SMARTPASS: A NEW AUTHENTICATION SCHEME

USING GEOLOCATION

By

SUNIL KANCHARLAPALLI

Bachelor of Engineering in Information Technology

Osmania University

Hyderabad, AP, India

2010

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
July, 2014

SMARTPASS: A NEW AUTHENTICATION SCHEME USING GEOLOCATION

Thesis Approved:

Dr. Eric Chan-Tin

Thesis Adviser

Dr. K M George

Dr. Nohpill Park

Name: SUNIL KANCHARLAPALLI

Date of Degree: JULY, 2014

Title of Study: SMARTPASS: A NEW AUTHENTICATION SCHEME USING GEOLOCATION

Major Field: COMPUTER SCIENCE

Abstract: Authentication is critical in today's digital world. Everything from e-mail access to e-commerce to online banking requires users to authenticate themselves. The most common form of authentication used is text or character passwords. A good password is hard for someone else to guess and easy for the user to remember. Creating good passwords is a challenge.

We propose a new technique based on using a geographic location as the secret instead of characters. The proposed tool is web-based and can be used on either mobile devices or legacy machines. The new authentication scheme is very easy to use, easy to remember the secret, can easily replace the current password authentication scheme, can be deployed incrementally, and hard for someone else to guess the secret.

We performed a user-based experiment, using mobile devices, to validate the usability, memorability, feasibility, and accuracy of the proposed new authentication scheme. All of our users reported they preferred this new authentication method and feel that the new method is better than the current password-based one. On average, users took 32 seconds to authenticate successfully. Although, this is slightly higher than the current password-based scheme, the majority of the users were able to login even after four weeks, leading us to conclude that the secret selected is easy to remember.

TABLE OF CONTENTS

Chapter Page

LIST OF FIGURES

Figure Page

CHAPTER I

INTRODUCTION

1.1 Introduction

Authentication is the only method which protects information or data of an individual or organization from a second party to access. Based upon the confidentiality of that particular data or information, the level of authentication depends. Now-a-days, all this data and information what we are talking about is getting digitized all around the world. For this digitized data or information to be secure, a proper authentication procedure must be set. This arise the need for an authentication secret which belongs to the category “Something we know” to come into picture. These secrets authenticate each secret holder as the authorized legitimate user to access their particular account. Technology is getting more advanced every day, existence and usage of online applications increase. This requires each user to remember more such authentication secrets or to reuse the same secret to access multiple accounts.

In this paper, we focus particularly on the above mentioned category that is, something we know, which is popularly used for most of the online applications. This particular category involves authentication secrets consisting of characters (text passwords). As various applications have different constraints for an authentication secret to be set depending on the level of security needed, a particular user would be having many such secrets to remember. Thus, it becomes harder to remember all different authentication secrets for any individual. Even if remembered, the user might have a good chance of getting confused with which particular secret associated with which login. Many individuals, to remember the authentications secrets, might even have to make a note of them or save them in a secure place unless the secret is very familiar and easy to remember. This would lead to transformation of category from "something we know" to "something we have" which is a physical thing. This would increase insecurity of the information further if someone had access to that particular file and might even make it easier for hackers to crack if it is very obvious to guess respective to that particular user.

Our contribution to minimize the above mentioned vulnerability is to introduce a new authentication scheme; SmartPass, that works for both legacy systems and emerging systems. SmartPass is a web based application, which provide a way for the secret to be easy to use as well as to remember and hard for an adversary to guess. This application is compatible for both regular PCs and mobile devices. More specifically, the secret will be a geographic location on a map where a user can set any geolocation (latitude and longitude) of his/her interest as an authentication secret.

As smart-mobile devices are more popular these days, to know the experience and acceptance of a user, initially we have tested the application on a smart mobile device expecting that it would provide same or even better experience and results for a user using a desktop version. The user testing of the application was conducted in different sessions where each participant is asked to take an entry survey just for once(first time), to gather the basic details and his method of selecting or using an authentication secret both for mobile as well as desktop login. After registering the secret, the user is asked to login into the same application after a day, 2 days, 3 days, a week and a month. In these particular sessions, each time the user logs in into the application he/she is requested to complete an intermediate survey for the progress analysis. And at the last session i.e., on the day a month after the registration, an exit survey is taken from each participant for the overall opinion from them.

The analysis of the results and feedback given by each user is gathered and sectioned according to two groups created based upon the approximation allowed to login and was documented and presented for the conclusion. The system works well in both mobile and desktop environment. And the results from the above experiment are very positive towards the respective proposed approach. All the participants were able to use the application with ease and also were able to locate the secret to login after the registration process. Though participants have taken some time to get acquainted with the new system they were able to remember the location with a very minor error deviated from the error bound every time they fail to login. Overall every participant have managed to login into the application within a minute and an average of just 30 seconds to login.

CHAPTER II

RELATED WORK

2.1 History of Passwords:

I say authentication is necessary only if something have a restricted access or to restrict the access to that particular something. Here the something can be anything in matter. In olden days, we would just have locks to everything before computers, which were the basic and sufficient enough security system for authentication. When these locks became easier to unlock, the need to a better authentication system was very much in need to be found. This evolution of authentication systems has continued over a large period where mechanics have played a crucial role in the "something we have" category. As a revolution, computers came into existence and the start of digital world occurred. This increased the need to have a better system which happened to be the next advanced category "something we know", in the form of an authentication secret even for all online applications.

When a user is given an option to pick a password, he just wants the password to be so simple that it would be too easy to remember and at the same time it would be too obvious to guess [6]. This makes the secret very easy to crack and reduces the level of security. In order to overcome this, organizations have placed constraints for choosing a password and wanted it to be more random [7]. This makes the passwords complicated, lengthier, unique, and the most important thing harder to remember. Password's entropy gives us the measure of its strength [8]. Even if the entropy is too high for a complicated password, there is a possibility that the password fall into most common repetitive passwords and could be guessed quickly by a password cracking algorithm [9]. Here, one of the factors has to be compromised to have a greater level of security.

One cannot compromise on security provided by the password but there is a possibility of increasing the rememberability of such secure password by changing the type of it. Human psychology says that images can be remembered more easily than a character sequence [3]. Based on this, a lot of approaches were introduced in the name of graphical passwords which are discussed below in comparison to our approach.

2.2 Graphical Passwords:

There are many types of graphical passwords [10]. These passwords categorized by the kind of memory leveraged by the scheme are (i).Recall-based, (ii).Cued recall-based (iii).Recognition-based.

Recall-based passwords, also known as drawmetric, are those which have to be redrawn on a grid. Example schemes include Draw-a-Secret (DAS) [11]. Cued recall-based passwords are those which ask the user to accurately click on the same point on an image. These passwords are click-based graphical passwords or locimetric. PassPoints [12] is one of the examples of this kind. Recognition-based passwords, also known as cognometric passwords ask the user to recognize the images belonging to the set of password images from a set of distracted images. PassFaces [13] is one of the examples of this category.

2.3 Map Based Passwords:

The graphical approaches discussed earlier which are having a static predefined image and asking user to choose one or more among them would be like restricting the user from having a different authentication secret. Rather, SmartPass, the authentication approach discussed in this paper uses Google maps to have an optimum way which has the ability to show all parts of the world and allowing the user to navigate to particular place of interest. As per the study, the map location based authentication secrets are used by Spitzer's system [1] in a security project in graphical passwords, another system called PassMap [2], and a very similar application to our study called GeoPass [4].

Spitzer's system makes the user to select multiple locations on a map at each level of zoom of North America to get authenticated whereas our approach asks the user to remember a single location. In SmartPass approach, we have an additional search box to select a location that user already knows and zoom in and zoom out functionalities can be made by pinch zoom or by a single tap to zoom in.

PassMap, which asks the user to remember two locations as their authentication secret allows the user to choose a location even at lower levels of zoom whereas the SmartPass approach allows the user to zoom in up to level 15 and restricts him not to zoom in further and allows locating the point only at that particular level. PassMap does not normalize about the error tolerance at any of the zoom level whereas our proposed approach has a particular error tolerance explained clearly at zoom level 15. Upon search, PassMap zooms into zoom level 18 whereas SmartPass approach takes the user to zoom level 15 or lower depending upon the search criteria where the user can directly locate a point or zoom in further up to zoom level 15 to set the authentication secret.

GeoPass application is very similar to SmartPass approach proposed except with some enhancements in our method. GeoPass allows the user to zoom in to the maximum level and allows the user to choose a point at any zoom level at or after zoom level 16 whereas our approach gives the user to zoom in only up to zoom level 15 where each and every user has the same chance for selecting the authentication secret and after selection, GeoPass just places an X marker at the respective point but the proposed approach plots a marker and shows the user the latitude and longitude values on a balloon on top of the marker for a better experience. In addition, the SmartPass approach discusses the possibility of having the application even in a smart mobile device and tests it under all the test cases possible.

CHAPTER III

IMPLEMENTATION OF THE NEW APPROACH

SmartPass application is a browser-based authentication system developed using PHP, JavaScript and Google maps API. Discussing about the Google maps, it has zoom levels from 0 to 21 where zoom level 0 is the minimum level showing the compete world map multiple times on a very small scale and zoom level 21 is the highest possible zoom which shows even every street view for a particular area. SmartPass uses a minimum zoom level 2 where most of the world map is shown just once. Starting from zoom level 2, user can zoom in using the default options provided by the maps API till he/she reaches zoom level 15. At this level, the user is restricted to zoom-in further and is allowed to select the location for being the authentication secret.

The point behind choosing zoom level 15 particularly is because at this point, the user will be able to have a good look of what exactly the selected area consists of. At zoom level 15, the map shows major street names and places by which the user can easily recognize and navigate to any place he/she wishes to choose or locate. The statistics comparing zoom level 15 to its lower and higher levels will be discussed later.

3.1 Registration Procedure:

The home page has a simple text field named “Username” which asks the user to enter the individual’s unique username and two buttons named “Register” and “Sign In” whose functionalities are defined by their names as shown in Fig. 1.

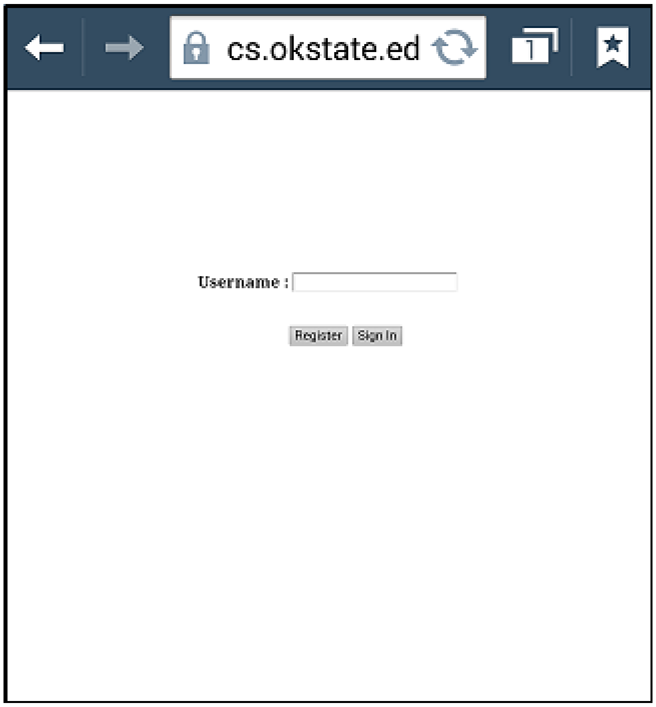


Fig. 1 Home Screen

After entering his unique username, when the user clicks on “Register” or “Sign In” button, the user will be navigated to the next page containing most part of world map at zoom level 2. Here the user can zoom in into his/her respective place of interest until the maximum allowed zoom level and will be able to select a place to register as well as locate the already set authentication secret for login. This page at zoom level 2 is shown in the Below Fig.2.

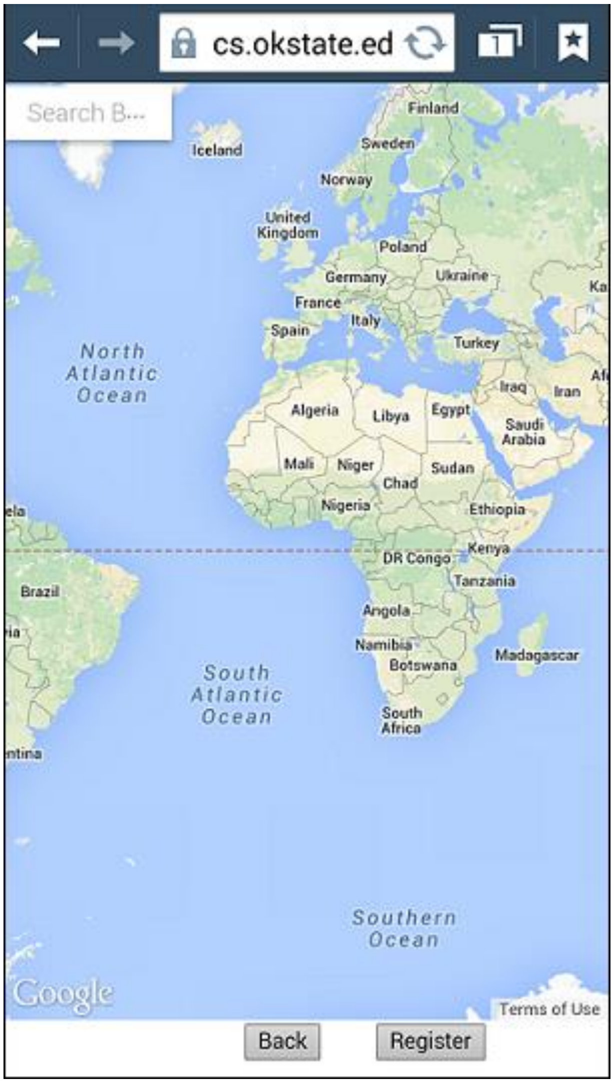


Fig. 2 Registration page

In the registration page, it has a search box to top left corner and two buttons at the bottom center of the page namely “Back” and “Register” whose functionality is defined by their name. The user needs to select a location of his/her interest by zooming in with any of the options provided into the map till the maximum allowed zoom level is reached.

The search box in the page serves the functionality same as that of the search box in Google maps which suggests the places when the user starts typing. After typing the name of interest and selecting the location from the suggestions, the map shows the particular place at the maximum zoom level set. In case the user types a very common name such as a country name like “United States of America” or “India”, the map get zoomed to a level less than the maximum possible as the search criteria is very huge by showing the respective place. Here the user needs to zoom further so that he reaches the maximum level for the selection or locating the authentication secret.

After reaching the maximum level of possible zoom at the user’s area of interest, selecting a location by tapping sets the authentication secret. A marker is placed at the place selected and the latitude and longitude values are shown on a balloon above the marker informing the user that he/she has selected the particular values as authentication secret. However, the user need not have to remember these values to login into the application. The scenario is shown in the below figure Fig.3.

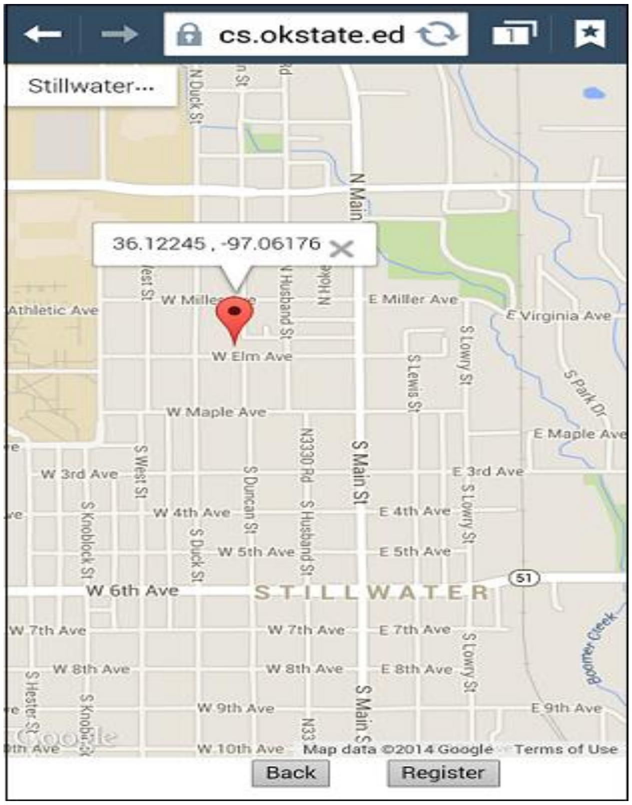


Fig. 3 selecting the authentication secret at zoom level 15

“Back” button of the page takes the user to the home page again if he/she changes mind to go back after entering the registration page. After selecting a location as authentication secret, upon clicking the “Register” button the registration process will be completed and the user is navigated to the registration success page.

3.2 Login Procedure:

Once the registration is complete, the particular user gets a chance to login into the system to access the contents. For this, the user needs to click on “Sign In” button on the login page entering his/her respective username correctly. After the click, the user is navigated to the similar page used for registration except for the “Login” button instead of Register button. All the other functionalities of the page are the same corresponding to the registration page. Clicking the “Login” button does the validation of the user with the values registered. If the values match with the registered one, it will display a page showing the success message.

3.3 Validations

As SmartPass is a browser application, user may have a very good chance of making a mistake and each possible mistake is handled accordingly with an appropriate error message. Starting from the login page, user must register before signing into the application. If the user tries to sign in before registering, the application validates with the username entered and displays “Username does not exists. Please register first to login”. And if the user tries to register with a username which is already registered before, the application does not allow a duplicate registration and prompts the user the with proper error message and to try registering with another username.

If the user clicks "Register" button without selecting the authentication secret, as the system should not allow null values as the authentication secret, it will show the respective error message saying "Please select a location of your interest to set as authentication secret" while registering and "Please locate your authentication secret to login" during login. The last step in the procedure of new authentication approach is to locate the exact point on the map to get the access to application. If the user fails to locate the point that was set as the authentication secret at the time of registration, the application gives the respective error message "Login Failed. Please try again" with a link to get back to the home page.

3.4 Error Tolerance

What if the user is unable to locate the exact point? It is difficult to any user to locate the exact coordinates again on the map. This could be resolved by allowing an optimized error tolerance around the selected or registered coordinates. Error bound allows some reasonable error around the actual authentication secret so that the user is authenticated to login. This allowable error tolerance should not be very big making the secret weaker and also should not be very small making it difficult to the user to locate. So, as the user uses his/her finger when used on a mobile device, the approximate area covered by the index finger touch is chosen as the error tolerance and is explained digitally in the further discussion.

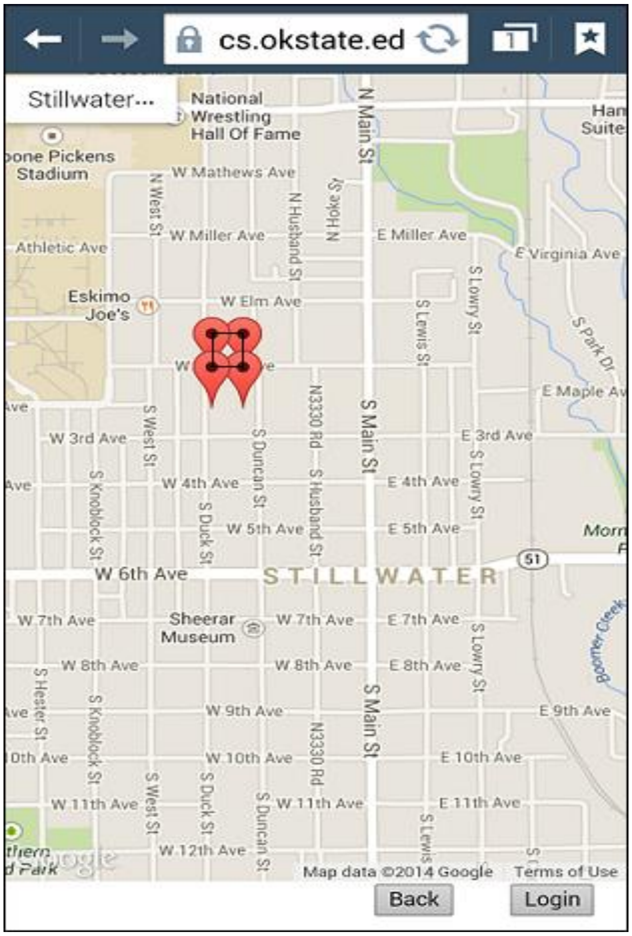


Fig. 4 Figure showing the error tolerance around the authentication secret

Fig 4, shows the error bound where, if the user selects the center of the square as his/her authentication secret at the time of registration, the application allows the user to login if the user clicks anywhere inside the box with the respective point as center of it. Here the error tolerance is 0.00040 (measures 243 feet on ground)[5] which allows the user to an error at most 0.00040 in both latitude and longitude as error from the exact point that was set as the authentication secret.

The area inside the square which is shown around the authentication point is called the allowable error area. If this area decreases, then the number of un-overlapped error bounds per page will increase. As the scale at zoom level 15 is 1:36112, at any particular time, the horizontal length of the screen measures to 6.2* 36112 centimeters or 1.4 miles and a vertical length of 9.5*36112 centimeters or 2.14 miles when measured on Samsung Galaxy S4 mobile. This varies on the device the application is launched.

3.5 Statistical Comparison:

Factor\ Method	**Number PIN (4 digit)**	**Text password (8 character)**	**SmartPass**
Possible choices	**10000**	**21834 x 10^{10}**	**20000 x 10^{10} Graphically & 40000 x 10^{10} mathematically**

Table 1. Possible number of choices for various authentication procedures used

Table 1 shows the total number of possibilities for different authentication procedures discussed in the paper. A 4 digit number PIN has at most 10^4 i.e., 10000 choices as an authentication secret. A character password of length 8, including lower case, uppercase and numbers has 62^8 i.e., 21834 x 10^{10} possible choices which is clearly very difficult to crack compared to a 4 digit number PIN.

Compared to the new approach discussed in the paper, at zoom level 15, the coordinates of map area recorded on a Samsung Galaxy S4 at the 4 corners shown on the screen are 36.12037, -97.05163 (top right); 36.12045, - 97.0667 (top left); 36.10127,-97.06696 (bottom left); and 36.10123,-97.05168 (bottom right). Considering only the 5 decimal places of precision in latitude and longitude values, the user has approximately 1533 different longitude values and 1921 different latitude values possible which multiply to around 3 million possibilities of having a unique password. The land area covered on screen at zoom level 15 is just 7.67 km^2 compared to the total area on earth which is 510 million km^2. Calculations come around 20000 x 10^{10} total possible authentication secrets, which is very near to the number of possibilities of an 8 character password which makes it equally difficult to guess.

Though the mathematical permutation calculations shows that we could have even more possible number of secrets as the latitude and longitude can have 7 and 8 possible digits with a negative and positive symbol possible for both. This comes to 4 x 10^{15} possible values for latitude and longitude. Together from the above calculations and calculations based on the area of the earth, the possible choices is nearly equal or more than an 8 character password. The number of possibilities of choices can be further increased in SmartPass approach by increasing the precision of latitude and longitude values. Increase in 1 additional digit will have a lot more possibilities of authentication secrets possible; however, it is a little difficult achieve that precision on a mobile device.

The number of passwords per screen depends on the zoom level the map is in. If the zoom level is decreased, we can have more number of passwords per screen but the clarity of the screen has to be compromised. Similarly if the zoom level is increased, the number of passwords per screen will decrease but in both the cases, the total number of possible passwords around the map remains the same.

CHAPTER IV

TEST DESIGN AND IMPLEMENTATION

The proposed approach is a browser based application compatible for both desktop and mobile devices. Human participants were required to evaluate the feasibility and practicality of this application. Technically this kind of testing is called the user testing which involves people from various backgrounds. As this user testing experiment involves human subjects, IRB approval was obtained. Additionally, a respective questionnaire at each session of testing was prepared for gathering some basic details about each user for the statistics purpose and to get feedback from the user about the usability of smartPass application compared to current authentication system.

4.1 Test set selection:

To choose a set of test-group subjects, we have approached graduate students of Computer Science department to volunteer participating in the survey for testing the application. The reason for choosing graduate students is, in the previous online survey a higher response rate from the graduate students was received for survey participation than undergraduates. From the group of people who volunteered, we have taken the first 20 members into consideration. The reason behind taking a smaller set of people is, as the researcher has to be with the participant to make a note of comments and procedure followed by the participant and that we have decided to have only one participant involved in testing. For the sessions to be performed on successive days, this particular group of 20 is sufficiently large for this initial stage of testing. This design with this particular test set is specifically to find the capability of the application to get acceptance of the people and to know if the approach works well for a smaller.

4.2 Demographics:

The test set contains group of people from the same category of age 20's and all the people are graduate students at Oklahoma State University. All the students chosen are from Computer Science majors because the participants have to visit the department often for the first week and after a month later. Most of the participants are from India as we have a number of Indians in the respective department.

As this kind of group is more involved in internet activities, there might be a possibility for remembering the password more efficiently for this group, when compared to the people from higher ages and different backgrounds. There might be a possibility for the results to be biased. This biasness will be nullified by having a larger group of participants with different backgrounds and different ages in the further stages of testing the application.

4.3 Organization of the experiment:

As proposed, the experiment was scheduled to be conducted in 6 sessions. The experiment was conducted in a closed environment lab which is located in the computer science department for one participant at a time. This is to avoid any disturbances for a participant and particularly to make sure that each of the participants is having the same kind of environment around them while taking part in the experiment. For session1, which is on day 1, has an entry level survey questionnaire for each participant having the basic details of the participant and his previous experience with authentication system. Each participant is made to know about the IRB approval taken and the conditions mentioned in it. Participant has also been informed that any data related to him/her would not be public and is protected in a secure file. After demonstrating the sample application using the test link, the participant is made to register into the application. After registering the secret, the user is also asked to login into the application. During the registration and login process, the method the participant uses to choose the location of interest as authentication secret like using the search box, using the zoom in and zoom out properties, or using the panning property of the map is also noted for analysis purpose. The time taken for the participant for registration and login are recorded programmatically for analysis.

Session2 of testing will be on the next day of registration, where the user is asked just to login again into the application. After the login, the user is asked to answer the intermediate questionnaire where the details of number of attempts taken to login, opinion towards the new approach, the way the participant used to remember the secret. The same process is followed through session3 session4 and session5 on day 3, day 4 and day 7 respectively considering the registration day as day1, the next day after registration as day2 and so on. For session6 on day 30, an additional exit interview questionnaire is taken from each individual regarding the overall experience with the application.

4.4 Testing the Error Bound:

We have made the authentication secret easier to remember by making the user to choose a location instead of a character sequence. Now we need to make sure the user should be able to plot the authentication secret while login in an easier way. We have defined a term error bound around the same point of location as it will be most difficult task for a person to select again to login into the application. The next important thing is to set a comfortable error bound which would be sufficiently small for the secret to be secure. As the application is tested mainly on the touch interface (smart mobile interface), considering most of the users uses their figure tip to plot a location on the map, the impression of impact to the screen is taken as the measure of error bound to be defined.

To test this comfortable error bound, we decided to test the application on two different error bounds, one with a lesser error bound (0.00025 i.e., difference between the plotted coordinates and registered coordinates cannot be greater than 0.00025), and the other with larger error bound (0.00050) whose average is very close to the area covered by the impression of index figure mostly used for touch on a smart mobile and should also be good enough for mouse click on a desktop version. To support this, we have designed two different applications whose functionality is the same except for the tolerable error bounds. In the process of testing these two applications, the whole group of participants was further divided into two groups of 10 each and was assigned to different error bound application. The division of these groups is made in the order the people who came to participate alternatively into each group. This approach particularly is to study the accuracy, easiness and most comfortable error bound for the application. The members were uninformed about the applications error bound they are logging into, so that every user pays the same attention to login and to obtain genuine results.

The tested error bounds were shown below with the boundaries corresponding to them.

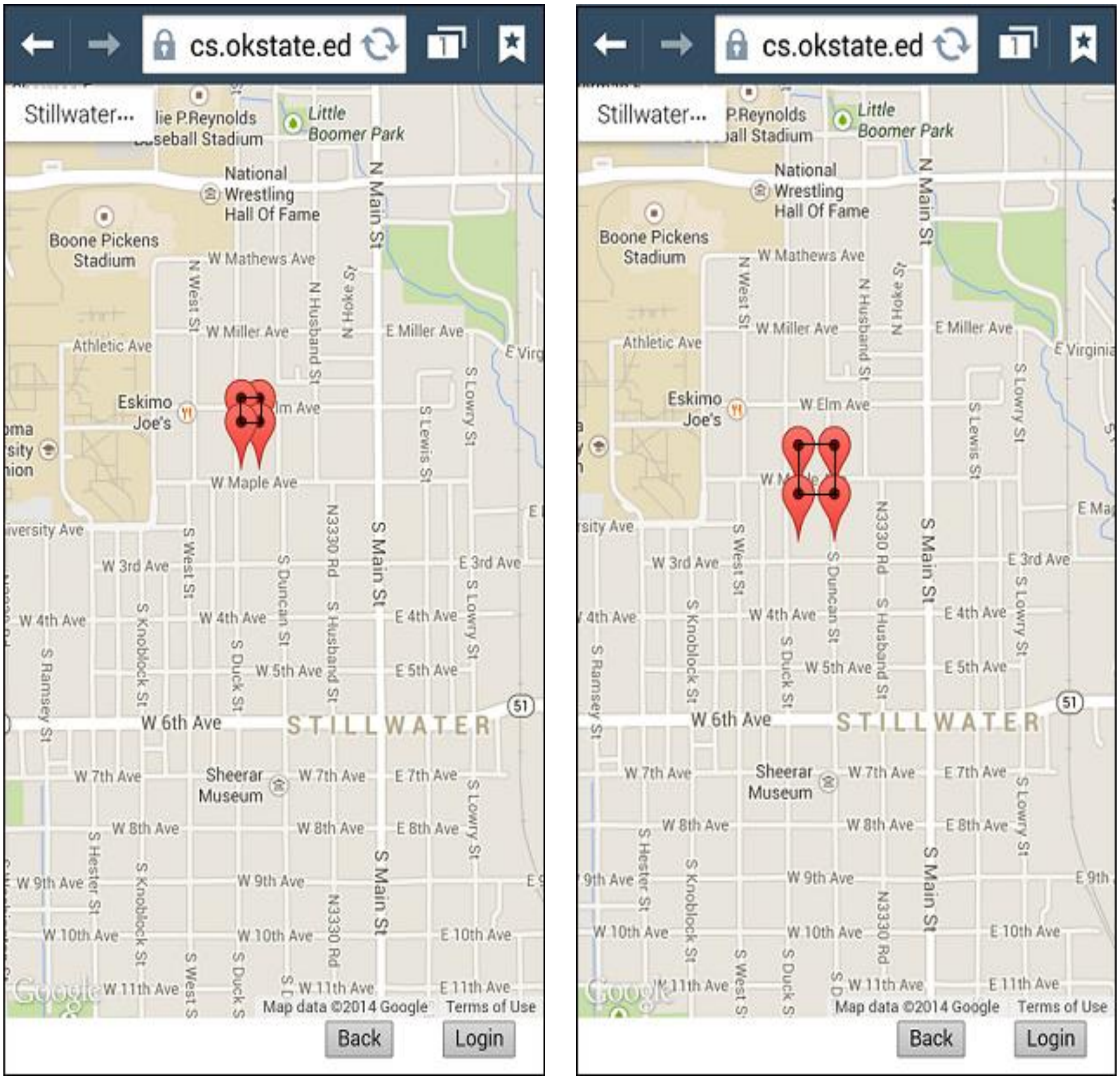


Fig 5: Boundaries showing smaller Error bound (0.00025 precision) and larger Error bound (0.00050 precision)

CHAPTER V

EVALUATION

5.1 Importance:

Evaluation is the most important part for an application. Even if the application has many advantages technically, it has to be accepted by the people and should come into usage. Coming to our application, it is a web based application where a user testing is a must to know its chance of acceptance and success in the real world. This kind of application needs to be tested on a wide range of participants with different age, sex, professions and practices. Analysis of the feedback given by each user leads to the evaluation of the approach introduced about how a real user feels experiencing the new approach as the new authentication system. This analysis is done based on the number of results in favor of and against the application.

5.2 Analysis:

Analysis is done based on the feedback given by the participants, the results got from the experiment programmatically and notes that have been taken during the experimental procedure.

5.2.1 Entry Survey Analysis:

For the entry level questionnaire where the general information of the participant is involved, some of the interesting factors derived from them are given below

1. 100% were using a Smartphone where 60% have a number pin, 20% have text passwords and 20% have pattern as authentication to access their mobile devices.
2. 80% need an authentication on their device to protect their information from others
3. 80% of the participants login more than 10 times into a computer or a website or an application or a mobile device or other electronic system approximately and 20% for just 5-10 times.

   Note: This high percentage might be due to the biased group of students who would be more frequently logging into their email accounts and college website both on a desktop as well as in mobile device.

4. 50% use a unique password for each website or device, 40% use the same password as often as they can, and only use a different password when required and 10% use unique passwords on only the most important sites and services.

   Note: Here 40% of the participants use the same password as often as they can and this reduces the number of passwords to remember which makes the text passwords easier.
5. 100% would think up a new password for themselves when an application gives them a choice of selecting a password.

6. While registering into a new website or service, 60% would make their own unique password, 30% use a variation on a password they already have and 10% use the password they already have.
7. 90% think remembering the password is easy and 10% think that it is moderate.

   Note: Remembering a password is easy to a high percentage of the group as all the members of the group are in their 20's, their profession and their access to the most recent advanced technology.
8. 60% have to keep track of 9-20 different passwords and 30% to keep track of 4-8 and 10% to keep track of 1-3 different passwords.
9. 80% remember the passwords they keep track of and 20% don't.
10. 100% would like to have a new way of authenticating system.

From the above results, though it is easy to remember a password to most of the participants, they want to have a new way of authentication. After introducing the application to these participants and registering the authentication secret for the first session, the feedback given concludes the following results summary is as follows

All the participants think the application is definitely user-friendly or just user-friendly and setting the authentication secret is easy or very easy. All of them have thought that the application is easier than character password and would be secure or very secure compared to the character password. All the participants have voted that the respective approach is as good or very good.

5.2.2 Intermediate and Exit survey Analysis

The intermediate survey questionnaire which is taken at the end of each session after the user has tried to login into the application using the registered authentication secret from Session2 until Session6. This questionnaire involves the questions which evaluates about the factors that are to be compared with the existing system namely, memorability, accuracy and easiness. This intermediate survey results are different for the two different groups as the error bound was different. The following table, Fig.5, and Fig.6 describe the analysis of the intermediate survey results.

Question/Factor	Group1	Group2
Do you remember the secret	100% yes for all sessions	100% yes for all sessions
How did you remember	100% just memorized for all sessions	100% just memorized for all sessions
How easy is to remember the secret	100% easy or definitely easy for all sessions	100% easy or definitely easy for all sessions

Table 1. Intermediate survey common questions over all sessions and responses

The above table summarizes the answers of all the users of both groups for all sessions. All the participants have remembered the secret and just memorized it and think that the respective approach provides an easier way to remember an authentication secret.

The computer science department hosts a few servers allowing ssh access. Authentication is performed through username and passwords. We parsed the ssh logs and evaluated the number of attempts needed for a user to login. We found that 90% of users can login with one try but close to 10% of users have at least one failed attempt. This shows that our proposed scheme memorability is comparable to current authentication schemes.

Moreover, all the users login to ssh servers at least once every day to compile an run homework programs and to submit their homeworks.

Fig.6 shows the graph where the percentage of participants is plotted against the number of attempts taken on each session marked as Day2, Day3, Day4, Day7 and Day31 respectively. As the participants don’t know about the error tolerance exact value and boundaries they are logging into, the first login session gave poor percentage of logging at single attempt. Gradually, the participants are more habituated to the location password and were able to locate the secret without any difficulty which is clearly shown in the graph i.e., on Day7, 90% of the participants from group1 were able to login on the first attempt.

On Day31, the number of first attempt logins decrease as the participants have almost 3 weeks of gap between the login. Still all the participants were able to login by the third attempt and 80% of them were able to login within 2 attempts. No participant has said that they don’t remember the authentication secret. The reason for the failed login is due to the error bound and time gap between the previous login.

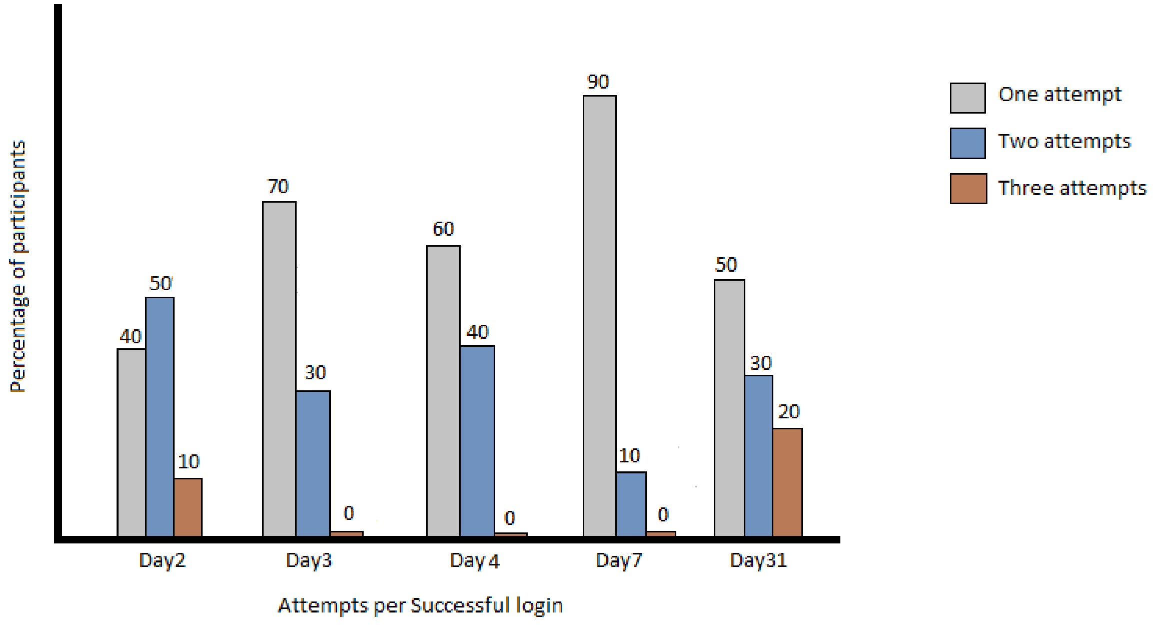


Fig.6 Group1 analysis of successful attempts

Fig.7, similar to Fig.6, which is the analysis of the results taken from the second group feedback, having smaller error bound, took more number of attempts by more number of participants for them to login into the application. This group does have a considerable improvement where, by the end of the session3 i.e., Day4, all the participants were able to login within two attempts. Still some of this group participants suggested that the error boundary could be increased by another fraction so that it could be more comfortable to login.

On Day31, same as in the case of the Gropu1, this group also had a tough experience with login into the application in the first attempt or second. Even though, 80% of the group was able to login by the second attempt which is equal to the Group1's performance.

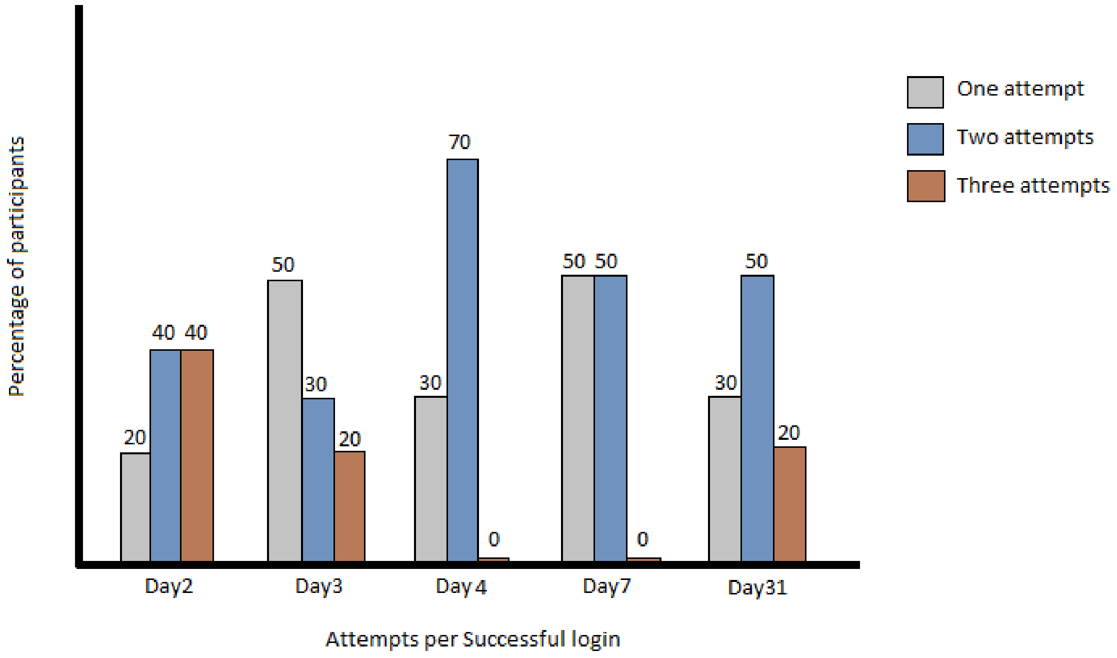
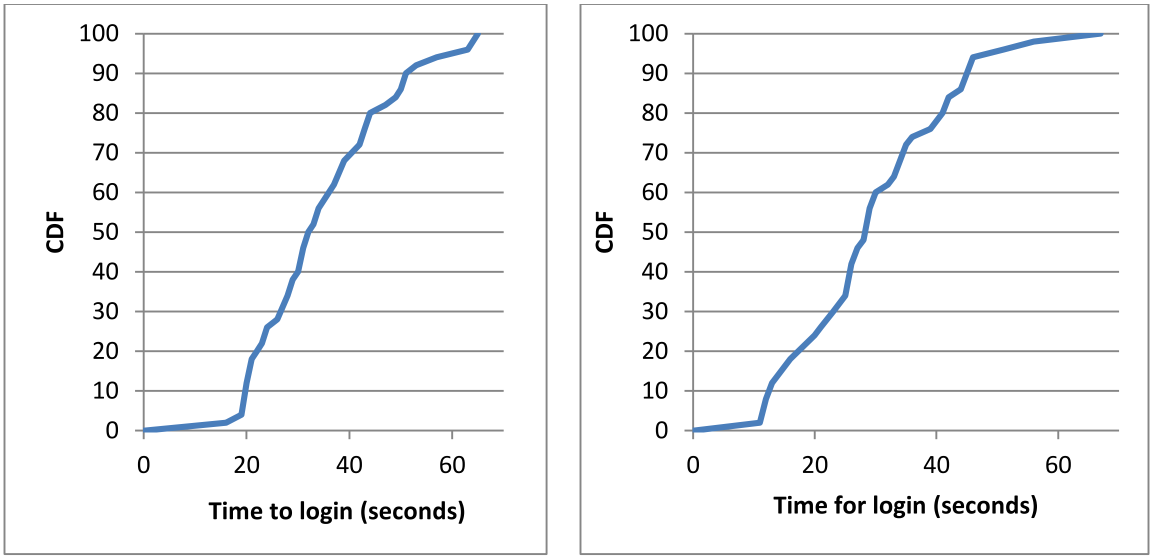


Fig.7 Group2 analysis of successful attempts

5.2.3 Cumulative Distribution Frequency (CDF) Analysis:

The second thing that needs to be considered in this kind of graphical passwords is the time taken for a user to successfully login into the application. This time is programmatically calculated when the user enters into the authentication selection page and till the time he clicks on the login button. These timings were recorded into a separate text file for each respective group to have a separate analysis of the results. The following figure shows the CDF of time taken by a participant to exclusively locate his/her authentication secret for Group1.



(i) **(ii)**

Fig.8 Cumulative Distribution Frequency Analysis of Group1 and Group2 test set

Fig.8 (i), shows that a participant takes a minimum of 16 seconds for a user to reach his location and to plot the secret and a maximum of 67 seconds at least for the conducted sessions of application testing. As these results were gathered over a month with 5 sessions, a total of 50 records have been recorded and used as the data set. Among these 50 records, 50% of the people were able to login into the application within a 34 second period of time which is significantly small when compared to the procedure followed for clicking the forgot password link, getting an email for resetting the password, and then logging into the application. This duration of 34 seconds is an average time taken by all the participants. It could be more or less depending mostly upon the method used to reach the location after entering the authentication page, and on location of choice and memory to a little extent. As described earlier, as images can be remembered easier compared to text, this would be easier to even remember than a character password.

Fig.8 (ii) shows the CDF representation for the login timings for Group2 which is having a lower error bound compared to Group1. As said earlier, the login time depends upon the method of searching the location of interest mainly. Once the user goes to his particular location of interest, it doesn't take much of time to locate the secret and to click on the login button.

Method used	**Time taken(seconds)**		**Percentage of users**
	Min	**Max**	
Tap Zoom & pan	21	64	45
Pinch zoom & pan	28	67	15
Search box & pan	11	39	40

Table 2: Methods used for searching the location of interest

Table 2 shows the analysis of minimum and maximum time encountered from all the users for a respective method for searching the location to plot the secret and the percentage of participants choosing the particular method. Clearly from the table, using search box and pan allows the user to login more quickly than other methods. Though more percentage of participants used Tap Zoom & pan as their method of search.

CHAPTER VI

CONCLUSION

From the analysis of results gathered from all the sessions of user testing, it can be clearly said that all the users from the test group wishes to have a new way of authentication system and do like the presented approach to be the kind one to be replaced with. The only difficulty the user faced to locate the password is due to the error bound where the participant have plotted it a little away from the original point. But, the thing to be noticed is that none of the participants have said they forgot the password even on day 30 from the day of registration. Based on the feedback, we can affirm that the smartPass can be definitely introduced into the real world replacing the text passwords especially for mobile applications where the user will have the sole access.

One could not have a very obvious password in any type of authentication system. Particularly in this approach, one could not choose his living place or home as a password. Though locating the secret is not very easy in the approach even for guessing an obvious secret, the second person (one who is not a legitimate user) might want less number of attempts to crack it. Choosing a completely different location would also be a little difficult to remember which the user hasn't had any relation with it before. And the other possible threat would be shoulder surfing [14] where another person will be able to see the secret when registering or login and increasing the possibility to guess in that particular area. Though this shoulder surfing is minimized in mobile phones, coming to desktop applications using LCD screens with concurrent dual views [15] interacting with the system through eye gaze input [16] could prevent shoulder surfing. Upon further user testing and enhancements to the present application like adding the feature of recovering the password if forgotten, to have additional interface of the same map to choose another place of interest for strengthening the authentication procedure, there is a very good possibility of having even better results and to be more user-friendly than those encountered now and the respective approach would be ready and good enough to be implemented into the real world applications.

REFERENCES

[1] J. Spitzer, C. Singh, and D. Schweitzer, A Security Class Project in Graphical Passwords. *Journal of Computing Sciences in Colleges*, 2010.

[2] H. Sun, Y. Chen, C. Fang, and S. Chang. PassMap: A Map Based Graphical-Password Authentication System. In *Proceedings of 7th ACM Symposium on Information, Computer and Communications Security*, 2012.

[3] D. Nelson, V.Reed, and J. Walling. Pictorial Superiority Effect. *Journal of Experimental Psychology: Human Learning and Memory*. (1976).

[4] Thrope, MacRae, Salehi-Abari (2013-07-24). Usability and security Evaluation of GeoPass: Geographic Location-Password Scheme. In *Symposium on Usable Privacy and Security (SOUPS)*, 2013.

[5] GPS Latitude and Longitude Distance Calculator. http://www.csgnetwork.com/gpsdistcalc.html, site accessed February 03, 2014.

[6] D. A. Milman. Death to Passwords, December 2010.

[7] D. Florencio and C. Herley. Where do security policies come from? In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. 2010.

[8] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*. 1948.

[9] C. Ngak. The 25 most common passwords of 2012. October 2012.

[10] R. Biddle, S. Chiasson and P. C. van Oorschot. Graphical Passwords: Learning from the First Twelve Years. *ACM computing surveys*, 2012.

[11] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX SecuritySymposium*, Berkeley, CA, USA, 1999. USENIX Association.

[12] 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*, 63(1-2):102–127, July 2005.

[13] Real User Corporation. The Science Behind Passfaces. Technical report, Real User Corporation, June 2004.

[14] Julie Thorpe, Brent MacRae, Amirali Salehi-Abari. Usability and Security Evaluation of GeoPass: a Geographic Location-Password Scheme. *Symposium on usable privacy and security (SOUPS)*. 2013.

[15] S. Kim, X. Cao, H. Zhang, and D. Tan. Enabling Concurrent Dual Views on Common LCD screens. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2011.

[16] A. Forget, S. Chiasson, and R. Biddle. Shoulder surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2010.

APPENDICES

Survey Questions

Entry Survey questionnaire: (just once for a user for the very first time**)**

<You don't have to answer every question.>

1. Which best represents your gender?
   a) Male
   b) Female

2. What age group are you in?
   a) 18-23
   b) 24-30
   c) 31-40
   d) 41-50
   e) 51-62
   f) 63+

3. Have you ever taken a computer course of any type?

   a) Yes
   b) No

4. Which of the following best describes your computer/IT technical skill?
   a) I have no experience or knowledge of computers.
   b) I mostly only surf the web, use a few applications like word processing, and check email.
   c) I can use a wide variety of applications, but do not setup or manage my computer.
   d) I know how to program computers, or setup and manage my computer and install and configure devices and applications.
   e) People look to me as an expert and help with computers.

5. Do you use a smartphone regularly (such as iPhone or Samsung Galaxy)?

   a) Yes
   b) No

6. Do you require a password or other authentication to access your mobile device?
   a) Yes
   b) No

7. What kind of authentication system do you use on your mobile device?
   a) None
   b) Text password/passcode
   c) Numerical PIN
   d) Pattern
   e) Others (Please specify:)

8. If you do require a password or other authentication to access your mobile device, which of the following apply to you?
   a) I use authentication because someone else manages the device configuration for me and required it
   b) I use authentication because that's the way it was set by default and I kept it that way.
   c) I use authentication because I want to protect information on it
   d) I use authentication for another reason (Please specify:)

9. If you do NOT require a password or other authentication to access your mobile device, which of the following applies to you?
   a) I don't use authentication because someone else manages the device configuration for me and they didn't set it up
   b) I don't use authentication because I don't know how to set it
   c) I don't use authentication because I don't want to have the delay for logging in
   d) I don't use authentication because I don't keep important information on the device
   e) I don't use authentication because it's hard for me to remember login information
   f) I don't use authentication because I just have never got around to setting it up.
   g) I just have never thought about using a password or other authentication to log in to my device.
   h) I don't use authentication for another reason (Please specify:)

10. Approximately how often do you login to a computer, website, application, mobile device, or other electronic system?
    a) More than 10 times a day
    b) 5-10 times a day
    c) 2-5 times a week
    d) Once a week
    e) Less than once a week

11. Do you use unique passwords for different websites, devices, and services, such as logging in to your computer? For this question, even a single character difference makes a password unique.
    a) Yes, I use a unique password on most or every website, device, and service.
    b) Yes, I use unique passwords on only the most important sites and services.
    c) No, I use the same password as often as I can, and only use a different password when required.
    d) No, I only use one password, and I don't use services that require a different one.

12. If an application gives you a choice of selecting new password, which way do you prefer to set up your new password?
    a) Think up the new password myself.
    b) Use my own password generator to find and choose a suitable new password for me.
    c) Choose among a few password options that the system provides for me.
    d) Let the system generate and show a password to me.

13. In general, how do you pick a password when you register for a new website or service?
    a) I use a password generator to make one for me.
    b) I make up a new unique password myself.
    c) I use a variation on a password I already have.
    d) I use the same password I already have.

14. How hard is it for you to remember a password?
    a) Easy
    b) Moderate/neutral
    c) Hard

15. Approximately how many total different passwords do you use/have to keep track of?
    a) 0

b) 1-3
c) 4-8
d) 9-20
e) 20 or more

16. Of the passwords you use/have to keep track of, approximately how many do you memorize/use from memory?
    a) 0
    b) 1-3
    c) 4-8
    d) 9-20
    e) 20 or more

17. Would you like to have a new way of authenticating other than using text passwords?
    a) definitely yes
    b) yes
    c) neutral
    d) no
    e) definitely no

[Register authentication secret]

18. How would you rate the user-friendliness of the application?
    a) Very friendly
    b) Friendly
    c) Neutral
    d) Unfriendly
    e) Very Unfriendly

19. How would you rate the easiness of setting an authentication secret on the respective application?
    a) Very easy
    b) Easy
    c) Neutral
    d) Hard
    e) Very hard

20. What kind of location did you choose for the authentication secret?
    a) A place I have visited
    b) A place I really like but haven’t visited
    c) My place of birth
    d) Place where I live or once lived
    e) A place of significance to a family member or a friend
    f) A place that is famous, well-known, or in the news
    g) Random
    h) Other (Please specify:)

21. Do you think the digital security authentication approach (authentication approach used in the study) is easier than having a character password?
    a) Definitely yes
    b) Yes
    c) Neutral
    d) No
    e) Definitely no

22. How secure do you feel the digital security authentication approach (authentication approach used in the study) is compared to a character password?
    a) Very secure
    b) Secure
    c) Neutral
    d) Unsecure
    e) Very unsecure

23. How would you rate the respective approach?
    a) Very good
    b) Good
    c) Neutral
    d) Bad
    e) Very bad

Intermediate Survey Questionnaire

<You don’t have to answer every question.>

1. When did you last log in to the application?
   a) A day
   b) A week
   c) 2 weeks

d) A month
e) None

2. Did you remember the authentication secret you previously set?
   a) Yes
   b) No

3. If you have answered yes to the above question, how did you remember the authentication secret?
   a) Just memorized
   b) Wrote it down
   c) Other

4. How easy is it to remember/recall your authentication secret?
   a) Definitely easy
   b) Easy
   c) Neutral
   d) Not easy
   e) Definitely not easy

5. How many attempts did you take to authenticate?
   a) 1
   b) 2
   c) 3
   d) 4
   e) 5 or more

6. Do you think the authentication approach used in this study is easier than having a character password?
   a) definitely yes
   b) yes
   c) neutral
   d) no
   e) definitely no

7. Do you have any comments?
   [Free-form answer]

Exit Survey questionnaire: (just once for a user at the very last time**)**

1. What do you think of the alternate approach for authentication used in this study?
    a) Excellent
    b) Good
    c) Neutral
    d) Bad
    e) Very bad

2. How do you rate the ease of setting your authentication secret for the authentication mechanism used in this study?
    a) Very easy
    b) Easy
    c) Neutral
    d) Hard
    e) Very hard

3. How easy is it for you to remember the authentication secret used in this study?
    a) Very easy
    b) Easy
    c) Neutral
    d) Hard
    e) Very hard

4. Did you write down a reminder for the authentication secret you used for this study?
    a) Yes, I wrote down precise details that would allow anyone to log in.
    b) Yes, but I wrote down only a general reminder or clue to jog my memory, not enough for anyone else to know how to log in.
    c) No, I did not write down any reminder; I relied only on my memory.

5. Do you think this authentication secret is easier to remember than a text password?
    a) Definitely yes
    b) Yes
    c) Neutral
    d) No
    e) Definitely no

6. Would you like to see this authentication approach implemented for many applications?
    a) Definitely yes

b) Yes
c) Neutral
d) No
e) Definitely no

7. Would you like to see this authentication approach implemented for smartphones and tablets?
    a) Definitely yes
    b) Yes
    c) Neutral
    d) No
    e) Definitely no

8. How comfortable do you feel about the security of using this authentication approach?
    a) Very secure
    b) Secure
    c) Not secure
    d) Definitely not secure
    e) Not sure

9. Do you have any suggestions/ideas for the respective approach to become more effective and user-friendly?

    [Free-form answer]

10. Do you have any other comments?

    [Free-form answer]

VITA

Sunilmanohar naidu Kancharlapalli

Candidate for the Degree of

Master of Science

Thesis: SMARTPASS: A NEW AUTHENTICATION SCHEME USING GEOLOCATION

Major Field: Computer Science

Biographical:

Education:

Completed the requirements for the Master of Science in Computer Science at Oklahoma State University, Stillwater, Oklahoma in July, 2014.

Completed the requirements for the Bachelor of Engineering in Information Technology at Osmania University, Hyderabad, Andhra Pradesh, India in 2010.

Experience:

Graduate Teaching Assistant, Department of Computer Science, Oklahoma State University, Stillwater, OK. Jan 2014-May 2014

Graduate Research Assistant, Department of Computer Science, Oklahoma State University, Stillwater, OK. Aug 2012-Jul 2013

Systems Engineer, Infosys Limited, Hyderabad, India. Jun 2010-Jun 2012