Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Click Based Graphical Passward Authentication- Review

**Ms.Vina S. Borkar**
(PG Scholar)
Dept. of Computer Engg and Information Tech.
St. Vincent Pallotti College of Engg. & Tech.
Nagpur, India

**Mrs. Priti C. Golar**
Asst.Professor
Dept. of Computer Engg and Information Tech.
St. Vincent Pallotti College of Engg. & Tech.
Nagpur, India

***Abstract— Authentication is process of determining whether someone or something is, in fact who or what to be stated. Passwords are the most commonly used method for identifying users in computer and communication systems. For authentication mostly textual passwords are used. Such passwords have the disadvantage of being hard to remember. Alternative to text password, graphical passwords provide much security. It also makes feel comfortable to user Graphical passwords, which made of some actions on an image that the user performs. In this paper, we are conducting a comprehensive survey of existing graphical image password authentication techniques.***

***Keywords— Graphical Password, cued click Point, DAS, Pass point, Persuasive.***

## I. INTRODUCTION

User authentication is a most important component in most computer security. It provides user with access control and user liability. We know there are many types of user authentication systems in the market but alphanumerical username/passwords are the most common type of user authentication. They are many methods easy to implement and use. Due to the limitation of human memory, most users tend to choose short or simple passwords which are easy to remember. Surveys show that frequent 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.

Graphical passwords is harder to guess or broken by brute force. If the number of possible pictures is sufficiently large, the possible password space of a graphical pass-word scheme may exceed that of text-based schemes and thus most probably offer improved security against attacks. The use of graphical password methods is gaining awareness because of many advantages. Graphical passwords were originally described by Blonder. In his description, an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated.

## II. Graphical Based Authentication Technique

In general, the graphical password techniques can be classified into main two categories: recognition-based and recall-based graphical techniques.

### *2.1. Recognition Based System*

Using recognition-based techniques, a user is presented with a number of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. There are many graphical password authentication schemes which designed by using recognition-based techniques. They are listed below.

Jensen et al.[2] proposed a graphical password scheme based on "picture password" designed especially for mobile devices such as PDAs. During the password creation, the user has to select the theme first (e.g. sea and shore, cat and dog and etc) which consists of thumbnail photos. The user then selects and registers a sequence of the selected thumbnail photo to form a password. The user needs to recognize and identify the previously seen photos and touch it in the correct sequence using a stylus in order to be authenticated. However, as the numbers of thumbnail photos are limited only to 30, the size of the password space is considered small. A numerical value is assigned for each thumbnail photo and the sequence of selection will produce a numerical password. This password is shorter than the length of textual password. To over-come this problem a user can select one or two thumbnail photos as one single action in order to create and enlarge the size of the password space. However, this will make the memorability of the created password become more complex and complicated.

Fig.1 An example of Passfaces [2]

 

Based on the assumption that human can recall human faces easier than other pictures. A comparative study conducted by Brostoff [2]and Sasse [3]in which 34 subjects involved in the test showed that, the Passfaces pass-word is easier to remember compared to textual passwords. Basically, Passfaces works as follows, users are required to select the previously seen human face from a grid of nine faces one of which is known while the rest are decoys (Fig. 1). This step is continuously repeated until all the four faces are identified. Results also showed that Passfaces took a much longer login time than textual passwords.

*2.2 Recall-Based System*

In recall-based systems, the user is asked to reproduce something that user created or selected earlier during the registration phase. Recall based schemes can be broadly classified into two groups, viz. pure recall-based technique and cued recall-based technique.

*2.2.1. Pure Recall-Based Techniques*

In this group, users need to repeat the passwords without any help or reminder by the system. Draw-A-Secret technique, Grid selection, and Passdoodle are some examples of pure re-call-based techniques. DAS (Draw-A-Secret) scheme is the one in which the password is a shape drawn on a two-dimensional grid of size G * G. Each cell in this grid is represented by distinct rectangular coordinates (x, y). The values of touch grids are stored in temporal order of the drawing. If exact coordinates are crossed with the same registered sequence, then the user is authenticated. As with other pure recall-based techniques, DAS has many drawbacks. In 2002, a survey concluded that most users forget their stroke order and they can remember text passwords easier than DAS. Also, the password chosen by users are susceptible to graphical dictionary attacks and replay attack.

Passdoodle, is a graphical password of handwritten drawing or text, normally sketched with a stylus over a touch sensitive screen. Goldberg et. al have shown that users were able to recognize a complete doodle password as accurately as text-based passwords. Unfortunately, the Passdoodle scheme has many drawbacks. Users were fascinated by other users' drawn doodles, and usually entered other users' password merely to a different doodles from their own. It is concluded that the Passdoodle scheme is vulnerable to several attacks such as guessing, spyware, key-logger, and shoulder surfing.

*2.3 Cued recall-based technique.*

Blonder [3] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password). Passlogix has developed a graphical password 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. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse.

The "PassPoint" system by Wiedenbeck, et al. [4] extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence. This technique is based on the discretization method proposed by Birget, et al. [2]. Because any picture can be used and because a picture may contain hundreds to thousands of memorable points, the possible password space is quite large.

Wiedenbeck, et al. [4]conducted a user study in which one group of participants were asked to use alphanumerical password, while the other group was asked to use the graphical password. The result showed that graphical password took fewer attempts for the user than alphanumerical passwords. However, graphical password users had more difficulties learning the password, and took more time to input their passwords than the alphanumerical users. Later conducted a user study estimate the effect of tolerance of clicking during the re-authenticating stage, and the effect of image choice in the system. The result showed 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. The result showed that the system works for a large variety of images.

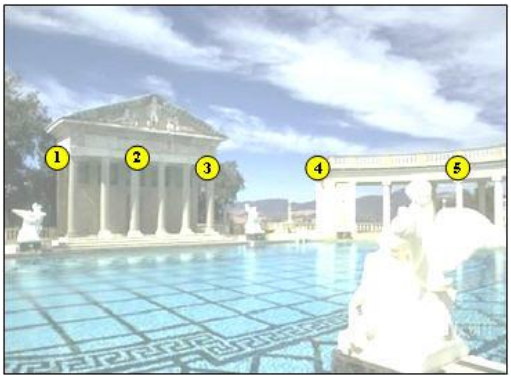


Fig 2. Passpoint method[4]

 

*2.3.1. Cued Click Points (CCP):*

Cued Click-Points (CCP) is first alternative to PassPoints. In CCP, users click one point on each of images rather than on five points on one image. It offers cueing, where each image acts 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 It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in effect leading users down a as they click on their sequence of points given in figure. A wrong click leads down 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 involving different click-points to get different images.

In case of attacks shoulder-surfing is anxiety with CCP. A major usability enhancement over PassPoints is the fact that valid users get immediate feedback about an error when trying to log in. When they see an incorrect image, they know that the latest click-point was incorrect and can immediately cancel this attempt and try again from the beginning. The visual cue does not explicitly make known “right" or “wrong" but is evident using knowledge only the genuine user should possess. Text passwords and PassPoints can only safely provide feedback at the end and cannot reveal the cause of error. 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 cues should not help attackers in this way. Another intended usability enhancement is that being cued to recall one point on each of five images appears easier than remembering an ordered sequence of five points on one image.

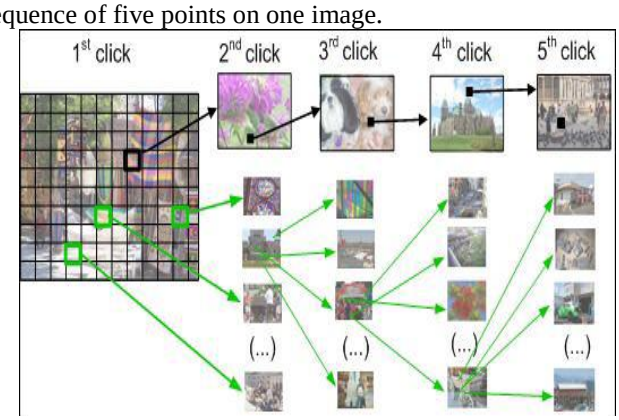


Fig.3 CCP [3]

*2.3.2. Persuasive Cued Click-Points-(PCCP)*

In case of Pass-Points and cued click points [3] the guessing attacks, capture attack, and hotspot problems which reduces the security of graphical password schemes and to overcome this persuasive cued click point method implemented. In which a password consists of five click-points, one on each of five images. During password creation, a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the viewport moves to the specific location.

Persuasive Technology used to motivate and influence people to behave in a desired manner. Persuasive Technology was first articulated by Fogg. An authentication system which applies Persuasive Technology should insist users to select stronger passwords. PCCP’s [1] design follows Fogg’s Principle of Reduction by making the desired task of choosing a strong password easiest and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.


Fig. 4 The PCCP password creation interface [1**].**

 

## III. CONCLUSION

In this paper we have studied comprehensive study of existing graphical authentication methods. We conclude that for using graphical password is they can be easily remembered; also graphical passwords are provides more security than text based passwords. Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of usefulness.

**References**

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

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

[3] 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.

[4] 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.

[5] 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.

 