An Efficient Three Stage Graphical Password Authentication Scheme

Mamta Bhilare[1], Amruta Bhadgaonkar[2], Swati R. Biradar[3], Pranjal S. Mahadik[4], Prof. Dr. Mrs. D. A. Godse[5]
[1, 2, 3, 4, 5] Department of Information Technology
[1, 2, 3, 4, 5] BVCOEW, Pune, India.

Abstract- *Now a day's security is the primary need of every asset. And in world of Computer systems user authentication is the primary means to protect system resources from unauthorised users. Also day by day all the methods are going to merge into shared resources pattern, due which multiple users are sharing a single asset, in that case secured authentication is necessary. Over the years, several authentication methods have been developed. The most commonly used method is the textual password based authentication, voice based authentication, biometric based authentication. In such authentication method users are required to choose a text comprising of alphabets, numbers and symbols, voice, finger print scanning and so on. Once passwords are registered with the system, users need to recall and submit it each time of their login. But textual password can be difficult to remember, similarly, biometric password can be failed many time due changes in physical characteristics. Also they need expensive devices to implement. Recently images based graphical password schemes have received the attention of researchers. Human being's ability to remember images is well established. So in this paper, another graphical secret key plan in light of geological maps is proposed. The proposed plan has got three phases of validation. Contingent on the level of security fancied, clients could choose maybe a couple or three stages. After the underlying secret word creation, clients could increment or abatement the quantity of stages whenever and they could likewise change the chose watchword in a specific stage. Client studies were led on the proposed framework to test its convenience and memorability.*

Keywords- Graphical Passwords, Authentication, security, Image, Password

I. INTRODUCTION

A graphical watchword is a verification framework that works by having the client select from pictures, in a particular request, displayed in a graphical client interface (GUI). Consequently, the graphical-secret key methodology is now and again called graphical client validation (GUA).

A graphical secret key is less demanding than a content based watchword for the vast majority to recall. Assume a 8-character watchword is important to pick up section into a specific PC system. Rather than w8KiJ72c, for instance, a client may choose pictures of the earth (from among a screen loaded with genuine and imaginary planets), the nation of France (from a guide of the world), the city of Nice (from a guide of France), a white stucco house with angled entryways and red tiles on the rooftop, a green plastic cooler with a white cover, a bundle of Gouda cheddar, a container of grape juice, and a pink paper glass with minimal green stars around its upper edge and three red groups around the center.

Graphical passwords might offer preferable security over content based passwords since numerous individuals, trying to remember content based passwords, utilize plain words (as opposed to the suggested clutter of characters). A word reference hunt can regularly hit on a secret word and permit a programmer to pick up section into a framework in seconds. In any case, if a progression of selectable pictures is utilized on progressive screen pages, and if there are numerous pictures on every page, a programmer must attempt each conceivable blend aimlessly. In the event that there are 100 pictures on each of the 8 pages in a 8-picture secret word, there are 1008, or 10 quadrillion (10,000,000,000,000,000), conceivable blends that could frame the graphical watchword! On the off chance that the framework has an inherent postponement of just 0.1 second after the determination of every picture until the presentation of the following page, it would take (by and large) a huge number of years to break into the framework by hitting it with irregular picture arrangements.

In the proposed graphical secret word framework, there are three phases of confirmation. At first at the season of enrolment with the framework, clients need to pick the number stages that they wish to incorporate into their secret key framework. They might pick between one, two and three stages. The clients will be required to experience that numerous stages every time they endeavor to login. In any case, clients might change the quantity of stages last mentioned. They might either expand the stages or diminishing the stages according to their benefit. In any case, this change is allowed when their effective verification in light of the present choice. Toward the finishing of the validation process, framework would demonstrate to them the alternative for the change of watchword. The secret word change might be utilized either to overhaul a specific stage by changing the watchword determination in that stage or to include/uproot a whole stage.

II. PREVIOUSLY WORK DONE

One of the key areas in security research and practice is authentication. It determines whether a user should be allowed access to a given system or resource. Traditionally, text based passwords were used for authentication. For text passwords, user creates a password which is easy to remember; hence these types of passwords are easy for attackers to hack. For more security users use strong system assigned passwords which will be difficult for users to remember [1]. The security and usability problems associated with alphanumeric passwords are referred as ‘‘the password problem.’’ The problem arises because passwords are expected to comply with two conflicting requirements, namely:

(1) Passwords should be easy to remember, and the user authentication should be done quickly and easily by humans.

(2) Passwords should be secure, i.e. they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text. Meeting both of these requirements is almost impossible for users. The problem is well known in the security community [2].

According to the previous research we can conclude that graphical password can be used as an alternative to text-based passwords, biometric and tokens as humans can remember images better than texts.

III. PROPOSED ARCHITECTURE

Following are some features of our proposed architecture:

a. Memorability: User capability to memorize created graphical password. There are eight factors that contribute to the password memorability are meaningfulness, human faces, organized by theme, user assign image, icon based, abstract image, navigation through image and drawing password.

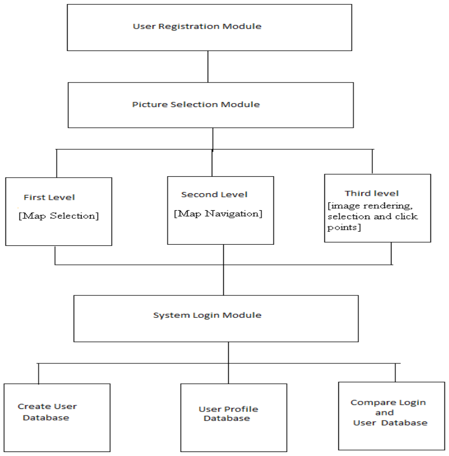
b. Efficiency: How quick users can create the password and how fast user can login using the graphical password. Almost all existing scheme provide some training on how to create a password. This training has reduce the time taken creating the password.

c. Input reliability and accuracy: Pointing to right spot is basically depends on input devices in term of software in recall based, the size of tolerance area cannot be too big or too small. If size is too big the process of inputing passwords are not consistent and accurate especially for those who have weak vision. In recognition based, basically the size of clickable are is fixed by the number of images that containing one picture.

d. Easy and fun to use : System should provide a good platform in creating password for example, using challenge-response or training session technique in order to make the user feel at ease when using the system.

e. Grid based : Clickable area are arranged in form of grid based technique. Each grid is leveled using coordinate. Using grid based technique can increase pointing accuracy.

f. Freedom of choice : User can click anywhere whining the selected picture thus providing the freedom to choose password location.



Authentication Using Graphical Password by Susan Widenbeck[2] explains the problems with alphanumeric passwords and need of graphical password. Textual passwords are difficult to remember and once a password has been chosen and learned the user must be able to recall it while login. A user need to choose memorable locations in an image depends on the nature of the image itself, because human being’s ability to remember images is well established.

Design and Longitudinal Evolution of Graphical Password system by Jim Waters [4] explains PassPoint method which overcomes some of limitations of Blonder’s method. PassPoint method is flexible because it allow any image to be used, the image could be provided by the system or chosen by the user. A user’s password consists of any arbitrary chosen sequence of points in the image since an intricate image easily has hundreds of memorable points, not many click points are needed to make password hard to guess. Three stages Graphical Password authentication scheme by M.Prabhu [1] explains possible attacks on graphical password and alphanumeric password. Three levels of graphical password systems which are Map Navigation, Image Selection and Click Point Selection.

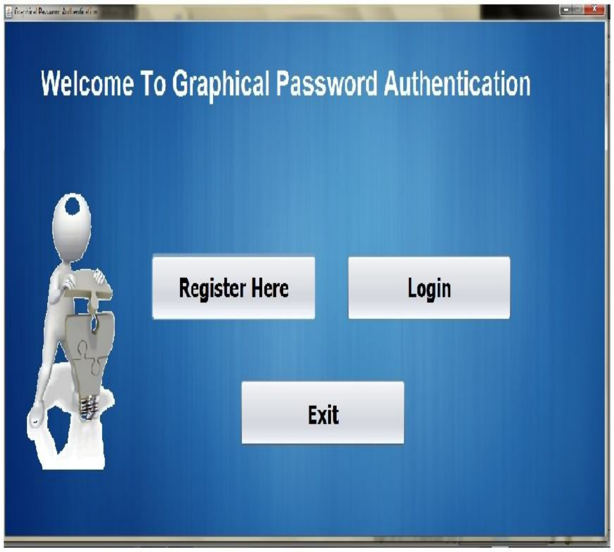
Graphical Password Authentication using Persuasive Cued Click Point by Pankaja Patil [3] explains PCCP(Persuasive cued click point) method which includes persuasive features added to CCP(cued click point) to encourage users to select more secure password and make it more difficult to select password where all click points are Hotspots.

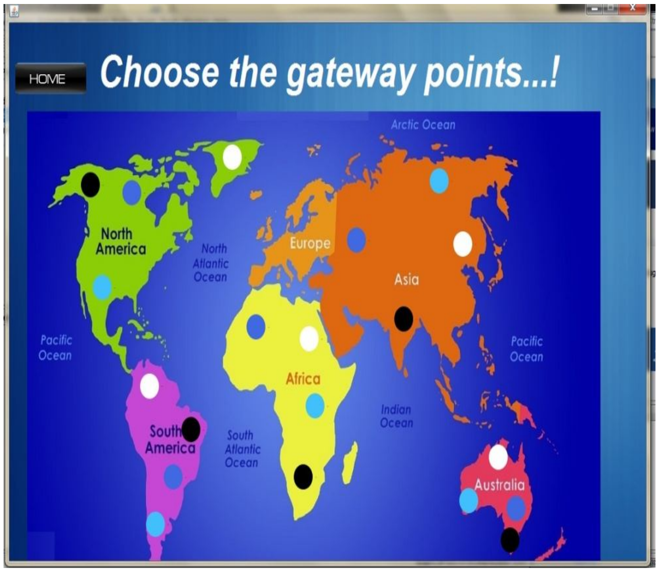
IV. ALGORITHM USED

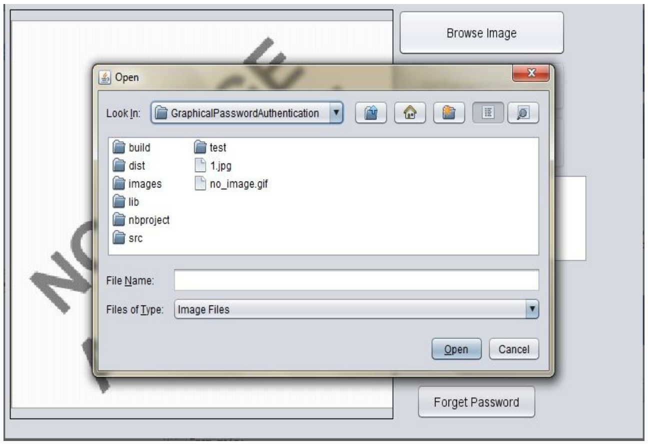
Cued Click Points was designed to reduce patterns and to reduce the usefulness of hotspots for hackers. In preference to five click-points on one single image, CCP uses one clickable region on five distinct images. The next new image presented is based on the location of the previously entered click-point; it creates a path through an image set. One best feature of Cued Click Point is that the explicit indication of authentication failure is only provided after the final clickpoint, to defend beside accumulative guessing attacks. But this method also has more drawbacks like false accept (the incorrect click point can be accept by the system) and false reject (the click-point which is to be correct can be reject by the system). We are using this algorithm to implement our system.

V. SYSTEM RESULTS

Following are some system results:







Look In: GraphicalPasswordAuthentication

File Name:

Files of Type: Image Files

VI. CONCLUSION

A new graphical password scheme with three stages of password authentication was proposed in this work. Among the three stages of the scheme, the first stage is mandatory. But the other two stages are optional and it is up to the users to include them into their password system. The first stage of authentication is based on the user’s ability to navigate to a specific location with the help of a series of maps. It moves from the continent level to the level of a country and ends with the state in the country. The second stage is about the selection of an image correctly from a gallery of images. The third stage involves the clicking of few points on the picture. The experimental analysis conducted on the implementation and data collected through the questionnaires showed the proposed scheme is suitable for usage and it has adequate security protections.

REFERENCES

[1] S.Rajarajan, M. Prabhu, S. Palanivel, M.P.Karthikeyan, “Gramap: Three Stage Graphical Password Authentication Scheme”, Journal of Theoretical and Applied Information Technology, March 2014.

[2] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, NasirMemon, “PassPoints: Design and longitudinal evaluation of a graphical password system”, Int. J. Human-Computer Studies, Elsevier ,Volume 63, Issues 1–2 July 2005, Pages 102–127.

[3] Iranna A M ,PankajaPatil. “Graphical Password Authentication Using Persuasive Cued Click Point” , International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, WorldwideScience ,ISSN (Print) : 2320 – 3765 ,ISSN (Online): 2278 – 8875, Vol. 2, Issue 7, July 2013

[4] P. R. DevaleShrikala M. Deshmukh, Anil B. Pawar. “Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme” , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013

[5] P. R. DevaleShrikala M. Deshmukh, Anil B. Pawar , “Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme “ International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013 280

[6] Julie Thorpe, Brent MacRae, AmiraliSalehi-Abari, “Usability and Security Evaluation of GeoPass: a Geographic Location-Password Scheme”, Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.