Volume 1, Issue 7, October 2016

ISSN: 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

Authentication Using Geographic Location: A Recent Overview

Jain Diksha[1]
Department of Computer
Gangamai College of Engineering, Nagaon,
Maharashtra, India

Sonar Karishma[2]
Department of Computer
Gangamai College of Engineering, Nagaon,
Maharashtra, India

Pingale Sanjivni[3]
Department of Computer
Gangamai College of Engineering, Nagaon,
Maharashtra, India

Suryawanshi Nilesh[4]
Asst. Prof., Department of Computer
Gangamai College of Engineering, Nagaon,
Maharashtra, India

Abstract-: **The user authentication selecting locations in an online map are an emerging password schemes. We implement password schemes GeoPass and GeoPass Notes which is two geographic authentications. This scheme can overcome the drawback of security issue of password and privacy. GeoPass is the most promising such scheme because it provides satisfactory resilience against online guessing and showed high memorability (97%) for a single location-password. In this scheme, we test the user usability and location passwords security and annotated location passwords. In that, user to select a place on the digital map to authenticate with a location password i.e GeoPassNotes, which is extension of the GeoPass. In this GeoPassNotes user can authenticated by correctly entering both a location and an annotation. As compare to the location password, annotated location passwords more reliable and secure.**

Keywords: **- Security, User Authentication, Passwords, Geographic location-password.**

I. INTRODUCTION

Now days, security and privacy has been formulated as an important problem. Main area of security and privacy is authentication which is the determination of whether a user should be allowed access to a given system or resource.Geographic location-password, where the user's password is a location on an online map (e.g., Google Maps), is a recent inclusion in the studies of user authentication. Geographic location-password, where the user's password is a location on an online map (e.g., Google Maps), is a recent inclusion in the studies of user authentication. While both textual [1, 2]. To guess the password easily it creates the security problem. The security problems with passwords appear to be even worse than previously believed [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 type of issue induces new user authentication strategies that improved security and privacy. As noted by Thorpe et al. [7], the geographic location password offers unique design features, as it involves elements of recognition, cued-recall, and pure recall, in addition to a mnemonic association of a meaningful place for the user.

II. LITERATURE REVIEW

In this section, we give an overview of location password existing scheme.

J. Spitzer, C. Shingh, and D. Schweitzer,"A security class project in graphical passwords" in that scheme requires five or seven locations at different zoom levels to be selected as the location-password [8].

R. A. Khot, K. Srinathan, and P. Kumaraguru,"Marasim: 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 [9].

H. Sun, Y. Chen, C. Fang, and S. Chang,"A map based graphical-password authentication scheme," in that password scheme PassMap requires the user to choose two locations and the scheme. PassMap is a location password system that GeoPass differs from in various ways [10].

In 2013, proposed by Thore, show most potential in terms of usability and security. Geographic location-passwords is a recent category in password research. In these schemes, users select one or more locations in an online map (e.g. Google Maps) as their password. Thorpe et al. [7] have shown that GeoPass is more usable than other digitalmap- based schemes because of its requirement to click on a single location and normalized error tolerance to a given zoom level. The login success rate in GeoPass (97%) was found to be higher than that in PassMap (92:59%).

W. Meng ,"RouteMap, 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 [11].

A. Hang, A. De Luca, M. Smith, M. Richter, and H. Hussmann, "Where using location-based security questions for fall back authentication," Fallback authentication using location-based security questions has recently been studied, 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 [12].

III. GRAPHICAL PASSWORD METHODS

In this section, some existing graphical password methods are discussed. Graphical based password techniques have been proposed to solve the limitations of the conventional text based password techniques, because pictures are easier to remember than texts. It is referred as "Picture superiority effect" [13].

Graphical password schemes can be divided into three categories, based on the kind of memory leveraged by the systems

i) Cognometric (recognition-base ii) Drawmetric (recall-based) iii) Hybrid schemes

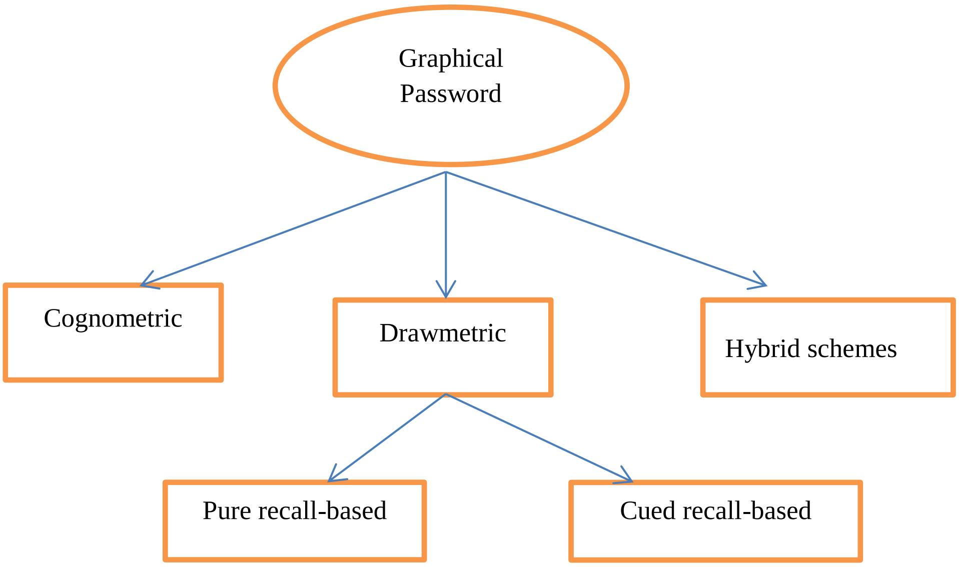

Fig.1. Categorization of Graphical password authentication techniques

i) Cognometric graphical. In this recognition-based category of graphical passwords, In this category, users will select images, icons or symbols from a collection of images. At the time of authentication, the users need to recognize their images, symbols or icons which are selected at the time of registration among a set of images. Researches were done to find the memorability of these passwords and it shows that the users can remember their passwords even after 45 days [14].

ii) Drawmetric-:

a) Pure recall-based-: In this category, users have to reproduce their passwords without being given any type of hints or reminder. Although this category is very easy and convenient, but it seems that users can hardly remember their passwords. Still it is more secure than the recognition based technique.

b) Cued recall-based-: In this category, users are provided with the reminders or hints. Reminders help the users to reproduce their passwords or help users to reproduce the password more accurately. This is similar to the recall based schemes but it is recall with cueing.

iii) Hybrid schemes-: In this category, the authentication will be typically the combination of two or more schemes. These schemes are used to overcome the drawbacks of a single scheme, such as spyware, shoulder surfing and so on [15].

IV. PROPOSED APPROACH

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% o 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.

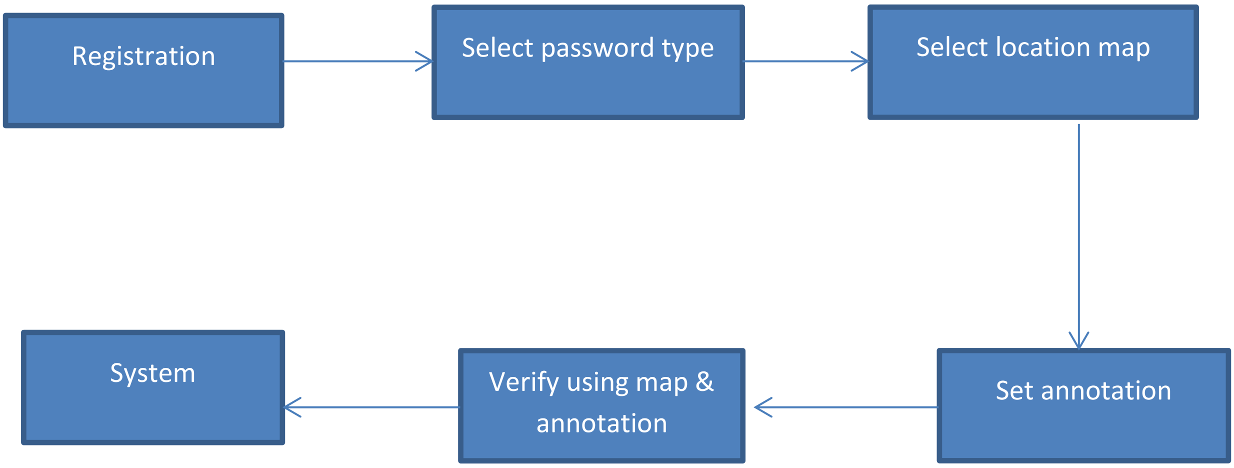

Fig.2 .System Overview

Advantages:

- 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 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.

CONCLUSION

Passwords have well-known problems relating to their memorability and vulnerability to being easily guessed by an adversary. Passwords are forgotten. To overcome this type of problems we are using location as password. Thus we can overcome password forgotten problem because people have better memory over place than the passwords. Stronger authentication. The addition of the annotation is simple but purposeful. Increase resistance to both online and offline attacks. Reduce time for searching the route between the locations. Gives accurate details about the current location. User friendly. Reduces paper works. Easy communication between user and the admin. Thus geo authentication is explained.

REFERENCES

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

2. A. Forget, “A world with many authentication schemes,”Ph.D. dissertation, Carleton University, 2012.

3. 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. J. Thorpe, B. MacRae, and A. Salehi-Abari, “Usability and security evaluation of geopass: a geographic locationpassword scheme,” in SOUPS, 2013.

8. J. Spitzer, C. Shingh, and D. Schweitzer, “A security class project in graphical passwords,” Journal of Computing Sciences in Colleges, vol. 26 (2), p.7, 2010.

9. 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.

10. H. Sun, Y. Chen, C. Fang, and S. Chang, “A map based graphical-password authentication scheme,” in ASIACCS, 2012

11. 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.

12.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.

13. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. “Influencing users towards better passwords: Persuasive Cued Click-Points”. *In Human Computer Interaction (HCI)*, The British Computer Society, September 2008.

14. K. Renaud and E. Smith. Jiminy: “Helping user to remember their passwords”. *Technical report, School of Computing, Univ. of South Africa*,2001.

15.Saranya Ramanan1, Bindhu: “A Survey on Different Graphical Password Authentication Techniques” in International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014,Issn-2320-9801,pp,7594-7602.

16.Brent MacRae, Amirali Salehi-Abari, and Julie Thorpe; “An Exploration of Geographic Authentication Schemes” in Proceedings of the 2016 IEEE Transactions on Information Forensics and Securitys, pp. 01 –16.