Geographical Security Questions for Fallback Authentication*

Alaadin Addas
Ontario Tech University
Oshawa, Canada
alaadin.addas@uoit.ca

Amirali Salehi-Abari
Ontario Tech University
Oshawa, Canada
abari@uoit.ca

Julie Thorpe
Ontario Tech University
Oshawa, Canada
julie.thorpe@uoit.ca

***Abstract*—Fallback authentication is the backup authentication method used when the primary authentication method (e.g., passwords, biometrics, etc.) fails. Currently, widely-deployed fallback authentication methods (e.g., security questions, email resets, and SMS resets) suffer from documented security and usability flaws that threaten the security of accounts. These flaws motivate us to design and study Geographical Security Questions (GeoSQ), a system for fallback authentication. GeoSQ is an Android application that utilizes autobiographical location data for fallback authentication. We performed security and usability analyses of GeoSQ through an in-person two-session lab study (n=36, 18 pairs). Our results indicate that GeoSQ exceeds the security of its counterparts, while its usability (specifically login time and memorability) has room for improvement.**

I. Introduction

Authentication mechanisms (e.g., passwords, biometrics, PINs, etc.) play a critical role in securing our accounts and devices against unwanted access. However, our primary means of authentication fail when we forget our *secrets* (e.g., passwords or PIN) or when our biometric measurement is malfunctioning. These failures of authentication mechanisms motivate the need for secondary authentication, referred to as *fallback authentication*, for the users to gain access to their accounts or devices. The most popular fallback authentication methods are security questions, email resets, and SMS resets. Security questions (or personal knowledge questions) are often in the form of predefined questions (e.g., what is the color of your first car?). For fallback authentication, the users' answers to these questions must match their answers provided at registration time. Some other popular fallback authentication methods use other communication channels such as email or phone to send a link or PIN for password reset. These fallback authentication methods suffer from security flaws that compromise the security of our accounts and devices.

Security flaws in widely-utilized fallback authentication methods motivate us to explore alternative fallback authentication methods. We investigate the usability and security of GeoSQ (Geographic Security Questions) as a means of fallback authentication. In GeoSQ, users are expected to answer a sequence of autobiographical location questions (e.g., where were you on the 18th of December at 4:00 PM?) by clicking on a digital map. GeoSQ attempts to address some of the security flaws prevalent in other fallback authentication systems such as the easy guessability of security questions [2], the avalanche effect vulnerability in email resets [3] and SMS resets, and attacks on telecommunications protocols [4].

We investigate the security and usability of GeoSQ through a user study that spanned two sessions (n=36). From a security perspective, our results indicate that GeoSQ is resilient to throttled online guessing attacks, and phishing attacks. However, GeoSQ is not resilient to the known adversary threat due to the predictability of locations by known adversaries. The large key space of $2^{94.25}$, offered by GeoSQ, makes it very difficult to conduct a successful throttled online guessing attack (see Section V-A). When compared to the security of security questions, email resets, and SMS resets, GeoSQ offers improved protection against several threats including throttled online guessing attacks, and unthrottled guessing attacks. From a usability perspective, GeoSQ needs improvement in several key metrics. The long login time and the frequency of errors is a point of concern when compared to currently utilized fallback authentication systems. Our study and investigation has shed light on important future work to make GeoSQ more usable while maintaining its security.

II. Related Work

The most popular methods for fallback authentication are security questions, email resets, and SMS resets. Autobiographical authentication has also recently attracted attention as a viable alternative [5]–[7].

Current Fallback Authentication Methods. Security questions are easy to guess [2], [8]. Users don't recall security questions 40% of the time [9]. In email resets, the email is a single point of attack: if the recovery email is compromised many other accounts are easily compromised [3]. From a usability perspective, the loss of the recovery email would complicate the fallback authentication process [3]. Guri *et al.* [10] has shown that rogue applications in a mobile environment can request access to sensitive resources such as email, thus giving an attacker the capability of snooping on email resets. SMS resets are also susceptible to snooping attacks [11], [12] and flaws in telecommunication protocols [4].

Autobiographical Authentication. The aforementioned security and usability flaws have motivated alternative authentication techniques. Das *et al.* [5] has determined 9 distinct cate-

*For more details and results, refer to the extended version [1] gories of autobiographical data, including location data from everyday activities. This helped the development of *MyAuth*, an application that logs different types of autobiographical data and queries the user about them. Through a field study (n=24), it was found that location questions of "where were you on $<$time$>$" were more likely to be answered correctly than others. This was part of our motivation to further investigate autobiographical location in GeoSQ.

Hang *et al.* [6] identified 7 categories of autobiographical authentication data. Their pre-study (n=19) showed that outgoing SMS, incoming SMS, and app usage questions are the most promising in terms of memorability. Recruited adversaries (n=19) were highly successful in guessing outgoing SMS and incoming SMS , but not in guessing app usage (35%).

AlBayram *et al.* [7] conducted a field study (n=24) on 9 categories of autobiographical authentication data. A monitoring application was utilized to log autobiographical data, and participants were asked questions from the last 24 hours for each category. Autobiographical data has episodic memory, this being more memorable in short time spans [13]. The most memorable categories of autobiographical data in terms of memorability were incoming/outgoing call, and location data.

Hang *et al.* [6] and AlBayram *et al.* [7] investigate the threat of known adversaries on their proposed autobiographical authentication systems. The frequency of unauthorised access to smartphones by known adversaries has also been studied [14]. The known adversary is any individual with first-hand knowledge of a potential victim and/or elevated access to their devices, who uses these privileges with malicious intent [15].

Relevant Authentication Systems. Alphanumerical passwords, widely-used method for primary authentication, suffer from usability and security weaknesses [16]. Modern password crackers can efficiently guess a large number of passwords [17]–[20]. The developments in password cracking have motivated alternative primary authentication systems such as graphical passwords [21]. A well studied class of graphical passwords are click based graphical passwords (e.g., PassPoints [21], Cued Click Points [22], and Persuasive Cued Click Points [23]). The security of various passpoint-style graphical passwords is studied [24]–[28] which has motivated the development and design of click-based authentication systems on videos [29], and digital maps [30]–[32]. The memorability of geographical authentication systems (e.g., GeoPass and GeoPassNotes) is very high (97% and 100% respectively) after 1 week of setting the credentials. Map-based authentication systems (e.g., GeoPass and GeoPassNotes [31], [32]), are of relevance to our work.

III. GeoSQ: Implementation and Design Decisions

We designed and developed a location-based fallback authentication system called Geographical Security Questions (GeoSQ), a variant of previously-proposed autobiographical authentication systems [7], [33]. GeoSQ runs in the background with enabled location services to log unique locations visited by the user. A location is considered *visited* if the user has stayed at least 5 minutes in that location. The *uniqueness* of locations is determined by checking if a location is 400 meters away from any previously logged location.[1] Locations are logged in GeoSQ by geographic coordinates (latitude and longitude). When 10 locations have been logged, the user can be queried about their unique visited locations in the following format: Where were you on the dd of mm of $yyyy$ at t, where dd, mm, $yyyy$, and t stands for specific day, month, year, and time, respectively (e.g., where were you on 14/02/2018 at 4:00PM?). The user is then expected to navigate to a location on the map and set a marker on the correct logged location. A response location is correct if the marker is set within 200 meters of the logged location. For a successful authentication, the user must answer 7 out of 10 location questions correctly. As shown in Fig. 1a, the user is required to click the next button after answering a location question. The user can change the selected location by using the remove button to first deselect the location, and then selecting a new location. Lastly, users have the ability to withdraw at any time and uninstall the application using the withdraw button.

Users can also switch between default map mode (see Fig. 1a) and satellite map mode (see Fig. 1b). Map navigation can be done either by dragging over the map, or using the search bar with location keywords (see Fig. 1c). Search results are ordered based on the current location. GeoSQ users also have the ability to zoom in and out (see Fig. 1d). GeoSQ was implemented with several usability and security goals in mind discussed in Sections III-A and III-B.

A. Security-Oriented Design Decisions

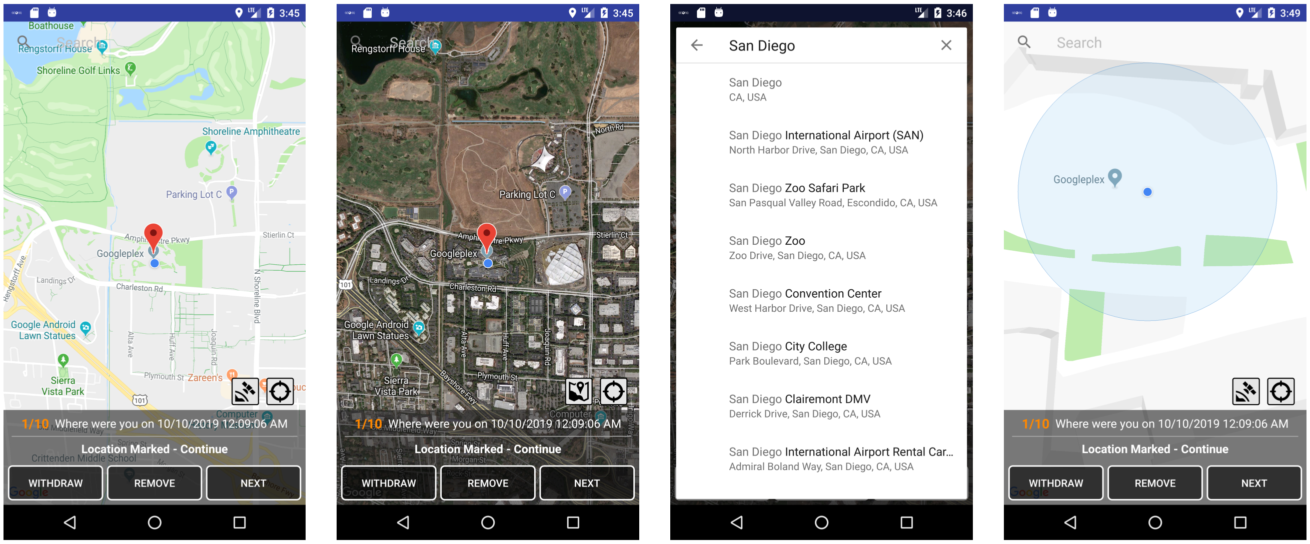
An important security concern with location-based autobiographical authentication is that the daily mobility patterns of users are predictable (e.g., users go to work and return home during weekdays). This makes mounting attacks easier (even with limited guesses). To address this security concern, we filter out these predictable easy-to-know locations by a simple heuristic. We assume that the locations at which the user spent more than 5 hours are predictable and easy-to-know by an adversary. This security decision has a usability cost, as GeoSQ requires a longer period of time (e.g., 7–10 days) to log enough unique, and less predictable locations.

To ensure resilience to guessing attacks, GeoSQ asks 10 unique location questions, and requires 7 (out of 10) correct answers for a successful authentication. The choice of 70% threshold is supported by earlier findings that users are able to recall roughly 70% of their locations [7].

B. Usability-Oriented Design Decisions

It is unrealistic to expect users to input their exact locations in GeoSQ. As such, we considered a 200-meter error margin that would account for human input errors as well as errors in the accuracy of logging locations. This hinders security by making the key space smaller, but is necessary for usability purposes. Our decision on 200-meter error is based on *location accuracy settings* (discussed below) and *input errors* in touch

[1] A 400 meter threshold was set to ensure that participants on a campus or a large building do not obtain multiple location questions in the same vicinity.



(a) Default Mode (b) Satellite Mode (c) Search (d) Zoom

Fig. 1: GeoSQ Interface; (a) Default map mode, users can set/remove markers; (b) Satellite map mode that users can switch to for better memorability; (c) Search functionality for easy navigation; and (d) Zoom functionality.

screen interfaces. Through our pilot studies, we noticed that input errors vary depending on the zoom level. Therefore, we set the default zoom level to be 16, at which the 200-meter error margin is effective enough to reduce such errors.

Location services in smartphones drain a considerable amount of battery power. Thus, we adjusted the location setting so as to minimize the risk of missing locations and battery usage. GeoSQ to refreshes the location every 2.5 minutes with the *balanced power* setting. Our decision to log visited locations, at which user remained for more than 5 minutes, was necessary to prevent logging transient locations (e.g., a sequence of locations where a user is walking from work to his vehicle). Recalling transient locations are hard especially over a span of 7-11 days.

IV. User Study and its Design

We evaluated the security and usability of GeoSQ through a 38-participant (19 pairs) user study, approved by our universitys Research Ethics Board. Participants were students, visitors, or staff of our university, who met the following criteria: (i) 18 years of age or above; (ii) Participants must bring a pair; (iii) Participants must have an Android smartphone; and (iv) Participants must be willing and able to turn on location services throughout the week. Our user study contained two sessions spanning 7–11 days. The pairs completed the exact same steps (i.e., we did not have a main participant and a pair).

Session 1. This session was an in-lab session held on several different dates, and time slots. Each participant was compensated $8 for their participation. Followed by reading the pre-written instructions to the participants, we also ran a demonstration of the GeoSQ application. Then, they proceeded to complete the entry survey. We instructed participants to download, install and read the embedded instructions within GeoSQ. Lastly, they would be reminded to keep location services on as GeoSQ is logging location information *locally* in the background. They were informed that location services could be turned off when they were not comfortable.

Session 2. This session was held 7–11 days after Session 1 in the lab to provide enough time for logging 10 unique visited locations. Participants were compensated $10. Similar to Session 1, Session 2 also started with the instructions being read off a pre-written script. GeoSQ prompted each participant with ten location questions regarding their whereabouts of their previous 7–11 days. Then, each pair was asked to switch phones and attempt to guess each other's location questions. A set of 10 identical questions were asked for each user and his/her paired attacker. Lastly, participating pairs returned phones to each other and answered usability questions in an exit survey.

In Session 1 and Session 2, we also tested another completely independent authentication system [34] that is not discussed in this paper. As another system was tested, Session 1 was approximately 35 minutes and Session 2 was approximately 45 minutes. In both sessions, the GeoSQ memory test was performed second.

Demographics Details. Recruited participants were all undergraduate students in the range of 18–30 years old (with the average of 21.3). Out of 38 initial participants, 13 were female (34.2%), 25 were male (65.7%), and 15 (39%) had already taken some computer security/IT course .

V. Security and Usability Analyses

We discuss the security and usability analyses of GeoSQ.

A. Security Analysis

We analyse the security of GeoSQ under various threats that GeoSQ is expected to be resilient against as an autobiographical fallback authentication. For each threat, we first define it and then measure the resilience of GeoSQ against it.

Throttled Online Guessing Attacks. Resilience to throttled online guessing attacks, formally defined by Bonneau *et al.* [35], is necessary for any fallback authentication method. A system is resilient to throttled online guessing attacks if an attacker cannot compromise more than 1% of accounts a year, given ten guesses a day [35]. Throttled online guessing attacks can fall into two categories based on whether or how the adversary has knowledge of victim. We here first analyze the *classical* throttled online guessing attacks in which the adversary has no knowledge of the potential victim. We then analyze a special cases of *known adversary*.

We ensured that GeoSQ is resilient to classical throttled online guessing attacks by taking two important measures. (i) We only allow one attempt per location question. This restriction effectively enhances the security of our systems at the usability cost (discussed below). (ii) We also expand the key space by requiring 7 out of 10 questions to be correctly answered. In our user study, we didn't track mobility patterns of our participants (due to privacy and confidentiality) as such we have estimated the key space to be $2^{94.25}$. Our key space calculation is based on the assumption that users will be within a 12 km radius (452.3 km^2) of their home location. This is consistent with reported statistics for commute distances to work (the median commute is 12.9km) [36]. We then incorporate the concepts of central and robust discretization [37], [38]. Given our 200 meters error margin, one discrete location covers 0.04 km^2. We therefore have $\frac{452.3}{0.04} = 11,307$ ($2^{13.4}$) unique locations per question. Since we require 7 out of 10 location questions to be answered correctly for a successful authentication, our key space is $P(11,307,7) = 2^{94.25}$, where $P(n,k)$ is the the number of k-permutations of a set with n elements. As our system only allows one attempt per location question and its key space is very large, GeoSQ is resilient to throttled online guessing attacks.

The Known Adversary. We differentiate between known adversary and a throttling online attacker by determining whether or not an attacker has first-hand knowledge of the potential victim. Our known adversary model is similar to that of Hang *et al.* [6] and AlBayram *et al.* [7]. We consider a system to be resilient to the known adversary if known-adversary attackers cannot compromise more than 1% of accounts per year.

We allowed pairs to attempt to guess each others autobiographical location questions. In our analysis, 5.8% of participating pairs managed to login successfully with our threshold of 7 correct answers for a successful authentication. We conducted an analysis on the data to determine the true positive rate and the false positive rate in the form of a Receiving Operator Characteristics (ROC) curve (see Fig. 2). According to the ROC curve, the resilience to the known adversary depends strongly on the threshold. At a threshold of 7/10 correct questions, both false positive rate (FPR) and true positive rate (TPR) are low at 5.8% and 11.7%, respectively (see Section V-B for relevant discussion on usability analysis). The TPR can improve to 32.8% by setting the threshold to 6 at the cost of increasing FPR to 14.7%. However, 14.7% is much higher than 1% threshold, required for resilience to the known adversary. This analysis suggests that GeoSQ is not resilient to the known adversary.

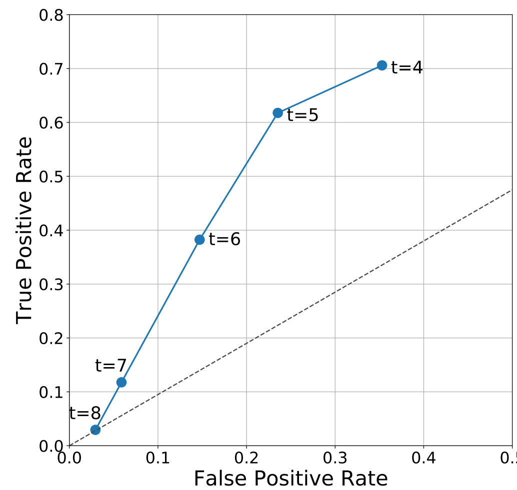


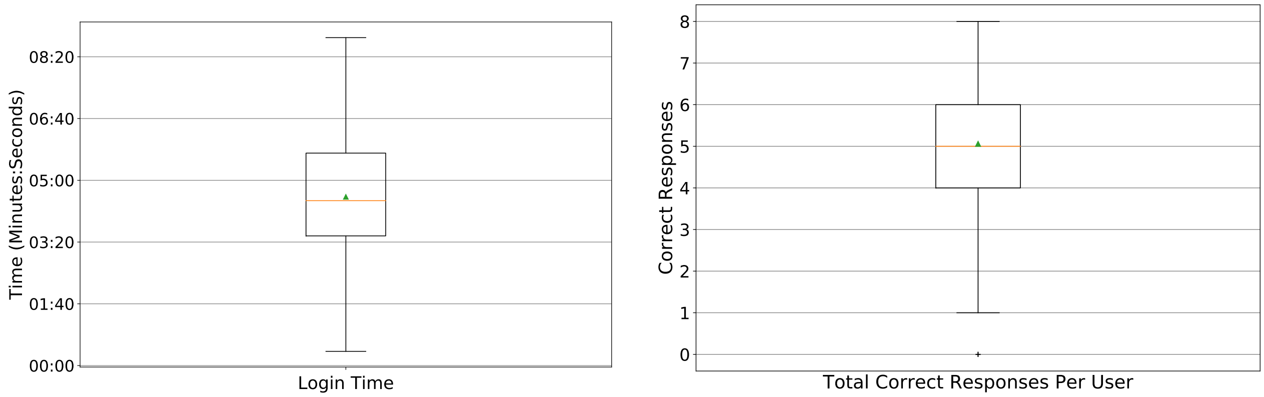
Fig. 2: ROC curve with varying thresholds (t), t=10 and t=9 (not shown) have zero true positive and false negative rates.

B. Usability Analysis and Results

We will evaluate GeoSQ under core usability metrics [35].

Efficiency of Use. An authentication method is *efficient to use* if the time spent for each authentication is acceptably short, and a user can also set up his/her credentials within a reasonable time determined based on the target environment [35]. For GeoSQ, the target environment is fallback authentication, therefore the comparison counterparts are commonly utilized fallback authentication methods such as security questions, email resets, and SMS resets. GeoSQ takes 7-11 days to set up credentials (i.e., 10 unique locations) per use, unlike security questions, email resets, or SMS resets with several seconds/minutes set-up time, [9]. This long set-up time of GeoSQ is due to its autobiographical nature. This usability flaw is mitigated by the fact that fallback authentication is not undergone as often as primary authentication by any typical user [9]. Another important metric for efficiency of use is the login time. Fig. 3a shows the average login time for all ten questions in our user study at under 5 minutes.

Frequency of Errors. An authentication scheme has infrequent errors if the login task is usually successful when performed by the true user [35]. Fig. 3b shows the average correct responses over both users and questions. The average number of correct responses is 5.06, slightly higher than 50% of the questions asked. Fig. 2 shows the ROC curve that



(a) Average total login time (10 questions)

(b) Average of correct responses

Fig. 3: (a) Average login time of GeoSQ for all 10 questions (n=36, each user was asked 10 questions). Two outliers above 6 minutes were removed due to technical difficulties. (b) average correct responses (over questions and users) (n=36).

determines the false positive rate and the true positive rate for each threshold. Given the number of incorrect answers in order to make this system usable for 61% of users, we must set the threshold to 5 correct answers out of 10. However, the risk becomes the security concern because at that threshold, the false positive rate is about 24% (n=36, 18 pairs).

Due to the high error rate of 50%, we consider GeoSQ highly prone to errors, requiring further investigation and improvement to make it usable.We also qualitatively evaluated GeoSQ's ease of use (see the extended version [1]).

VI. Discussion and Future Work

GeoSQ's security is comparable to other fallback authentication techniques. However, GeoSQ's usability has several shortfalls, when compared to SMS resets, email resets, and security questions. The shortfalls arise from several design factors: (i) The time span to log 10 unique questions was around 7-11 days, that design decision was expected to harm usability to some extent. However, the long login time and the frequency of errors by participants originate from low memorability of autobiographical location information over 7-11 days [7], suggesting a need for decreasing the logging time-span. (ii) During Session 2, we had a demonstration where GeoSQ features were explained. However, during the recall phase we observed many participants were still getting used to the interface because they did not have hands-on experience. The lack of training was a contributing factor to the long login time. (iii) The absence of the day of the week in our autobiographical location questions turned out to be an important factor in slowing down the users. More informative questions by incorporating the day of the week could have potentially improved login time and memorability.

One can make a few conclusions with regard to GeoSQ's usability shortfalls: (i) From a memorability point of view, non-significant location events (e.g., going to a coffee shop) are expected to have weaker memorability compared to significant location events (e.g., attending a concert). However, there is no guarantee that each user has had significant location events in the recent past, and those events were logged. Future work can study the detection of secure significant events for use in GeoSQ. (ii) GeoSQ can possibly be deployed for a subset of users. Individuals with location privacy concerns often keep their location services off. That's why we recommend using GeoSQ-like systems as an optional method for fallback authentication. (iii) Setting the error margin to be 200 meters makes map based authentication more usable, and does not hinder the security to a great extent (see Section V-A). Slightly increasing the errors margin from 200 meters should improve the usability of GeoSQ.

GeoSQ offered strong security when compared to other fallback authentication methods due to its large key space. However, GeoSQ lacked in several usability metrics including login time and failure rate.

Future work should focus on making questions more memorable by detecting significant events. Utilizing hints for location-based questions has proven to be effective in the past [39]. Hints paired with significant event detection has the potential to improve the memorability of similar authentication systems. Furthermore, current focus on location-based autobiographical authentication is on discrete location questions (i.e., where were you at a certain point in time). However, one can investigate location questions based on the sequence of locations or continuous locations (e.g., routes taken).

VII. Conclusion

Fallback authentication techniques such as security questions, email resets, and SMS resets suffer from usability and security issues. To address these issues, we developed GeoSQ that logs location data, then asks 10 unique location questions where 7 correct answers are required for successful authentication. Our user study suggests that GeoSQ offers several security benefits over commonly utilized fallback authentication methods. However, the usability of GeoSQ is not comparable. Several changes are proposed to improve the usability for large-scale deployment.

VIII. Acknowledgment

We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), funding reference numbers 402500-2013 and RGPIN-2018-05903.

References

[1] A. Addas, J. Thorpe, and A. Salehi-Abari, "Geographical security questions for fallback authentication," *CoRR*, vol. arXiv:1907.00998v1, pp. 1–18, 2019.

[2] M. Golla and M. Dürmuth, "Analyzing 4 million real-world personal knowledge questions (short paper)," in *Proceedings of the 9th International Conference on Passwords*, 2015, pp. 39–44.

[3] S. L. Garfinkel, "Email-based identification and authentication: An alternative to pki?" *IEEE Security & Privacy*, vol. 99, pp. 20–26, 2003.

[4] B. Welch, "Exploiting the weaknesses of ss7," *Network Security*, vol. 2017, pp. 17–19, 2017.

[5] S. Das, E. Hayashi, and J. I. Hong, "Exploring capturable everyday memory for autobiographical authentication," in *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp'13)*, 2013, pp. 211–220.

[6] A. Hang, A. De Luca, and H. Hussmann, "I know what you did last week! do you?: Dynamic security questions for fallback authentication on smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI'15)*, 2015, pp. 1383–1392.

[7] Y. Albayram and M. M. H. Khan, "Evaluating smartphone-based dynamic security questions for fallback authentication: A field study," *Human-Centric Computing and Information Sciences*, vol. 6, p. 16, 2016.

[8] M. Just and D. Aspinall, "Personal choice and challenge questions: A security and usability assessment," in *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS'09)*, 2009, pp. 8:1 – 8:11.

[9] J. Bonneau, E. Bursztein, I. Caron, R. Jackson, and M. Williamson, "Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google," in *Proceedings of the 24th International Conference on World Wide Web (WWW'15)*, 2015, pp. 141–150.

[10] M. Guri, E. Shemer, D. Shirtz, and Y. Elovici, "Personal information leakage during password recovery of internet services," in *Proceedings of the 2016 European Intelligence and Security Informatics Conference (EISIC'16)*, 2016, pp. 136–139.

[11] F. A. Maqbali and C. J. Mitchell, "Web password recovery—a necessary evil?" in *Proceedings of the Future Technologies Conference 2018 (FTC'18)*, 2018.

[12] A. Lilly, "Imsi catchers: Hacking mobile communications," *Network Security*, vol. 2017, pp. 5–7, 2017.

[13] M. A. Conway, "Episodic memories," *Neuropsychologia*, vol. 47, pp. 2305–2313, 2009.

[14] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Know your enemy: The risk of unauthorized access in smartphones by insiders," in *Proceedings of the 15th international Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI'15)*, 2013, pp. 271–280.

[15] A. Addas, J. Thorpe, and A. Salehi-Abari, "Towards models for quantifying the known adversary," in *Proceedings of the 2019 Workshop on New Security Paradigms (NSPW'19)*, 2019.

[16] J. Bonneau and S. Preibusch, "The password thicket: Technical and market failures in human authentication on the web," in *proceedings of the 9th Workshop on the Economics of Information Security*, 2010.

[17] R. Veras, C. Collins, and J. Thorpe, "On semantic patterns of passwords and their security impact," in *proceedings of the 2014 Network and Distributed System Security Symposium (NDSS'14)*, 2014.

[18] M. Weir, S. Aggarwal, B. De Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in *Proceedings of the 30th IEEE Symposium on Security and Privacy (IEEE S&P'09)*, 2009, pp. 391–405.

[19] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, and L. F. Cranor, "Fast, lean, and accurate: Modeling password guessability using neural networks," in *Proceedings of the 25th USENIX Security Symposium (USENIX'16)*, 2016, pp. 175–191.

[20] M. Dürmuth, F. Angelstorf, C. Castelluccia, D. Perito, and C. Abdelberi, "Omen: Faster password guessing using an ordered markov enumerator," in *Proceedings of the 2015 International Symposium on Engineering Secure Software and Systems (ESSoS'15)*, 2015.

[21] 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, pp. 102–127, 2005.

[22] S. Chiasson, P. C. Van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *European Symposium on Research in Computer Security (ESORICS'07)*, 2007, pp. 359–374.

[23] S. Chiasson, A. Forget, R. Biddle, and P. C. Van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*, 2008, pp. 121–130.

[24] A. Salehi-Abari, J. Thorpe, and P. C. v. Oorschot, "On purely automated attacks and click-based graphical passwords," in *Proceedings of the 2008 Annual Computer Security Applications Conference (ACSAC'08)*, 2008, pp. 111–120.

[25] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 393–405, 2010.

[26] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in *Proceedings of 16th USENIX Security Symposium (SS'07)*, 2007, pp. 8:1–8:16.

[27] J. Thorpe, M. Al-Badawi, B. MacRae, and A. Salehi-Abari, "The presentation effect on graphical passwords," in *Proceedings of the 2014 SIGCHI Conference on Human Factors in Computing Systems (CHI'14)*, 2014, pp. 2947–2950.

[28] Z. Zhao, G.-J. Ahn, and H. Hu, "Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation," *ACM Transactions on Information and System Security*, vol. 17, p. 14, 2015.

[29] J. Thorpe, A. Salehi-Abari, and R. Burden, "Video-passwords: Advertising while authenticating," in *Proceedings of the 2012 New Security Paradigms Workshop (NSPW'12)*, 2012, pp. 127–140.

[30] A. Hang, A. De Luca, E. Von Zezschwitz, M. Demmler, and H. Hussmann, "Locked your phone? buy a new one? from tales of fallback authentication on smartphones to actual concepts," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI'15)*, 2015, pp. 295–305.

[31] J. Thorpe, B. MacRae, and A. Salehi-Abari, "Usability and security evaluation of geopass: A geographic location-password scheme," in *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS'13)*, 2013, pp. 14:1–14:14.

[32] B. MacRae, A. Salehi-Abari, and J. Thorpe, "An exploration of geographic authentication schemes," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1997–2012, 2016.

[33] 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 11th Symposium On Usable Privacy and Security (SOUPS'15)*, 2015, pp. 169–183.

[34] A. Addas, J. Thorpe, and A. Salehi-Abari, "Geographic hints for passphrase authentication," in *Proceedings of the 17th Annual Conference on Privacy, Security, and Trust (PST'19)*, 2019, pp. 1–8.

[35] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy (IEEE S&P'12)*, 2012, pp. 553–567.

[36] "Statistics canada - commuting statistics, https://www.statcan.gc.ca/nhs-enm/2011/as-sa/99-012-x/99-012-x2011003_1-eng.cfm," site accessed February 2019.

[37] J.-C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical passwords," *IACR Cryptology ePrint Archive*, vol. 2003, pp. 168–177, 2003.

[38] S. Chiasson, J. Srinivasan, R. Biddle, and P. C. van Oorschot, "Centered discretization with application to graphical passwords (full paper)," in *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC'08)*, 2008, pp. 6:1–6:9.

[39] Y. Albayram and M. M. H. Khan, "Evaluating the effectiveness of using hints for autobiographical authentication: A field study," in *proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS'15)*, 2015, pp. 211–224.