Click Based Graphical Password with Text Password Authentication

Vina S. Borkar **Priti C. Golar**

Department of Information Technology St. Vincent Pallotti College of Engineering & Technology, Nagpur, India

Abstract
From various years, authentication process used for security which is a way of determining whether someone or something is, in fact, who or what to be stated. For authentication process tokens and biometric methods are used mostly. Such passwords have the issue to remembrance and attacks. Alternative to traditional password methods, graphical passwords provide much security. It also makes feel comfortable to user .It is easy to remember password in form of images. In this paper, we implemented two-factor authentication method which provide reliability and overcome limitations. However, very little research has been done to analyze graphical passwords.

Index Terms
Graphical Password, cued click Point, Pass Point, Persuasive.

I. Introduction

User authentication is a most important component in most computer security. Access control and user accountability it provides the user. As we know there are many types of user authentication systems at present, but alphanumerical username/passwords are the most used user authentication. They are many in numbers and easy to implement and provide better usability. Due to the limitation of human memory, most users used to choose short or simple passwords which are easy to remember. Reviews show that frequently passwords are personal names of family members, birth date, or dictionary words. In most cases, these passwords are easy to guess and susceptible to dictionary attack. Presently users used many passwords for personal computers, social networks, E-mail, and more. User may decide to use one password for all system accounts to decrease the memory burden, which decrease security.

Graphical passwords are harder to guess. If the possible number of pictures is suitably large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus most probably offer improved security against dictionary attacks. The use of graphical password methods is gaining awareness because of advantages of text password. Graphical passwords were first introduced by Blonder. In his study, an image would appear on the given screen, and the user would click on a few chosen regions of it. If the correct regions were clicked on, the user would be authenticated.

II. Graphical Based Authentication Technique

In general, the graphical password techniques can be classified into two main categories: recognition-based and recall-based graphical techniques and Cued recall-based technique, but here we will discussed Cued recall-based technique.

2.1 Cued recall-based technique.

In Cued recall-based techniques, firstly Blonder [1] given a graphical password scheme, in which a password is created by making the user click on several areas (locations) on an image. The user have to click on the near areas of those locations during login(authentication). The image can helps users to recall their passwords. Passlogix authentication system based on this idea. In their implementation users must click on various items in the image in the correct sequence in order to be authenticated. Hidden boundaries are defined for each item in order to detect whether an item is clicked by the mouse.

In the “PassPoint” system by Wiedenbeck, et al. [2] has extended Blonder’s idea of eliminating the predefined boundaries and allowing user to choose random images. In this scheme, a user can click on any place on an image to create a password. A tolerance area around each chosen pixel is calculated. For authentication, the user must click within the tolerance of their chosen pixels and also in the correct sequence. This technique belongs to the discretization method proposed by Birget, et al. Any given picture can be used and because a picture may contain hundreds of thousands of memorable points. Wiedenbeck, et al. conducted a user study in which one group of participants was asked to use traditional alphanumerical password, while the other group was asked to use the image password. The result evaluate that graphical password took less attempts for the user than alphanumerical passwords. However, graphical password users had less difficulty learning the password, and took

Manuscript received November 5, 2015
Manuscript revised November 20, 2015

less time to input their passwords than the alphanumerical users.

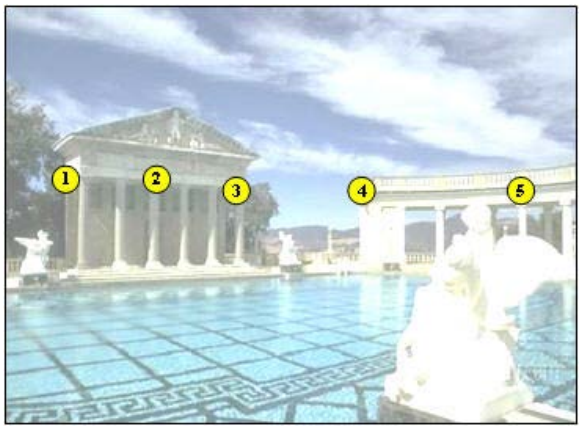

Fig 1. PassPoint method [2]

Further study in PassPoint,Wiedenbeck, et al. also conducted a user study to estimate the effect of tolerance square of clicking during the login stage, and the effect of image choice in the system. The result shown that memory accuracy for the graphical password was strongly reduced by using a smaller tolerance for the user clicked points, but the choices of images did not make a significant difference.

2.1.1 Cued Click Points (CCP):

In Cued Click-Points (CCP) scheme which is proposes alternative to PassPoints. At CCP, users click one point on each of images rather than to five points on one image. It offers one-to-one cueing to user, where each image plays as a cue for the one corresponding click-point, and introduces implicit feedback, where visual cues instantly alert legitimate users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and having facility of retry from the beginning). As shown in Fig. 3, each click results in showing a next-image, in effect leading users down a path as they click on their sequence of points. A wrong click gives an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If users dislike the resulting images, they may create a new password relating different click-points to get different images.

Shoulder-surfing is a concern with CCP. It should be noted that obtaining only the sequence of images does not provide enough information to log in directly; considerable additional effort is required to identify where to click on the images to obtain this sequence. A major usability improvement over PassPoints is that genuine users get immediate feedback about an error when trying to log in. When shown an incorrect image, they know that the latest click-point was incorrect and can immediately cancel this attempt and try again from the beginning. Providing explicit feedback in PassPoints before the final click-point could allow PassPoints attackers to increase an online attack to prune potential password subspaces, whereas CCP's visual cues should not help attackers in this way.

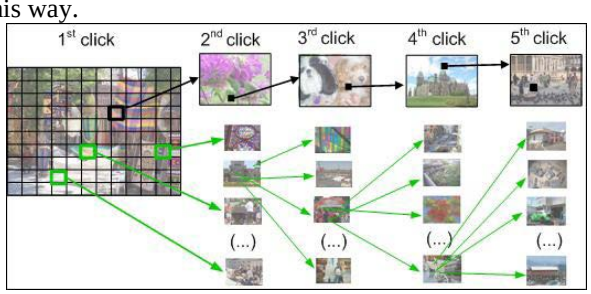

Fig.2 CCP method [3]

2.1.2 Persuasive Cued Click-Points (PCCP)

Pass-Points and cued click points have hotspot problems which reduces the security of graphical password schemes while implementation [3].To overcome this issues persuasive cued click point's graphical password method was implemented. In PCCP a password was created with five click-points, one click point on each of given five images. During password creation, for a small view port area was provided which is randomly positioned on the image. Users have to select a click-point within the view port. If users are unable or unwilling to select a click point in the current view port, they may press to the Shuffle button to change position the view port randomly. The view port was used as help of users to select more random image passwords that are reduce to hotspots problem. A user who is wants to reach a liked click-point area may still shuffle until the viewport moves to the specific location.

A persuasive cued click point scheme is basically based on Persuasive Technology This technology is used to motivate and provide control to people to behave in a desired manner. Persuasive Technology was first given by Fogg. An authentication system which based on Fogg's Principle of Reduction by making the desired task of choosing a strong password easiest and also provides the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

Fig. 3. PCCP password creation interface [3]

III. Limitations of Existing System:

Limitations related with existing system are mention below:

1. Images selection: In CCP, PCCP, DAS and PassPoint method the images provided during registration was system defined.

2. Hotspots problem: Hotspots are particular areas in the image that have a higher possibility of being selected by users as part of their passwords. It is the major problem which existing methods.

3. Password creation time. PassPoint, PCCP, Passdoodle and Cued click point, methods are more time consuming methods for password creation.

IV. Proposed System

Registration Process: As shown in Fig.5.It is a basic registration form provided to user. User will register her/his basic information with creation of alphanumeric or text password. After given basic information user move toward image password creation form for creation of image based password. In case of image based password, images are provides to user. We are used here multiple images for password creation.

Login Process: In authentication stage, user has to first login using text password given in Fig.6. If in text password authentication user will validated then he is allowed to confirm image password. If they forgot their password, they could return to the forget password step.

Flow diagram of proposed system:

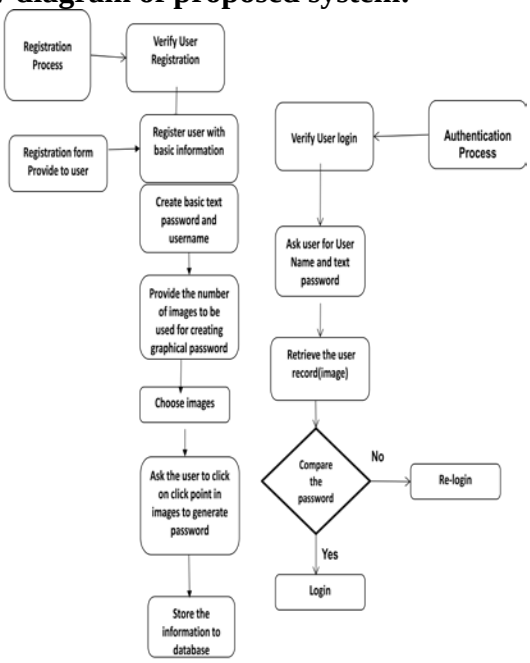

Fig.4.Flow diagram for Proposed methods

V. Result Analysis and Discussion

A user study was conducted in order to investigate the objective using total 25 images for password creation in given Fig.7. They are according to user click points on each image are shown in Fig.6. In this proposed method 20x20 tolerance square is used during user registration process. It is beneficial that images are providing more clickable points to user.

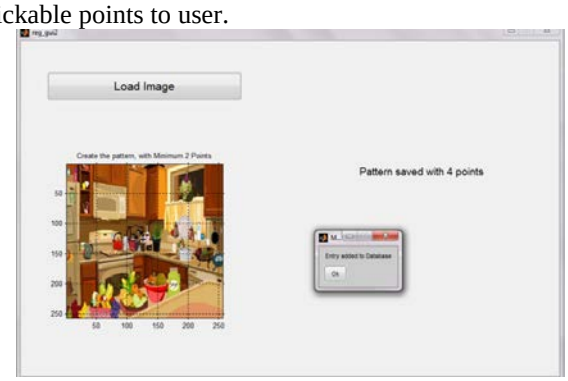

Fig.5. User Registration

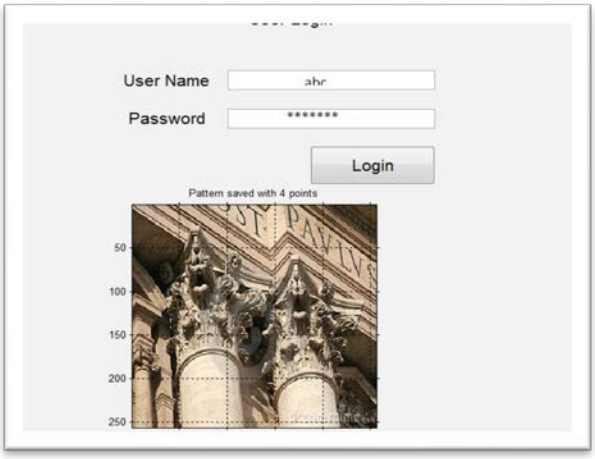

Fig.6. Login Process

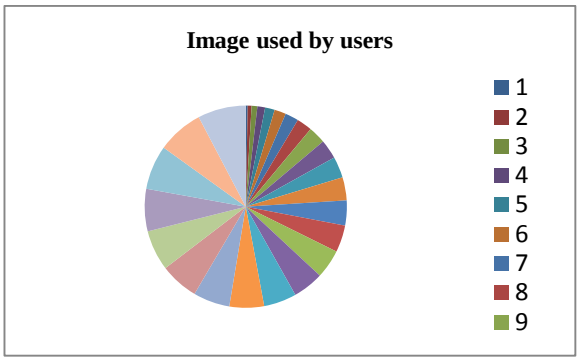

Fig.7.Images Used By Users

VI. Conclusion

In this paper we have proposed hybrid authentication methods. Users can be influenced to select stronger passwords through better user interface design. The approach has proven effective at reducing the formation of hotspots and patterns, thus increasing the effective password space. It also encourages and guides users in selecting more random graphical passwords.

References

[1] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[2] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” International Journal of Human-Computer Studies,2007.

[3] [3] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, “Persuasive cued clickpoints: Design, implementation, and evaluation of a knowledge-based authentication mechanism,” School of Computer Science, Carleton University, Tech. Rep. TR-11-03, February 2011.

[4] [4] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, “Persuasive cued clickpoints: Design, implementation, and evaluation of a knowledge-based authentication mechanism,” School of Computer Science, Carleton University, Tech. Rep. TR-11-03, February 2011.

[5] [5] S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical password authentication using Cued Click Points,” in European Symposium on Research in Computer Security (ESORICS), LNCS4734, September 2007.

[6] [6] P. C. van Oorschot and J. Thorpe, “Exploiting predictability in click-based graphical passwords,” Journal of Computer Security,vol. 19, no. 4, pp. 669–70,2011