the Dazzlepod list [37] to generate guesses based on the trained grammar rules. The semantic guesser was trained using the RockYou dataset [39] and run with and without word mangling (which modifies capitalization on word boundaries). The semantic guesser (with mangling) correctly guessed 63% (19/30 notes), which outperformed PCFG and JtR; as such we only focus on it for the remainder of this analysis.

4) Attacker Strategy: To perform a reasonable security estimate, we must consider how an attacker would approach guessing an annotated location password. For optimal security, a GeoPassNotes system should hash the combination of location and note, and not provide any feedback to the user until both have been entered. The attacker must then correctly guess *both* the location and note without any feedback to indicate they have guessed the correct location.

A sensible approach for an attacker attempting to guess an annotated location password would be to guess the location component using the location dictionaries discussed in Section V-A, ordered based on their relative size and guessing efficiency, as follows: (1) POI–local, (2) All land–local, (3) POI–known, (4) All land–known, (5) POI–unknown, (6) All land–unknown. Of course, for each of the location guesses in this ordering, the attacker must guess the note as well. An attacker should choose a maximum number of annotation guesses to make per location (e.g., 3 billion), meaning that for each location guess, they would guess at most this maximum number of notes. For each failed location guess, they would need to guess exactly this maximum number of notes, even if one of the note guesses were correct (as it is the combination of location and note that form a password).

5) Security Analysis: For our security estimates of GeoPassNotes, we assume that the attacker uses the strategy described above. For our calculations, we assume the attacker's maximum number of annotation guesses is different for each note and set to the number of guesses required by semantic (with mangling) to guess that specific note. This essentially assumes the attacker knows exactly how many guesses to make for each note (but no more than necessary). By this assumption, we underestimate the security of GeoPassNotes. For example, if the target's note is the 3000th guess in the semantic attack's ordering, but the location is the 1,000,000th entry of the location dictionary ordering, the attacker would need to make $(10^6-1)\times(3\times10^9)+3000 \simeq 3\times10^{15}$ guesses. However, our estimates assume that the attacker would need to make $10^6 \times 3000 \simeq 3 \times 10^9$ guesses.

The estimates in Figure 5 represent the total estimated security for all of the annotated location passwords gathered in our study. The number of total guesses for an annotated location password is computed by multiplying the number of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2570681, IEEE Transactions on Information Forensics and Security

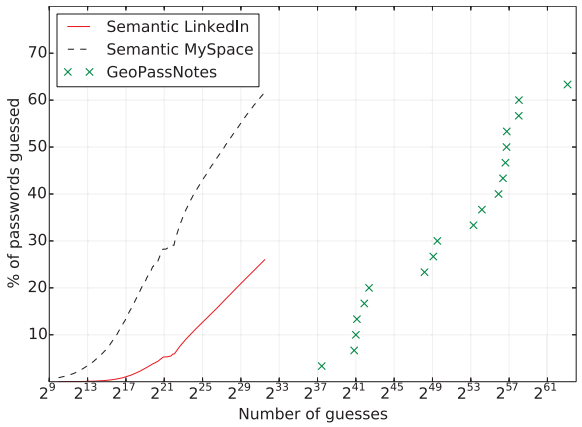

Fig. 5. Results of GeoPassNotes security estimate compared with the semantic (with mangling) attack against the MySpace and LinkedIn password sets. Note that we underestimate GeoPassNotes security as described in Section V-B5.

guesses required by semantic (with mangling) to guess the annotation with the sum of the sizes of all location password dictionaries exhausted and half of the size of the last dictionary used. We consider half of the last location dictionary as the annotated location password can be anywhere within it (as the entries within each are not ordered). For example, to guess an annotated location password whose location component exists in the All land-local dictionary, the dictionary size would be the size of the POI-local dictionary plus 50% of the size of the All land-local dictionary, times the number of the semantic attack's attempts to guess the corresponding note.

We compare our estimates for GeoPassNotes with the results of password guessing with semantic with mangling against the MySpace and LinkedIn leaked password sets. This will provide a baseline for the strength of text passwords in practice as compared to our conservative estimate of the security of GeoPassNotes. For the location passwords that would be guessed by each of the POI dictionaries, only 3 notes were guessed. The first POI annotated location password was not guessed until approximately 2^{37} guesses had been exhausted whereas $> 30\%$ of the MySpace passwords and $> 4\%$ of the LinkedIn passwords were correctly guessed within 2^{20} attempts.

The weakest two annotated location passwords are estimated to be guessed after 2^{41} guesses (these two fell into our POI dictionaries), which is still much better than the weakest passwords from both MySpace and LinkedIn data sets. A comparable number of the LinkedIn passwords are guessed within approximately 2^{23} guesses.

6) Trawling Attacks: The "unknown adversary" and "local knowledge adversary" methods can generate guesses to be used to attack all users (i.e., a trawling attack against multiple users).[1] Table II shows results for GeoPass with different attacks, including the unknown and local knowledge adversaries. The most efficient of these attacks (i.e., POI-local) shows that within $2^{16.75}$ (or approx. $110,000$) guesses, 11% of GeoPass accounts could be compromised in a trawling attack. For GeoPassNotes, our attacker strategy in Section V-B4 already starts with POI-local followed by All land-local, and the trawling attack would begin the same way. According to Figure 5, the weakest account would only be compromised after approx. 2^{37} guesses in a trawling attack.

[1]The attacks we discuss in Sections V-B4 and V-B5 also incorporate the "known adversary" method, which assumes the attack is built for a particular target user.

C. Discussion of Other Security Threats

In its present form, both GeoPass (with the policies discussed in VII-B) and GeoPassNotes appear to offer sufficient security against online guessing attacks (where the system stops or throttles the attack after a fixed number of failed login attempts). We discuss other security threats besides guessing attacks herein.

1) Shoulder Surfing: As with many password schemes, shoulder surfing is a possible threat in both GeoPass and GeoPassNotes. Recent work confirms that GeoPass is vulnerable to shoulder-surfing [16]. GeoPassNotes' annotation component offers some resistance as it should have similar vulnerability as a traditional text password (the typed characters appear as circles in the annotation input field). There are some technologies that 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 [40]. Alternatively, users could interact with the system through eye gaze input (e.g., while using Google Glass), which should reduce risk of shoulder surfing. Eye gaze has previously been used for inputting graphical passwords [41]. In the absence of such technologies, GeoPass and GeoPassNotes appear 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 (for GeoPass) in mobile environments where users can reposition themselves.

2) Social Engineering: The "known adversary" threat model discussed in Section V-A2 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 for GeoPass (in Table II) estimate that the attack would require approximately 2^{20} guesses (if only POIs are guessed, which is in the favor of the adversary). This offers protection against online attacks even when users choose such locations. Our results for GeoPassNotes indicate that for known adversaries, at least 2^{40} attempts would be required before before a successful guess is made.

3) Writing Down Location Password Information: It may be easy to assume that users can more easily write their (annotated) location password down than in other forms of graphical password. For example, consider if users chose addresses, or very small points of interest. However, our user study found that users usually can't describe their location by only a search term. This is because in the GeoPass study, only 7/35 (or 20%) used search terms that could bring them to zoom level 16 or higher; this value was similar for the GeoPassNotes study (5/30 or 17%). 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). Even if any of those users wrote their search terms down and were found by an adversary it would provide a hint, it would not reveal the entire location password.

We watched for users writing password information down in Sessions 1 and 3 of our user studies. We did not say anything to participants about writing anything down to see whether any would naturally do so. We did not observe any users writing anything down in the GeoPass study; however, there was a single user who referred to a written search term in Session 3, not because he/she forgot the location, but because of a glitch in the system (see Section VI-A1). In the GeoPassNotes study, we noticed two users writing down part or all of their annotated location passwords in session 1 (but none referring to them in session 3). In the questionnaire, 4/30 (13%) of users said they wrote part of it down.

4) Third Party Map Providers: In our implementation, which uses Google Maps, Google is capable of knowing the location password portion of the system. It is also conceivable that the traffic to Google could be analyzed by an adversary to narrow down which map was downloaded (e.g., based on packet size); however, Google's Map API can be linked to using SSL so such analyses would not be trivial if at all possible. These issues highlight an additional advantage of GeoPassNotes: the annotation does not require transmission to a third party server and thus offers protection against these issues.

D. Limitations

To analyze the security of notes, we performed a manual analysis, category-based analysis, and password cracking analysis of the notes. The best password cracking program results indicate that many of the notes are similar in strength to weak passwords, but of course it is always possible that a better (yet unknown) annotation guessing method exists. To determine this, we would need a significant amount of data (e.g., on the order of millions) to train an advanced guessing attack, which is not feasible given that investigations into geographic authentication systems have only just begun.

E. Security Comparison

Theoretically, the security of GeoPass is approximately 2^{37}, as measured through the high estimate for the unknown adversary attack (i.e., the total number of locations that could be chosen on the Earth's land mass). The theoretical security of GeoPassNotes can be computed by multiplying this value by the total number of notes that are possible. Assuming the maximum length for an annotation is 8 text characters, the theoretical security of GeoPassNotes is approximately 2^{90}.

However, the number of attempts estimated to guess the weakest 10% is approximately 2^{17} for GeoPass and 2^{41} for GeoPassNotes. Simple policies (discussed in VII-B) would prevent the most successful attack on locations and increase the security accordingly. In the absence of such policies, GeoPassNotes would still be considered secure against online attack under the criteria that passwords cannot be guessed within 2^{20} guesses [32]. Under the criteria that systems are considered resistant to offline attack if they require at least 2^{47} attempts [32], our estimates indicate that more than 80% of GeoPassNotes should be resistant to offline attack. All of the GeoPassNotes that are estimated to be guessed before 2^{47} guesses were guessed through the local adversary attack, which means a simple proactive check (to prevent locations in the system's or user's city from being chosen) may make the system resistant to offline attacks. GeoPassNotes' security estimates suggest it could offer stronger security against offline attack than text passwords, where within 2^{31} guesses over 60% of MySpace and 25% of LinkedIn passwords were guessed. However, these security results should only be viewed as indications of promise for GeoPass and GeoPassNotes, rather than definitive security results, as our study sample sizes are 35 and 30 for GeoPass and GeoPassNotes respectively. It is possible that with a larger dataset some exploitable patterns emerge that could not be detected with the data collected in these studies.

	Session 1	Session 2	Session 3
# failed login attempts	1,1,2,4	1,1	1,4,6

TABLE III
GEOPASS FAILED LOGINS FOR EACH SESSION. EACH NUMBER REPRESENTS A SINGLE USER'S # OF FAILED LOGIN ATTEMPTS.

For annotations in GeoPassNotes, we found patterns in user choice that appear to be similar to relatively weak passwords. The good news is that the annotation is not used in isolation, but is part of the annotated location password; the location component adds an additional layer of security. Although the note and location are technically two elements, they are quite different than two-factor authentication; they are elements that the user can (and normally does) associate.

VI. USABILITY ANALYSIS

We discuss the usability results of our user studies. We analyze the usability of GeoPass and GeoPassNotes in Section VI-A and VI-B respectively. Limitations are discussed in Section VI-C. User navigation strategies and their implications are discussed in Section VI-D. Finally, we compare GeoPass' and GeoPassNotes' usability in Section VI-E.

A. Usability Analysis of GeoPass

We study the memorability, login times, and user perceptions of GeoPass.

1) Memorability: Our study demonstrated high memorability for GeoPass. The memorability of the system can be quantified by the number of password resets (2.9% or 1/35 in session 1, 0% in session 2, and 3.3% or 1/30 in session 3). Most recently, a 66-day long field study of GeoPass obtained similar memorability results [16]. We further quantify the GeoPass memorability by the low number of failed login attempts in each session (see Table III). The user who forgot his/her location password on day one had four failed login attempts in Session 1. The user who forgot his/her location password in Session 3 had six failed login attempts. The user with four failed login attempts in Session 3 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. After 4 failures this user was reminded the marker is set through right-clicking.

Our 3% (1/30) forgotten location passwords after one week compares favorably to other password schemes; studies by

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2570681, IEEE Transactions on Information Forensics and Security

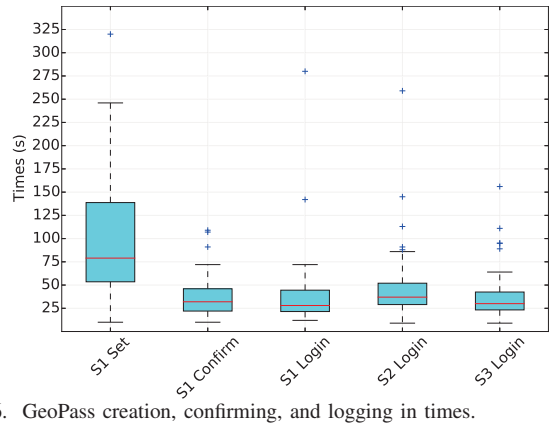

Fig. 6. GeoPass creation, confirming, and logging in times.

others [42] found that 35% (7/20) of regular text passwords and 30% (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 [14] 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).

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.

2) Login Times: Figure 6 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 [14], which had a median login time of 33s on day one, and 52s after one week. Of the users whose times were long, most were due to using substantial panning within the map to navigate to their chosen location. The users who had difficulty 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 [43] may be useful future enhancements to GeoPass by offering users a clearer picture 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.

In the GeoPass study, users were not given a fixed period of training before the creation phase. In session 1, 17% of users had an initial set of failed confirms before their first successful create; the time for these users' failures was not included in the time to create in Figure 6. We allowed GeoPassNotes users an opportunity to practice before the create phase.

3) User Perception: 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?". The answers indicate that 40% of users would use GeoPass for most of their accounts, 63% would use it (or consider using it) for some of their accounts (some users chose both). 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. The answers indicate that 67% of the participants 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. In the users' comments, 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.

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.

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 may increase the effective security offered by GeoPass. We observed navigation strategies (i.e., dragging and panning) that are more likely to result in failed navigation and longer login times which we explain further in Section VI-D.

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 only observed one user making use of satellite view rather than the default map view.

We observed users in the lab for writing down and/or referring to a written hint of their location password. See Section V-C3 for our observations.

B. Usability Analysis of GeoPassNotes

We discuss the memorability, login times, and user perceptions of GeoPassNotes.

1) Memorability: GeoPassNotes also exhibits very high memorability. No users forgot/reset their annotated location

	Session 1	Session 2	Session 3
# failed login attempts	2	1,1,4,4	1,1,4,4

TABLE IV
GEOPASSNOTES FAILED LOGINS FOR EACH SESSION. EACH LIST ELEMENT REPRESENTS A SINGLE USER'S # OF FAILED LOGIN ATTEMPTS.

password. We asked participants questions with Likert-scale responses from 1 (strongly disagree), to 5 (strongly agree). The majority of users (93%) reported no trouble in remembering their annotated location password.

This response complements our analysis of failed logins, which indicated that over the course of all three sessions, only 4/30 users had a failed login; overall, there were very few failed logins (see Table IV). Compared to GeoPass, GeoPassNotes has only a slightly higher number of login failures (22 vs. 21) and no password resets (0 vs. 2).

When asked if they could remember their annotated location passwords for up to 3 and 6 months, most users (see Figure 7) feel they would have no trouble remembering. While this gives us an idea of how memorable users believe their annotated location password to be, it does not tell us whether they actually will remember it; future work should test the memorability of annotated location passwords over longer periods of time.

We also asked participants if, at any point in time, they wrote down a part of their annotated location passwords: 4/30 (13%) mentioned they wrote down some part of their annotated location password. All four participants wrote down information pertaining to the name of the location they chose. Two users wrote down the annotation they chose; one exactly and the other in his native language. Another wrote down the countries and cities he saw on the map as he zoomed into his location. We noticed two of these users writing down a part of or all of their annotated location passwords during session 1. It was unclear whether or not they referred to this in session 2, however we did not observe anyone referring to their written information in session 3. In the GeoPass study, we observed users in the lab sessions to evaluate whether location passwords were written down; we only observed one user referred to their recoding in session 3 after experiencing a problem setting his/her marker.

2) Login Times: As shown in Figure 8, the median login times were 26, 33, and 36 seconds for sessions 1, 2, and 3, respectively. GeoPass median times are lower than those of GeoPassNotes (by 1, 3, and 11 seconds respectively). The time to create an annotated location password in GeoPassNotes is less than that of a location password in GeoPass; this is most likely due to the addition of a practice phase prior to creation in the GeoPassNotes study.

3) User Perceptions: The perceived security of the GeoPassNotes system was very high; 83% of respondents agreed that this method would make their accounts more secure (13% neutral). 86% of the respondents agreed that this method is more secure than text passwords (10% neutral). Most users agreed that they would use this method for some of their accounts if they knew it was more secure than passwords (see Figure 9c). When asked if they would use this method for most of their accounts, most remained neutral, neither agreeing or disagreeing (see Figure 9a). However, most (90%) users agreed they would use it for some accounts (see Figure 9b). Despite the increased time to login, users seemed accepting of the system, one of which mentioned "Even though it takes longer, I would use it because it is more secure". Other comments included "fun" and "a cool way to authenticate".

We asked participants a number of questions relating to their experience with GeoPassNotes. The majority of users (97%) did not report any difficulty using the system. Most (90%) indicated that they could easily use this method every week. Furthermore, most of the users (76%) reported not having any difficulty navigating back to the location they chose. More users indicated they could easily use the method every week than every day, most likely because 17% of users reported that this method was too time-consuming.

4) Qualitative Observations: One participant answered a phone call at the beginning of the login phase, which led to increased login time. The network in the laboratory that we ran our experiments in occasionally had some latency.

C. Limitations

We recruited non-IT UOIT students who had not taken a computer security course, to avoid participants who may have heightened awareness of security. We acknowledge that university students are not fully representative of the users who would use the system since 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. Thus, it is possible that they were more inclined to think about security and reflect this in their choices.

It is possible that variability of screen sizes could have contributed to some login failures. Our studies did not consider the effect of screen sizes, so there may have been some variation. However, our study users were students from our university, which provides laptops to all students. Thus, the majority of students used the same laptop model/size (this was expected and observed in Sessions 1 and 3).

D. Navigation Strategies

Most users followed the recommendation of using the search bar. In the GeoPass study, we observed that the search bar is used during login by 28/35 (80%), 26/33 (79%), and 23/30 (77%) of total users in sessions 1, 2, and 3 respectively. In the GeoPassNotes study, we observed the search bar being used by 26/30 (87%), 26/30 (87%), and 25/30 (83%) of users in sessions 1, 2, and 3 respectively.

All users (except for one in each study) who searched in session 1, continued to use the search feature in subsequent sessions. In the GeoPass study creation phase, 16 users searched for a point of interest, 1 user searched for a postal code, 1 user searched for a street, 11 users searched for a city/town, and 6 users did not use the search bar at all. In the GeoPassNotes study, 6 users searched for a point of interest, 3 users searched for a street, and 17 users searched for a city/town. This suggests that users can employ different

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2570681, IEEE Transactions on Information Forensics and Security

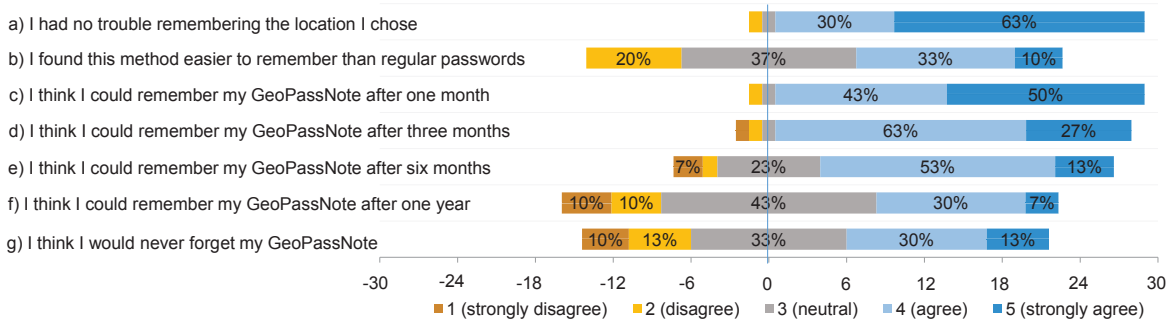

Fig. 7. Likert scale questionnaire responses to the associated questions pertaining to memorability.

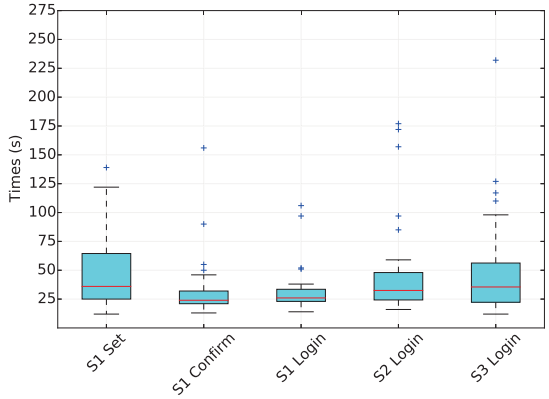

Fig. 8. GeoPassNotes times for creation, confirming, and logging in.

types of initial information to start navigating through maps to choose their location passwords.

There appears to be a relationship between the number of times the user drags (or uses the pan controls) and the time to login. We correlated the number of events the user performed (drag, zoom, double click, search, etc.) with the total login times for each user and found that the correlation coefficients for GeoPass study session 1, 2, and 3 logins were 0.8, 0.7 and 0.5. For the GeoPassNotes study, the correlation coefficients were 0.7, 0.6 and 0.7 for session 1, 2, and 3 respectively. These indicate that the more events a user performs, the longer their login times.

E. Usability Comparison

Our findings indicate that the GeoPass and GeoPassNotes systems have similar memorability, acceptability, perceived ease-of-use, and navigation strategies. Unsurprisingly, GeoPassNotes has higher login times (the medians are 1-11 seconds longer than in GeoPass). 17% of users agree that the GeoPassNotes system is time-consuming (vs. 10% for GeoPass), but only 1/30 (3%) found it difficult to use. We were concerned that the addition of the note would reduce the GeoPass system's excellent memorability, but this did not appear to be the case; on the contrary, there were no password resets in the entire study (0 vs. 2 for GeoPass) and a similar number of failed logins (22 vs. 21 for GeoPass).

VII. Discussion

We have gained some valuable insights from this research. The same patterns in users' location choices were observed in both GeoPass and GeoPassNotes (e.g., the same percentage choose unusual places only they know and places not in the current metropolitan area). Interestingly, it appears that by adding the annotation, users do not appear to modify their behaviour in selecting locations. Also, the memorability does not appear to be impacted by adding this annotation. Our analyses suggest that GeoPassNotes offers some resistance to offline attack, whereas GeoPass clearly does not. GeoPassNotes users did not appear to choose annotations with strongly observable relationships to their locations. The annotation also improves resistance to observation attack (such that it is as observable as a text password) and adds protection against attacks from third party map service providers (e.g., Google) who are capable of knowing the location portion of the password.

In this section, we also discuss the feasibility of using the navigation task within the authentication algorithm in Section VII-A. We discuss our resulting security policy recommendations in Section VII-B. Section VII-C summarizes an evaluation of GeoPass and GeoPassNotes using a web authentication framework. Section VII-D discusses plausible use cases for the system and additional studies that should be performed in future work.

A. Authentication Through the Journey

We noticed that the majority of users seemed to navigate to their chosen locations the same way every time. In the interest of determining whether a user's journey could be used to enhance the strength of GeoPass and its variants, we analyzed each user's navigation strategies across every session to see if this could be an added security requirement.

To evaluate this, we considered the sequence of navigation events (e.g., click, drag, double-click, search, or scroll) as the *journey*. We then tested the journey from the location password confirmation for equality with the journeys collected in each session. If we were to require the exact journey to be used for logins, then 70%, 63%, and 60% of users would have successful logins. However, it is not consistent enough to be a usable login requirement. Next, we evaluated how many users would successfully authenticate if the subsequent journey was off by at most one navigation event. For example, if the journey was (drag, double click, search), then (drag, search) would also be accepted. This changed the results to be 98% successful login rates across all three sessions. However, the security impact of this requirement would be very little.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2570681, IEEE Transactions on Information Forensics and Security

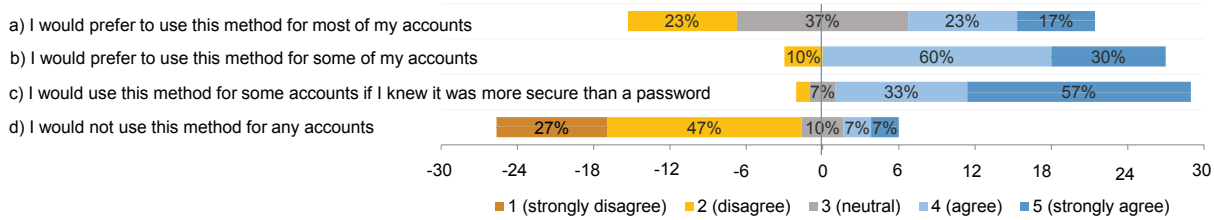

Fig. 9. Likert scale questionnaire responses to the associated questions pertaining to acceptability.

After all of the research we have conducted on using locations to authenticate, it is not clear why locations are so memorable. Is it the location itself, a special event and/or memory that occurred, or something else? One interesting idea is that users might be remembering parts of the journey associated with their location. Since the majority of users use the same journey for each login, it might be the key factor in making GeoPass and GeoPassNotes so memorable. It would be very interesting to research this more, and discover if the user's journey effects the memorability of the location they end up choosing.

B. Security Policy Recommendations for Geographic Authentication Systems

Based on our security analyses, we suggest a set of recommended policies for future implementations of GeoPass and GeoPassNotes. These recommendations are as follows:

- *Avoid choosing a location that you have previously worked or lived.*

The results of our studies indicate that nearly all users followed the recommendation not to choose a location previously lived or worked at. This was a positive result, and it did not seem to affect the overall usability of the system. We also recommend the following policy:

- *Avoid directly labelling a location in the note (e.g., do not annotate Daytona Beach with "Daytona" or "beach").*

This prevented the majority of study users from directly labelling their locations. Similar to our previous recommendation, the usability of the system did not appear to be affected, while the security was greatly increased.

One user of our study also chose a three character note. We did not disallow this as part of the study was to gain more understanding of possible notes; however, since it is a risky choice we observed, we recommend the following policy:

- *Avoid choosing a note with a low number of characters (e.g., less than 4).*

We recommend that proactive checking for these policies be employed for future versions of GeoPass and GeoPassNotes. Disallowing short annotations is easy, but implementing proactive checking of other policies might not seem as obvious. Using Google API's built in tools, it is possible to perform on-the-fly checks of the location password. Reverse geolocation requests return arrays of address components (e.g., formatted address, short name, long name, postal code, etc.), which can be searched for similarity to the user's annotation.

Enforcing that a user does not choose a place lived or worked before is more challenging. Relevant information could be collected as part of the registration/enrollment process such as a user's city of birth, or using social networking account information (e.g., Facebook or LinkedIn) with the user's permission. Then, it would be possible to restrict markers placed in those locations. The local adversary attack could be easily prevented through a coordinate lookup based on IP geolocation results.

C. Authentication Framework Summary

We evaluated GeoPass and GeoPassNotes according to the web authentication framework of Bonneau et al. [44] and summarize the results herein. The framework shows that GeoPass offers the same characteristics as passwords, with the following exceptions. GeoPass is better on the measures of "infrequent errors", and "resilient to throttled guessing" (with a policy to prevent local knowledge adversaries), but GeoPass is worse on the measures of "efficient to use", "accessible", "server compatible", "mature", and "no trusted third party". It also shows the benefits of GeoPassNotes over GeoPass with respect to the measures of "resilient to throttled guessing" (it doesn't require a policy to prevent local knowledge adversaries), "resilient to unthrottled guessing" (with a policy to prevent local knowledge adversaries), and "no trusted third party". The framework evaluation essentially shows that there are usability tradeoffs that indicate these systems are probably not good replacements for all of a user's web passwords, so we do not recommend GeoPass and GeoPassNotes to be candidate replacements for all of a user's web passwords, but possibly only a handful of them that are infrequently used. We also think another candidate use case for these systems might be for fallback authentication. Future work towards studying these use cases are discussed further in Section VII-D.

D. Use Cases and Future Studies

Due to the long login times, but high memorability of the GeoPass and GeoPassNotes systems, we do not consider them to be candidate replacements for all of a user's passwords, but rather possibly a handful of them that are infrequently used. Our survey results indicate that users also seem to be comfortable with using GeoPass and GeoPassNotes for some accounts, especially if they know they are more secure than text passwords. Before these systems are used for the purpose of infrequently used accounts, it is important that further testing be performed. Multiple password interference could be a problem; this issue was recently studied by Al-Ameen et al. [17] for GeoPass only. They performed a study to determine interference effects with 4 location passwords. They found that memorability dropped to 70%, but interestingly

they performed a second study to evaluate interference in the presence of a mnemonic strategy, whereby users are asked to think of a story to associate each account to its location password. The key finding was that if this mnemonic strategy is used, memorability rates are quite high ($> 97\%$). Meng [18] also performed a study on multiple location password interference, finding that with 5 location passwords, after 3 weeks 88.7% of users could login within 3 attempts. Such studies should also be performed for GeoPassNotes, using the mnemonic strategy of Al-Ameen et al. [17], in future work.

Another candidate use case for these systems might be for fallback authentication. Hang et al. [19] leverage GeoPass for fallback authentication by asking users a location-based security question, which they answer by entering a location. They found that their approach was memorable, and also that their security questions leaked little useful information to most adversaries. One can consider GeoPass/GeoPassNotes as a method of fallback authentication without posing any security question. If GeoPass itself were to be used for fallback authentication, the user would simply enter a location, in the absence of any questions. In this case, the user could set up a hint to help them recall their location if needed. Similarly, if GeoPassNotes itself were to be used, the user would simply enter their location and annotation. In both cases, there would not be any questions, making it distinct from location-based security questions. A separate long-term study would be required to compare fallback strategies using such location-based systems to others in the literature to determine differences in memorability and security.

Finally, field studies are required to better evaluate how both the GeoPass and GeoPassNotes systems would be used in practice. Al-Ameen et al. [16] recently ran a 66-day long field study with GeoPass, finding a 96.1% login success rate and that 100% of participants logged in successfully within five attempts on average. In future work, field studies are needed that specifically focus on the use case of infrequently used accounts by testing their usability over longer intervals between logins for both GeoPass and GeoPassNotes. These studies should also examine the impact of the security policy recommendations discussed in Section VII-B, in particular those related to proactive checking.

VIII. Concluding Remarks and Future Work

We propose, implement, and evaluate two systems for geographic authentication: GeoPass and GeoPassNotes. We evaluate the systems' security and usability through two user studies, finding that they both exhibit very strong memorability (over the span of 8-9 days, there were only two resets for GeoPass and none for GeoPassNotes). Usability was high in terms of there being few failed logins and user perceptions of the system. Although 67% of the GeoPass users and 80% of the GeoPassNotes users indicated that they could easily use the system every day, we must be cautious about recommending their use on frequently used accounts. Given that the login times for both systems are longer than text passwords, we suggest they would be most appropriate in contexts where logins occur infrequently. For example, it might be useful for infrequently used online accounts or possibly fallback authentication. We found that annotated location passwords have the potential to be stronger than text passwords against guessing attacks when proper policies are applied, thus they may be more desirable for higher-security environments.

Our initial thoughts were that event-specific memories are what would make annotated location passwords memorable. However, we noticed that some participants randomly chose places that looked interesting on the map (this was also supported by our questionnaire responses; in each study, 23% of users reported choosing random places). This raises the question of whether it is not the memories about locations, but simply locations themselves, that people remember well. This leads us to consider, as a possibility for future work, whether annotating a randomly generated location might yield the same positive results.

The geographic authentication schemes we explored appear to be highly memorable; it would be interesting to explore other ways to harness this memorability while enhancing security. One interesting direction is to explore the extent that the presentation effect [45] can improve security in geographic authentication systems. Another future direction includes exploring whether the memorability of geographic locations might translate if used in mnemonics for text passwords.

Acknowledgments

We are grateful to the reviewers whose comments helped us greatly improve this paper. We also thank the participants of our user studies, and the SOUPS 2013 participants and reviewers for their feedback on GeoPass. This research was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *IEEE Security and Privacy*, vol. 2, no. 5, pp. 25–31, 2004.

[2] R. Veras, C. Collins, and J. Thorpe, "On the semantic patterns of passwords and their security impact," in *Proceedings of the 21st Annual Network and Distributed System Security Symposium*, ser. NDSS'14, 2014.

[3] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, ser. SP'12, pp. 538 –552.

[4] 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*, ser. CHI '10, 2010, pp. 383–392.

[5] 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*, ser. SP '09, 2009, pp. 375–390.

[6] 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.

[7] D. Nelson, V. Reed, and J. Walling, "Pictorial superiority effect," *Journal of Experimental Psychology: Human Learning and Memory*, vol. 2, no. 5, pp. 523–528, 1976.

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

[9] S. Madigan, "Picture memory," in *Imagery, Memory and Cognition*. Lawrence Erlbaum Associates Inc., 1983, pp. 65–89.

[10] J. Thorpe, B. MacRae, and A. Salehi-Abari, "Usability and security evaluation of geopass: a geographic location-password scheme," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS '13, 2013.
[11] G. Kristo, S. M. Janssen, and J. M. Murre, "Retention of autobiographical memories: An internet-based diary study," *Memory*, vol. 17, no. 8, pp. 816–829, 2009.
[12] S. Fox, "Future online password could be a map," 2010, http://www.livescience.com/8622-future-online-password-map.html, site accessed Mar. 2014.
[13] J. Spitzer, C. Singh, and D. Schweitzer, "A security class project in graphical passwords," *Journal of Computing Sciences in Colleges*, vol. 26, no. 2, pp. 7–13, 2010.
[14] H.-M. Sun, Y.-H. Chen, C.-C. Fang, and S.-Y. Chang, "Passmap: A map based graphical-password authentication system," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '12, 2012, pp. 99–100.
[15] J. Shin, S. Kancharlapalli, M. Farcasin, and E. Chan-Tin, "Smartpass: a smarter geolocation-based authentication scheme," *Security and Communication Networks*, vol. 8, no. 18, pp. 3927–3938, 2015.
[16] M. N. Al-Ameen and M. K. Wright, "A comprehensive study of the geopass user authentication scheme," *CoRR*, vol. abs/1408.2852, 2014.
[17] ——, "Multiple-password interference in the geopass user authentication scheme," in *Workshop on Usable Security (USEC)*, 2015.
[18] W. Meng, "Routemap: A route and map based graphical password scheme for better multiple password memory," in *Proceedings of the 9th International Conference on Network and System Security*, ser. NSS'15, 2015, pp. 147–161.
[19] A. Hang, A. De Luca, M. Smith, M. Richter, and H. Hussmann, "Where have you been? using location-based security questions for fallback authentication," in *Proceedings of the Eleventh Symposium on Usable Privacy and Security*, ser. SOUPS '15, 2015.
[20] K. Renaud and M. Just, "Pictures or questions?: Examining user responses to association-based authentication," in *Proceedings of the 24th BCS Interaction Specialist Group Conference*, ser. BCS '10, 2010, pp. 98–107.
[21] 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*, ser. CHI '11, 2011, pp. 2605–2614.
[22] K. Bicakci and P. van Oorschot, "A multi-word password proposal (gridword) and exploring questions about science in security research and usable security evaluation," in *Proceedings of the 2011 Workshop on New Security Paradigms Workshop*, ser. NSPW '11, 2011, pp. 25–36.
[23] A. Stubblefield and D. Simon, "Inkblot Authentication," 2004, microsoft Technical Report MSR-TR-2004-85.
[24] J. Thorpe, A. Salehi-Abari, and R. Burden, "Video-passwords: Advertising while authenticating," in *Proceedings of the 2012 Workshop on New Security Paradigms*, ser. NSPW '12, 2012, pp. 127–140.
[25] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, ser. SS'07, 2007, pp. 103–118.
[26] J. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical passwords," *IEEE Transactions on Information Forensics and Security*, vol. 1, pp. 395–399, 2006.
[27] 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*, ser. CHI '11, 2011, pp. 2627–2630.
[28] Tripadvisor, http://www.tripadvisor.com, accessed Mar. 2014.
[29] 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, accessed Mar. 2013.
[30] T. Channel, "Top 10 vacation spots," http://www.travelchannel.com/interests/travel-tips/articles/top-10-vacation-spots, accessed Mar. 2013.
[31] "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, accessed Sept. 2012.
[32] D. Florêncio, C. Herley, and P. C. Van Oorschot, "An administrator's guide to internet password research," in *Proceedings of the 28th USENIX Conference on Large Installation System Administration*, ser. LISA'14, 2014, pp. 35–52.
[33] M. Davies, "Corpus of contemporary american english," http://corpus.byu.edu/coca/, accessed July 2013.
[34] N. Schmitt and M. McCarthy, *Vocabulary: Description, Acquisition and Pedagogy*. Cambridge University Press, 1997.
[35] Social Security Administration, "Beyond the top 1000 names," http://http://www.ssa.gov/oact/babynames/limits.html, accessed Sept. 2013.
[36] Openwall, "JohnTheRipper," https://github.com/magnumripper/JohnTheRipper, accessed Jan. 2014.
[37] dazzlepod, "Password list," http://dazzlepod.com/site_media/txt/passwords.txt, accessed Feb. 2014.
[38] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, ser. SP '09, 2009, pp. 391–405.
[39] S. Security, "Leaked passwords," http://downloads.skullsecurity.org/passwords/, accessed May 2014.
[40] 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*, ser. CHI '12, 2012, pp. 2175–2184.
[41] 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*, ser. CHI '10, 2010, pp. 1107–1110.
[42] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, no. 1, pp. 102–127, 2005.
[43] 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*, ser. CHI '12, 2012, pp. 287–296.
[44] J. Bonneau, C. Herley, P. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *IEEE Symposium on Security and Privacy*, 2012.
[45] J. Thorpe, M. Al-Badawi, B. MacRae, and A. Salehi-Abari, "The presentation effect on graphical passwords," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2947–2950.

Brent MacRae is a lecturer and graduate student researcher at the University of Ontario Institute of Technology (UOIT). He is currently pursuing a Masters of Science in Computer Science from UOIT and received a Bachelor of Information Technology (2013) from UOIT. His research interests include authentication, software security, usability, and network security.

Amirali Salehi-Abari is a Ph.D. candidate at the Department of Computer Science, University of Toronto. His primary research goals are directed towards designing effective decision-support and information systems, aiming to ease and assist human decision making. His interdisciplinary research in authentication and artificial intelligence has received a student best paper award (IEEE PST 2010), been granted a US patent, and been awarded scholarships from NSERC and OGS.

Julie Thorpe is an Assistant Professor at the University of Ontario Institute of Technology (UOIT). She has a Ph.D. in Computer Science from Carleton University and a Bachelor of Computer Science from Dalhousie University. Prior to joining UOIT, she worked in the field of IT security for 8 years. She has served on the program committee for various conferences including ACM CCS, USENIX Security, ACSAC, PST, and NSPW. Her research interests include authentication, human factors, security policy, software security, and operating system security.