International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

An Exploration of Geographic Authentication Schemes

Ashish Patil[1], Aditya Billore[2], Sagar Rao[3]

[1,2,3] *Computer Engineering, Yadavrao Tasgaonkar Institute of Engineering and Technology, Maharashtra, India*

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.*

***Key Words*: User authentication; passwords; usability; security; digital maps; map search; location-passwords..**

1. INTRODUCTION

Our project name "An exploration of geographical authentication schemes" is built on Android, java, php and wamp server. The documentation is designed for people familiar with android development and object oriented programming concept We design and explore the usability and security of two geographic authentication schemes: GeoPass—first proposed and analyzed in the preliminary version 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, 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. 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.

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 texti nformation; however, both components (location and text) are used together for stronger authentication.

1.1 Literature Survey

1)Password memorability and security: Empirical results

J. Yan, A. Blackwell, R. Anderson, and A. Grant

Users rarely choose passwords that are both hard to guess and easy to remember. To determine how to help users choose good passwords, the authors performed a controlled trial of the effects of giving users different kinds of advice. Some of their results challenge the established wisdom

2) On the semantic patterns of passwords and their security impact

AUTHORS: R. Veras, C. Collins, and J. Thorpe

We present the first framework for segmentation, semantic classification, and semantic generalization of passwords and a model that captures the semantic essence of password samples. Researchers have only touched the surface of patterns in password creation, with the semantics of passwords remaining largely unexplored, leaving a gap in our understanding of their characteristics and, consequently, their security. In this paper, we begin to fill this gap by employing Natural Language Processing techniques to extract and leverage understanding of semantic patterns in passwords

3) The true cost of unusable password policies: Password use in the wild

AUTHORS: P. G. Inglesant and M. A. Sasse

HCI research published 10 years ago pointed out that many users cannot cope with the number and complexity of passwords, and resort to insecure workarounds as a consequence. We present a study which re-examined password policies and password practice in the workplace today.32 staff members in two organisations kept a password diary for 1 week, which produced a sample of 196 passwords. The diary was followed by an interview which covered details of each password, in its context of use.

1.2 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.

2. EXISTING SYSTEM

In Existing system we use GeoPass, 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.

Like other authentication methods, the graphical password consisted of two steps, Thorpe et al. 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.

3. PROBLEM DEFINITION

Passwords have well-known problems relating to their memorability and vulnerability to being easily guessed by an adversary. The security problems with passwords appear to be even worse than previously believed. To ensure security requirements are met, unusable password policies are implemented that cause an increasing burden on users. 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. These issues motivate new user authentication strategies that have improved memorability and security.

Location privacy is an extremely important factor that needs to be taken into consideration when designing any location based systems. Revealing both identity and location information to an untreated party poses threats to a mobile users.

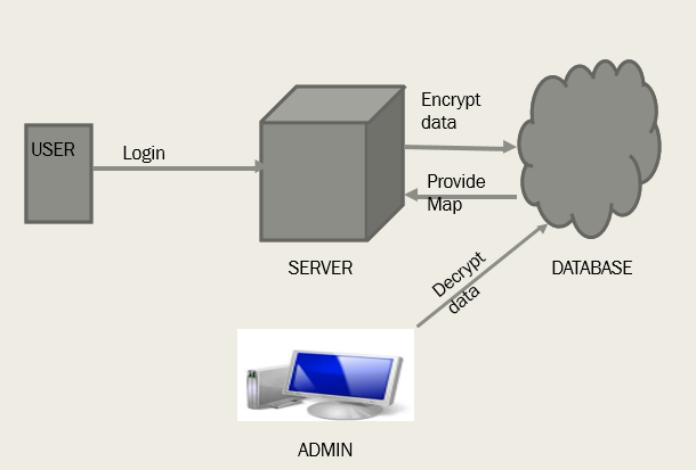
Today's location-based services solely rely on users' devices to determine their location, e.g., using GPS.In Existing system we use GeoPass, in which Geo user chooses a single place on a digital map as their password. we performed a multi-session in-lib/at-home user study of Geopass involving 35 users over 8-9 days. our result suggest that Geopass is highly memorable: none of returning participant forgot their location password after one day of 30 participants who return to login one week later only one participant failed to enter their password.

There were very few failed login attemps throught the entire study. our security result suggest that Geopass provides enough security to protect against online attacks under simple system-enforced policies may also be useful as a building block for future geographic authentication system.

4. PROPOSED SYSTEM

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.

4.1: System Architecture



MODULES:

- ❖ USER
- ❖ ADMIN

MODULES DESCSRIPTION:

1. User.

- a] geo Pass the location (Geo registration)
- b] Add geo notes to the location (App registration)
- c] View his/her own location on map..
- d] Find Route between any two locations and time taken to travel is measured..
- e] Send Passcode to admin to decrypt the location

2. Admin

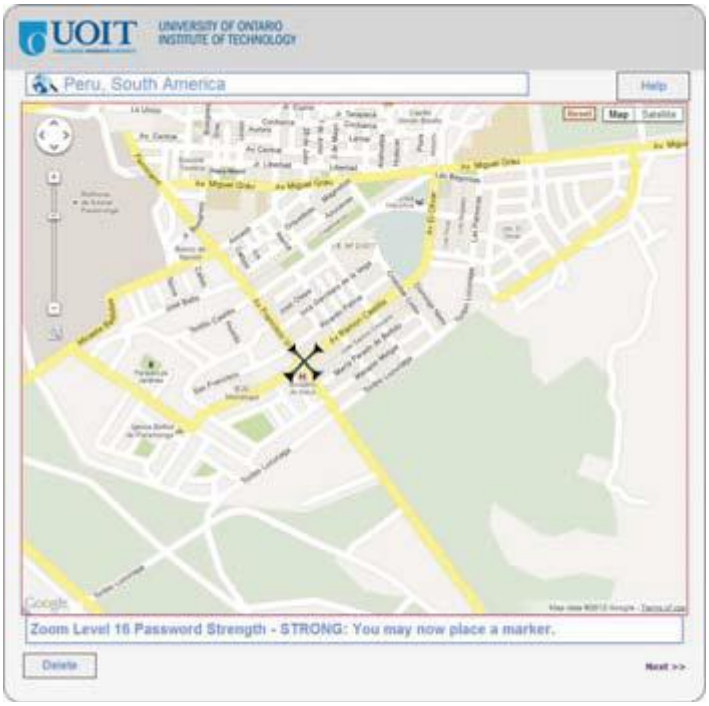
- a] View all users
- b] decrypts the location
- c] Finds distance between user location and office location.
- d] based on the distance help user in choosing transportation

We design and explore the usability and security of two geographic authentication schemes: GeoPass—first proposed and analyzed in the preliminary version 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, in which a user chooses a single place on a digital map as their password.

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.

We study annotations to evaluate the security and usability impact of adding this easily associable piece of information to the location password.

We propose, implement, and evaluate two system for geographic authentication Geopass and GeopassNotes. We evaluate the system security and usability through two users studies, finding that they both exhibits very strong memorability (over the span of eight & nine days, there were only two resets for Geopass and none for Geopass Notes).useability was high in terms of there being few failed login and user perception of the system. although 67% of the Geopass user and 80% of GeopassNotes user indicates that they could easily uses system everyday. We must be caution about recommended there use of frequently use account. Given that login times for both system are longer than text password, we suggest that they would be most appropriate in context were login occurs infrequently. for eg, it might be useful for infrequently used online accounts or possibly fallback authentication. We found that annotated location password have the potential to be stronger than text password against guessing attack when proper policy are applied, thus may be a more desirable for higher security environments.



The GeoPass system. The —X‖ marker represents the user's password.

5. HARDWARE AND SOFTWARE REQUIREMENTS

HARDWARE REQUIREMENTS:

System :- Pentium Dual Core.

Hard Disk :- 120 GB.

Monitor :- 15'' LED

Input Devices :- Keyboard, Mouse

Ram :- 1GB.

SOFTWARE REQUIREMENTS:

Operating system :- Windows 7.

Coding Language :- Android,JAVA

Toolkit :- Android 2.3 ABOVE

IDE :- Eclipse/Android Studio/Wamp

6. SECURITY ANALYSIS

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.

6.1 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.

7. CONCLUSION

We propose, implement, and evaluate an interface for map based authentication called GeoPass that allows users to choose a place as their password (i.e., a location-password). Our evaluation was in the form of a user study with 35 participants to evaluate the usability, memorability, and security of this system. Our results demonstrate very strong memorability of location-passwords (over the span of 8-9 days). Although 67% of the users indicated that they could easily use the system every day, we must be cautious about recommending its use on frequently used accounts. Given that the login times for GeoPass are longer than traditional text passwords, we suggest that GeoPass would be most appropriate in contexts where logins occur infrequently. For example, it might be useful as an alternative to secondary authentication methods used for password resets, or for infrequently used online accounts.

REFERENCES

[1] Password memorability and security: Empirical results- J Yan, A. Blackwell, R. Anderson, and A. Grant

[2] The true cost of unusable password policies: Password use in the wild - P. G. Inglesant and M. A. Sasse

[3] It's no secret. Measuring the security and reliability of authentication via secret questions - S. Schechter, A. J. B. Brush, and S. Egelman

[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] 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, 2016.

[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.