International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

# Graphical Password Authentication using Cued Click Points

Milouni Dattani[Ȧ*], Vaibhavi Kamani[Ȧ] ,Raveena Pandya [Ȧ] , Heta Mehta[Ȧ], Arjun Jaiswal[Ȧ] and Mitchell D'silva[Ȧ]

[Ȧ]Information Technology Department, DJSCE Mumbai University, Vile Parle, Mumbai 400 057, India.

Accepted 10 Nov 2014, Available online 01 Dec 2014, **Vol.4, No.6 (Dec 2014)**

## *Abstract*

*With the rapid use of computers, the security of passwords is must where privacy is important. For password protection various techniques are available. The main issues of knowledge based authentication, usually text based passwords, are well known. Users tend to choose passwords they can easily remember and hence can also be guessed by the hacker. To avoid the limitation of textual passwords, this paper focuses on the implementation of a Graphical Password Authentication System using cued click points based on the integrated evaluation of the cued click points. Click cued points (CCP) is a click-based graphical password scheme. Users click on one point per image for a sequence of images. The next image is based on the previous click-point. Users prefer CCP over Passpoints because selecting and remembering only one point per image is less secure, than having each image being triggered by the user's memory as to where the corresponding point was located. CCP also provides greater security than PassPoints because the number of images increases the workload for attackers.*

***Keywords:*** *Graphical Passwords, Computer Security, Authentication, Usable Security, User Study.*

## 1. Introduction

People select predictable passwords. This occurs with both text based and graphical passwords. Users often choose passwords such that they can easily remember in some way, which unfortunately means that the passwords tend to follow predictable patterns that are easier for attackers to exploit. Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and various experiences have shown that text-based passwords are fraught with both usability and security problems that make them less than efficient solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than remembering text. Graphical passwords are intended to benefit from this particular human characteristic so that by reducing the memory burden on users, coupled with a larger password space offered by images, more secure passwords will be generated and users will not resort to selecting common passwords.

In this paper, we propose a new click-based graphical password scheme called as Cued Click Points (CCP). The user password consists of selecting 5 images by using either a single click or double click. A password consists of one click-point per image for a sequence of images. The following image displayed is based on the previous click-point of the users. An important feature of CCP is that whether the password entered by the user is correct or incorrect is recognized at the end so the attacker doesn't come to know at which click-point he has gone wrong. Thus, CCP offers improved security and usability. Users can quickly create and re-enter their passwords. Another feature is that the user can even reset the password. Since one of the feature is that incorrect path will be known to user at end of the final click if the user sometimes makes a mistake while clicking on point in image he can use reset button rather than continuing till end and then logging in again. The reset option can help the user to move back to the login page rather than waiting till the final click. Another feature is the click based display of the next image. Users will be given a choice whether they want to choose a single click or double click. If he selects the double click on the point in the image then the next image will be displayed after a double click. If he selects single click then after one click on the point in the image next image will be displayed. This feature prevents shoulder surfing. As attacker will not be aware whether it is single/double click.

Section 2 discusses the background and work related to recognition based authentication techniques. Section 3 explains the working of CCP technique. Section 4 concludes and highlights the future scope for the proposed system.

## 2. Background and Related Work

Text based passwords is the most popular user authentication method, but it is less secure and requires a lot of effort to remember them. Some of the alternatives such as biometric systems and tokens have their own limitations. Graphical passwords offer another alternative, and are the focus of this paper. Graphical passwords can

*Corresponding author: **Milouni Dattani** be classified into two categories depending on the cognitive activity required to remember the passwords viz. recognition based authentication and recall based authentication. Recognition based authentication covers the following techniques:

### *2.1 Passfaces method*

Passfaces is a graphical authentication technique based primarily on recognizing human faces. The user has to choose from a large dataset of images a single image for making his/her password while logging in the user has to select the appropriate image out of a large number of false images(Vaibhav Moraskar, *et al*, 2014). Results showed that the users could accurately remember the images to the point of being insecure. Passfaces can be predictable as they are affected by race, gender and attractiveness.

### *2.2 Story*

This was an improvement over passfaces method. In this technique rather than selecting the images of faces users were asked to select day to day images in correct order in order to create a story. The user choices were much less predictable but it caused a memory load on the human brain.

### *2.3 PassPoints*

In PassPoints, a password consists of a sequence of PassPoints on a single image. Users may select 5 pixels in an image as click points and create their own password. To login they select their click points again within a system defined tolerance square of the original click points. Although, PassPoints is comparatively usable, it makes security a weakness and makes passwords easier for hacker to guess. It seems obvious that some areas of an image are more attractive to users as click-points. If this phenomenon is too strong, the probability that attackers can guess a password significantly increases. If attackers come to know which images are being used, they can select a set of likely hotspots through image processing tools or by observing a small set of users on the target image and then building a dictionary based attack on those points (Sonia Chiasson1, *et al*, 2014). These methods being not much effective for password security, this paper proposes another method called as Cued Click Points in order to eliminate the limitations of the existing techniques.

## 3. Cued Click Points

Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, users click on one point on each of c = 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning) (Vaibhav Moraskar, *et al*.,2014). It also makes attacks based on hotspot analysis more challenging( Reddy *et al*.,2013). As shown in Fig. 1. below, each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points [5]. A wrong click leads down to an incorrect path, with an explicit indication of authentication failure only after the final click( Reddy *et al*,2013). They can decide whether they want to use a single click or double click on the image which makes the proposed system a lot more secure and effective. If the user makes a mistake while logging in, then there is a reset button which will allow the user to make a correct click which would lead him to right image. Our system will have images of size 451x331 pixels and tolerance squares of 4x4 pixels. On the image there will be 16 grids and behind each there will the address of the image which on click will display the corresponding image. So, there will 4 overlapping images with tolerance square in 16 grids.

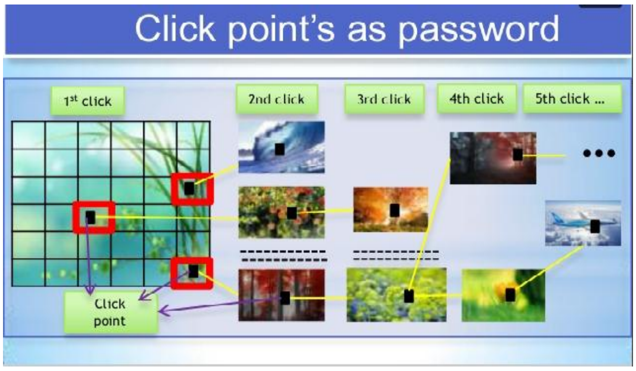

**Fig.1** Graphical password authentication using Cued Click Points (Reddy *et al.*,2013)

The process would begin with user registration where the user has to enter username and the name will be verified and stored in the database. The user will select image from the database of the password system. Then the user will be asked to select a point from the tolerance square and whether he wants to select using a single or double click for particular image and a message box will be displayed asking whether the user wants to continue or not and if the user wants to continue then the point, image and username will be stored in the database. Now the user has to select another point on the other image and continue with the above steps.

In the login module, the user has to enter username which is verified from the database and if correct the corresponding image is displayed. Then comes click point verification where the click of point in tolerance square is verified and if found correct the next image is displayed. But if the user makes a mistake by clicking on wrong point then reset button is provided to make a correct click. The path entered by the user is right or wrong is known to the user at the end of the final click.

## 4. Conclusion and future work

Picture passwords are a substitute to textual alphanumeric passwords. It satisfies both contradictory requirements i.e. they are simple to remember and hard to presume. It is an easier and secure password scheme and thus averts shoulder surfing attack to a great extent. The proposed

Cued Click Points scheme assures to be a more viable and memorable authentication mechanism. CCP has several benefits over PassPoints in terms of usability as it takes advantage of user's ability to recognize images and memory trigger associated with seeing a new image. It is easier to remember only one click point per image as compared to a series of clicks on a single image. CCP offers a more secure substitute to PassPoints. By virtue of CCP, the workload for attackers' increases tremendously as they are strained to first acquire sets of images for each user and then perform hotspot testing on each image. Moreover, the system's flexibility to increase on the whole number of images in the system allows us to arbitrarily increase this workload.

Future work should comprise of a thorough evaluation of the practicability of CCP as an authentication mechanism, which incorporates an extensive study of how these passwords work in practice and whether longer CCP passwords would be utilizable. The security of CCP must also be closely examined in order to address how attackers may take advantage of the emergence of hotspots.

## References

Vaibhav Moraskar, Sagar Jaikalyani, Mujib Saiyyed, Jaykumar Gurnani, Kalyani Pendke,(2014) Cued Click Point Technique for Graphical Password Authentication, *IJCSMC*, Vol. 3, Issue. 1

Sonia Chiasson1, P.C. van Oorschot1, and Robert Biddle, Graphical Password Authentication Using Cued Click Available at: *http://people.scs. carleton.ca/~paulv/ papers/esorics07-c.pdf*

Borkar *et al*.,(2014) *International Journal of Advanced Research in Computer Science and Software Engineering* 4(4), Click Based Graphical Passward Authentication- Review , April -2014, pp. 614-617.

Vaibhav Moraskar *et al*.,(2014) *International Journal of Computer Science and Mobile Computing,* Cued Click Point Technique for Graphical Password Authentication
Vol.3 Issue.1, January- 2014, pg. 166-172.

Reddy *et al*.,(2013) *International Journal of Advanced Research in Computer Science and Software Engineering* 3(8), ECCP: Enhanced Cued Click Point Method for GraphicalPassword Authentication pp. 321-325.