Volume 2, Issue 3, March 2017 ISSN (online): 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

Scrutiny of Geographical Authorization

Ms. Jain Diksha[1]
BE Student, Department of Computer Engg.,
Gangamai College of Engineering, Nagaon

Ms. Sonar Karishma[2]
BE Student, Department of Computer Engg,
Gangamai College of Engineering, Nagaon

Ms. Pingale Sanjivani[3]
BE Student, Department of Computer Engg,
Gangamai College of Engineering, Nagaon

Mr. Suryawanshi Nilesh [4]
Assistant Professor, Department of Computer Engg,
Gangamai College of Engineering, Nagaon

Abstract*: Password schemes based on selecting locations in an online map are an emerging topic in user authentication research.To make the system secure there are different authentication schemes. We design and explore the usability and security of two geographic authentication schemes: GeoPass and GeoPass Notes. 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 and makes a system more secure than previous one 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. This increase memorability, usability and authentication.

Keywords: Authentication, Security, Geopass, GeopassNotes, Digital maps

I. INTRODUCTION

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] and graphical passwords [3–4] have failed to provide a viable solution to the usability-security tension in user authentication, geographic location-password presents a promising avenue to addressing this issue. Thorpe et al. [6] presented a possible breakthrough with GeoPass in 2013. They show that this geographic location password scheme offers resilience to online guessing attacks while providing very good memorability (97%, found in a nine-day-long lab study) and high user satisfaction. People generally have better memory for images over words [4]; this has motivated many graphical password schemes that involve users remembering images (or parts of images) instead of words [5]. We hypothesize that location passwords should be highly memorable under an appropriate system design; after all, map locations are visual, and represent places. We hypothesize that location passwords should be highly memorable under an appropriate system design; after all, map locations are visual, and represent places. 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 [7] hypothesized that digital map could be used in user authentication to create a strong yet memorable password.. We developed a map-based user authentication system using the Google Maps API that we call GeoPass, in which a user chooses a single place as their password. Similar to other map-based user authentication systems [8], GeoPass makes use of the Google Maps API's search and zoom features to enable fast zooming of a digital map. Fast zooming is critical to reduce the amount of navigation required (and thus the input time, as long as these features are used). In GeoPass the user only needs to remember the location but not their method of navigating there.

II. LITERATURE SURVEY

PassMap[9] 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, PassMaps initial view starts at an already zoomed in map of Taiwan whereas GeoPasss 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. RouteMap[15] 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.

Spitzer et al.'s [10] 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. Fallback authentication using location-based security questions has recently been studied [11], 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. Renaud et al. [12] 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. Marasim [13] 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.

III. SYSTEM DESIGN AND COMPONENT

Ample options are there in now a day s operating systems it to execute applications at the remote end. The basic services used by these operating systems today promote executions of the applications at the remote end with just restricted access.

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. 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.

A. User Interface Components

The main components are the search bar, zooming options, panning options, and zoom level indicator.

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. 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.

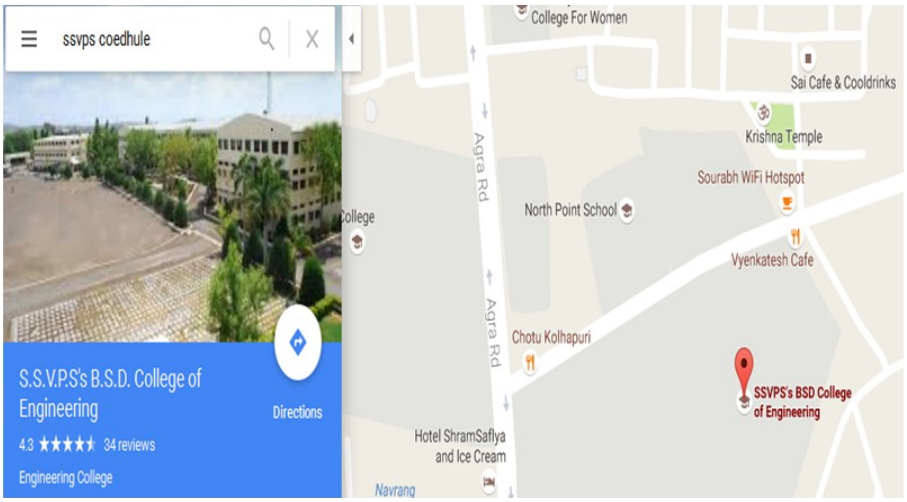
B. GeoPassNotes User Interface

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:

Note pop-up:- Once a user sets their 'X' marker, a box pops up to allow entering their annotation. 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.

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.



➢ Security threats

1) Shoulder Surfing: As with many password schemes,shoulder surfing is a possible threat in both GeoPass and GeoPassNotes. GeoPassNotes' annotation component offers some resistance as it should have similar vulnerability as a traditional text password. GeoPass and GeoPassNotes appear most appropriate to use in environments where the risk of shoulder surfing is remote.

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.

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.

IV. System Architecture

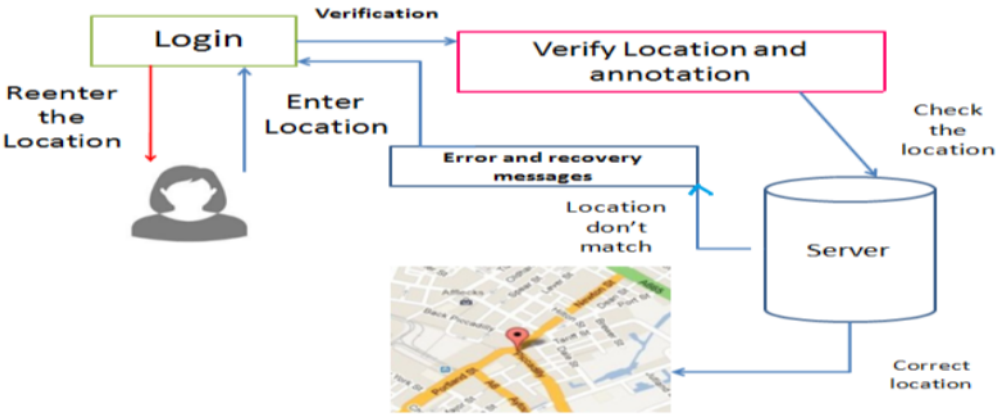


Fig.1. System Architecture

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.enter the location and if location is correct successfull login. If not reenter the location.after giving location as input the system will verify location an annotation.it will check the location through server and if correct it will login successfully. If the location doesn't match it will give error and recovery message and will allow to reenter the location.

Advantages

- It will be useful for infrequently used online accounts or possibly fallback authentication.
- GeoPass provides enough security to protect against online attacks under simple system enforced policies.
- GeoPass is highly memorable.
- The addition of the annotation is simple and it increases resistance to both online and one attacks
  It overcomes the shoulder surfing and attacks by third party map providers.

CONCLUSION

Geopass and GeopassNotes satisfies both conflicting requirements i.e it is easy to remember and hard to guess by giving the solution to shoulder surfing problem. Passwords have well known problem relating to their memorability and vulnerability.Passwords are forgotten. To overcome this problem we are using location as password. Thus we can overcome password forgotten problem because people have better memory over place than passwords. Stronger authentication. The addition of the annotation is simple but purposeful. Increase resistance to online attacks. Reduce time for searching the route between the location. Gives accurate details about the current location. User friendly. Reduce paper works. Easy communication between the user and admin. Geopass and GeopassNotes satisfies both conflicting requirements i.e it is easy to remember and hard . Thus geo authentication is explained by giving the solution to shoulder surfing problem.

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. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords,"in USENIX, 1999.
4. [4] 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.
5. R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys, vol. 4(44), 2012.
6. J. Thorpe, B. MacRae, and A. Salehi-Abari, "Usability and security evaluation of geopass: a geographic location-password scheme," in SOUPS, 2013.
7. S. Fox, "Future online password could be a map," 2010, http://wwwlivescience.com/8622-future-online-password-map.html, site accessed Mar. 2014.

8. H. Sun, Y. Chen, C. Fang, and S. Chang. PassMap: A Map Based Graphical-Password Authentication System. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS),2012.
9. 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
10. 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.
11. A. Hang, A. De Luca, M. Smith, M. Richter, and H. Hussmann, "Wherehave 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.
12. 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.
13. 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
14. M. N. Al-Ameen and M. K. Wright, "A comprehensive study of the geopass user authentication scheme," CoRR, vol. abs/1408.2852, 2014.
15. 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