ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Study of Geographic Location Based Authentication System

Sana Dawood Khan[1], Yogeshwari S. Borse[2]

Research Scholar, Dept. of Computer Engineering, SSBT'S COET, Bambhori, North Maharashtra University, Jalgaon, India[1]

Assistant Professor, Dept. of Computer Engineering, SSBT's COET, Bambhori, North Maharashtra University, Jalgaon, India[2]

ABSTRACT: In competitive world data security is a main concern. To make the system secure there are different authentication schemes use such as text based password, graphical password, bio-matrix password. But still this traditional password may crack by an attacker, i.e. shoulder-surfing, dictionary attack. Here is the methodology proposed for security enhancement over the internet will be a GeopassNotes.The proposed system present methodologies of GeopassNote in which user has to choose a location as a password on Google map along with annotation as a password. This increase memorability, useability and authentication and makes a system more secure than previous one.

KEYWORDS: *GeoPass; GeoPassNotes; annotated location password; PassMap; RouteMap; SmartPass.*

I. INTRODUCTION

There were so many ways present to make system authenticate by using map and location .Also, there is several methods make available for the user as geographical password scheme. In pass several years we use alphanumeric passwords as we know human attract to read those books having images rather than all letters that behaviour motivate others to make image password. And then it grows so far in different kind of technology. But still there is a need to make system secure and memorable by using GeoPass and GeoPassNotes. So as proposed scheme GeoPassNotes.The idea of authenticating using a digital map was first introduced by Cheswick [12] hypothesized that digital map could be used in user authentication to create a strong yet memorable password.

"The key idea is that you have a data set with very deep data, and you have to drill down. You could drill down on a map of anything. Probably better if it's a map of someplace you've never been, so you're not tempted to pick your childhood home," said Cheswick, a scientist at AT&T research. "You could have 10 digit latitude, and a 10-digit longitude, and then you have a 20-digit password."

Computer security protocols that involve clicking on a picture instead of typing a password have existed for 15 years. While clicking on a photo does defeat hacking programs that use dictionaries to break passwords, specially designed programs have evolved over the last decade that track mouse location specifically to break picture-based passwords.

By using a map with zoom, this new method renders those mouse-tracking programs useless. Sure, the virus will know where the mouse clicks, but unless it knows that map the user is looking at, and how deeply zoomed in they are, the hacking program can't record the longitude and latitude that serve as the password.

Motivation: Based on analyses, recommend security policies and use cases for these geographic authentication systems. 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.

DOI: 10.15680/IJIRCCE.2017. 0501065

Objectives: In this paper, to investigate the effects of interference on geographic location-passwords, where chose GeoPass for study, since Thorpe et al. [10] Show that GeoPass has the most potential among location-password schemes. To design a systematic approach of exploration to achieve the goal, where it conducted a study to understand the causes and effects of interference on GeoPass.In this study,to address the following research questions.
[Q1]: How usable would GeoPass be when peoples would have to remember multiple location-passwords?
[Q2]: How prominent will the interference effects be for multiple location-passwords?
To find that interference effects played a major role in the failure of login attempts in the study, and identified the following research questions to be addressed to find a possible solution to this issue.
[Q3]: Why does interference occur in GeoPass?
[Q4]: How could reduce interference effects and improve the multiple-password memorability for the GeoPass authentication scheme?

II. LITERATURE SURVEY

At first a digital map was introduced by Cheswick [12] for the authenticating user. After that, some digital map-based authentication method have been developed. 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 automatically zooms into it ,then user repeats this process by using this new view 5 or 7 times to form a password. For successful login users must remember every box clicked. The Initial view of systems begins as a zoomed in map of the USA. A survey was reported of 50 students who used the system for an undisclosed period of time and neither security analysis of user choice on the system were reported, nor usability metrics such as resets, or login time, failed logins.

PassMap [14] is a location password system that GeoPass [10] 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. And second, the initial view of PassMap's starts at an already zoomed in map of Taiwan, whereas GeoPass's begins as a view of the entire world to avoid influencing the user.

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.

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

Al-Ameen et al. [16], [17] 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 check 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. Results show 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.

Another system is a RouteMap[18] that requires a user to click a sequence of locations on a map, which then displays a "route" and a sequence of locations becomes the user's password. The memorability of multiple password of RouteMap got compared to GeoPass by asking 30 participants to create passwords for 5 accounts on each system (i.e., each user had 10 passwords, total) and after 3 weeks, the participants were requested to login again; after 3 attempts, 88.7% and 94% of participants successfully logged into GeoPass and RouteMap respectively. The login times and security analysis weren't reported for RouteMap.

Fallback authentication using location-based security questions also studied [19], where first a user has asks 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 [19]. The information leaked by the security questions was measured by asking both strangers and known adversaries to guess users' locations given the corresponding question.

Renaud et al. [20] make comparison how users responded to traditional text challenge questions and picture-based challenges for both name-based and location-based questions. Where the location-based questions were often answered incorrectly in both cases, due to the fact that users were needed to enter a text city and country name, which lead them to a incorrect inputs by users. In GeoPass, users may input text in the search bar, but if the text is not proper then they will receive instant feedback as the map they are shown would be different than what they intended to search for. And also, when users give's input text into the search bar, they are presented with a drop-down list from which they choose 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 exact locations. Authentication through a digital map can be seen as a type of graphical password. In a 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 shown up as a hybrid graphical-text method.

III. PROPOSED METHOD

Proposed solution:

(1) To propose a novel type user authentication method named as GeoPass and GeoPassNotes.
(2) To apply, plan, and conduct test these systems to improve their interface.
(3) To compute their usability by two different user studies.
(4) To plan adversary models and attacker strategies to permit estimation of the security these systems offer when considering patterns in user choice.
(5) To calculate the first, and to our knowledge only to date, estimates of the effective security give by geographic authentication systems, using an adversary models and the user study data collected.
(6) To complete the first analysis of user's navigation patterns to better understand how they may be used to enhance future geographic authentication schemes.

IV. CONCLUSION

There are various graphical and location based authentication schemes available, but still there is threat appears in the system every day. These offer a system for geographic authentication 'Geo-Pass' along with 'GeoPassNotes' which is an extension of 'Geo-Pass' scheme ,it uses Google maps as a password for user authentication along with annotation. So that system can evaluate security and usability by two differ user studies, discovering that they both exhibit very strong and high memorability. The login times for them are longer than text passwords, it suggests it 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. To find out the annotated location passwords has the potential to be stronger than text passwords in appose of guessing attacks when proper policies are applied, thus they may be more advantageous for higher user security environments .First basic thoughts are that event-specific memories are what would make annotated location passwords memorable.

This show a direction to consider whether annotation of a randomly generated location may produce an expected result.The geographic authentication technique to explored look like a strong to remember; also explore other directions to bind this memorability while improving security, another attractive way is to explore the extent that the presentation effect which can increase security in geographic authentication systems. Also, it can explore if it use mnemonics for text passwords, then whether the memorability of geographic locations may convert.

REFERENCES

1. J. Yan, A. BlackToll, 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*, NDSS'14,23-26,page no.1-16, February 2014.

3. Shraddha D. Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil ,"Location Based Authentication: A New Approach towards Providing Security", in International Journal of Scientific and Research Publications, Volume 2, Issue 4, ISSN 2250-3153, April 2012.
4. Dheeraj Dadhich ,Vipul Kumar Dubey , Viral Patel, "map based graphical authentication", Viral Patel et al , Int. J. Computer Technology & Applications ,Vol 4 (6),1005-1009,Nov-Dec 2013.
5. Ahmet Emir Dirik , Nasir Memon, Jean-Camille Birget, "Modeling user choice in the PassPoints graphical password scheme", in Symposium On Usable Privacy and Security (SOUPS)2007, July 18-20, Page no.1-9,2007.
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*, (FC '10),25-28 ,1 January 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.C van Oorschot, "Graphical passwords: Learning from the first twelve years", *ACM Computing Surveys*, vol. 4(44), January 4, 2011.
9. S. Madigan, "Representational storage in Picture memory," in Bulletin of the Psychonomic Society,Vol.4(6),567-568,1974.
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*(SOUPS), July24-26, 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", 20 Sep 2010, http://www. livescience.com/8622-future-online-password-map.html, site accessed Mar. 2014.
13. J. Spitzer, C. Singh, and D. SchToitzer, "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*, May 2-4-2012 ASIACCS '12, pp. 99–100, 2012.
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. Mahdi Nasrullah ,Al-Ameen and Matthew Wright, "Multiple-password interference in the geopass user authentication scheme", in *Workshop on Usable Security (USEC)*'15, 8 February 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, pp. 147–161, 2015.
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.