Improved Persuasive Cued Click Points for Knowledge-Based Authentication

M.Ashwini and K.C.Sreedhar

Dept of CSE, QIS College of Engineering & technology, ngole, Prakasam Dist, A.P, India

Summary

Authentication plays a major role in digital environment .In this environment we have different methods which generally use alphanumeric characters and special characters for password creation. These methods have problems like hard to remember password because it has no meaning and easily breakable by third parties or attackers. To address these issues, some of the researches suggested many techniques for authentication and reveals graphical password method which is best one in terms of cost and usage. Basically, graphical passwords use images for password creation and it has some demerits like hotspot and shoulder surfing problem.A persuasive cued click-point based method was proposed by Sonia Chiasson which reduces hotspot problem but it fails in the case of shoulder surfing problem. To address these issues, the proposed work enhances the persuasive cued click point based method with some changes in the login phase and it uses double click point method for selecting click point.in login phase, a single click method takes empty values whenever a user uses a single click for selecting the click point. Where as in the case of double click method, it takes click point actual value. With these two types of clicks an attacker peeping over the shoulders of the authorized user can be confused with the clicks, has he will not aware of the exact click points in the password. This reduces the shoulder surfing problem.

Key words:

Authentication, Graphical passwords, Hotspot, Shoulder surfing.

1. Introduction

Authentication is an essential thing, which prevents unknown person in a computer based environment system. Now a days, most frequently used method in the computer based system for authentication is text based authentication is text based authentication which user create passwords by using characters, numbers and special characters.Earlier experiments has shown that text based passwords have struggled with usability and security issues. To mitigate these problems graphical passwords techniques have been introduced. In graphical based authentication, instead of text it uses images to create a password. Graphical passwords can be classified into three types: Draw-based [1]type, choice based[2]type, click-based[3]type. In draw-based type, users have to draw some secrete. In choice-based type,users have flexibility to select sequence of images to set the password. In the case of click-based method, user has to select click points on the image. Familiar click-based authentication techniques include pass-points, cued click points and persuasive cued click points. In pass-points method, users have to select click points on a single image. In cued click point method, users can select click points up to n level of images i.e., in each level it take a single click point on a single image. In the case of persuasive cued click points (PCCP),it selects one click point on one image using persuasive technology.Form the security point of view, the click -based graphical authentication suffered with hotspot and shoulder surfing problems.to mitigate these issues, the following contributions are made in this paper:

To reduce hotspot problem, it uses persuasive technology. Here system activates some area for selecting the click point on the image and further user doesn’t have the rights to change that selected area.

To reduce shoulder surfing problem, it uses double click method for selecting the click points and single click method for storing empty values in the login phase. Even though an attacker got information about click points it’s hard to break our password. Because the user applies either single or double click methods randomly to confuse attacker.

2. Background

Text passwords are the most popular user authentication method but have some security and usability problems. Security problem is nothing but causing various attacks like shoulder surfing (looking over one’s shoulder to get information) etc and usability problem refers to limited password space. So to overcome from these drawbacks, graphical passwords had been introduced by Greg Blonder in 1996 which offers another alternative and are the focus of this paper. The passwords which we are focusing are cued recall click based graphical passwords(also known as locimetric [9]). In such systems, users identify and target previously selected locations within one or more images.

The images act as memory cures[10] to aid recall. Examples of these systems include Pass Points (PP) [11] and Cued click-Points (CCP) [12] which are present or existing systems.

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

A. Pass Points(PP):

User’s selects N random points in an image presented to user: In this system an image is picked from set of images present in a gallery and user is shown the image. Task of user is used click N points as shown in fig 1.As user clicks on the points are stored and not the point itself. Because strong points directly reduces the security of the technique .As it is very difficult to remember the random points, user chooses to select points on images that can be easily recognized in user chooses to select points on images that can be easily recognized on the image.

It is called Hot Spot [13] Advantage of this system is simplicity of implementation and drawback of low security. In another variant of this system, user himself picks the image which increases the security. However user has to always enter the same image and within some system defined to tolerance for each click point during authentication which means that image be physically present in the client system.

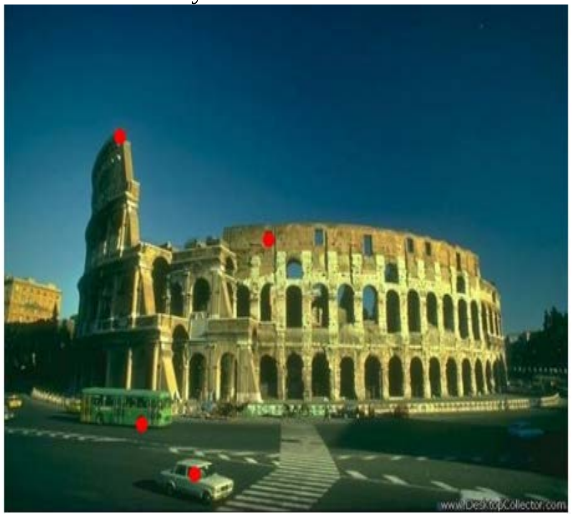

Fig 1: Pass Points(PP)

B. Cued click-point (CCP)

User selects one point in each of N images presented to user randomly: In order to increase the security loopholes mentioned in pass points system, password distribution scheme is developed. Here user is presented with N random different images and user has to click one point at every image. Based on selected click point of current image next image is displayed in fig 2. The complexity of this technique is high as user not only has to remember the images in proper order but also has to remember the password.

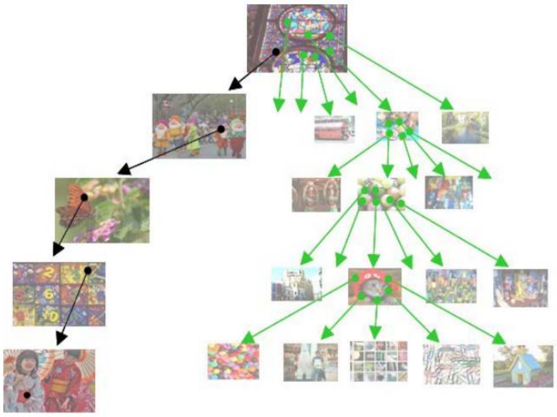

Fig 2:Cude Click Points, Each Click determines the next image

3. Related Work

This section describes the techniques and algorithms related to graphical password authentication.

S. Wiedenbeck et al.(2005)[4]introduces a pass-point technique which helps to achieveusability by reducing the problem of memorable passwords over text based passwords method. Here user needs to select five click points on the image for registration.For authentication user needs to select five click points in the tolerance area in the same order.But it fails in the case of hotspot problem.

Sonia chiassson etall[5] proposed one method called cued-click points which provides more usability and security than pass-points method. Here user can select one click-point for one image up to n levels. In login phase user should follow he order and select the click point within the tolerance area. cued-click points provide usability but suffered with hotspot problem.

Suo [8] proposes a shoulder-surfing resistant version of pass-points. During login, the image is blurred except for a small focus area. Rather than using a mouse to select their click-points, users enter Y (for yes) or N(for no) on the keyboard, or use the right and left mouse buttons, to indicate if their click-point is within the focused area. The process repeats for at most 10 rounds, until all 5 click-points are identified.

Robert Biddle[6] proposed an algorithm, called centered discretization, for calculating tolerance area of click-points. Ingraphical passwords, calculating whether user click-points are valid or not. It removes the problems like false accept and false reject.

4. Persuasive Cued Click Points(PCCP)

Hotspots and shoulder surfing problem reduces the security in the graphical based authentication . Attackers can retrieve the passwords using skewed password distribution.

An earlier result shows that most of the people are attracted on the same area of the same area of the image.So it is easy to attack. Observation reveals that if users select the click point without anyother involvement still there is a chance to appear for hotspot problem. Researchers suggest that the user choice in all types of graphical passwords is inadvisable. To eliminate this, system involvement is needed to select more random click points while maintaining usability.

The attackers acquire knowledge of a particular user's credentials through direct observation or through external recording devices such as video cameras while the authorized user enters the information. An attacker who accurately observes one login would have enough information to log in independently, so shoulder-surfing is a concern. The PCCP uses persuasive technology to motivate users to select less guessable passwords and make it more difficult to select every click point as hotspot. Mainly at the time of password creation the images are shaded except viewport and it is positioned randomly to avoid hotspots.

This hotspot information allows attackers to improve guesses and could have a chance to produce new hotspots. Viewport size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Selection of click point of user must be inside the viewport only. Outside of the view port will not respond for user clicks. The user has the flexibility to change the view-port area which is provided by the system whenever a user doesn't satisfy with the generated view-port area. At the login phase, images are displayed without shading and users needed to select correct click points for authentication.

5. Improved Persuasive Cued Clickpoints(Ipccp)

The PCCP heavily concentrated on hotspots issue. To eliminate this, it uses persuasive technology. This technology is good enough but usage is not much beneficial because here users have the facility to change the location. So still there will be a chance for hotspot. The PCCP doesn't provide any technique for minimizing shoulder surfingproblem. Improved persuasive cued click point method is enhancement of PCCP by adding some techniques. This paper mainly concentrates on reducing hotspot and shoulder surfing problem. In this method we have four phases

1. Preprocessing phase.
2. Registration phase.
3. Login phase.
4. Processing phase.

5.1 Preprocessing Phase

In order to achieve system involvement for click point'sselection in the login phase we need the following steps:

Divide the image into blocks: In generally, we use 2D images in the process of password creation. These images are generally represented by x, y coordinates.

By using these coordinate values we can divide image into blocks and will provide values for each block sequentially.

Merge the image blocks to get same original image: To do this, we use same sequential values to build the original image.

After merging the blocks blur the complete image. This image is not visible clearly.

Activate only one block to select click points in the registration phase: In this step randomly we can activate only one block for click point selection as shown in fig:

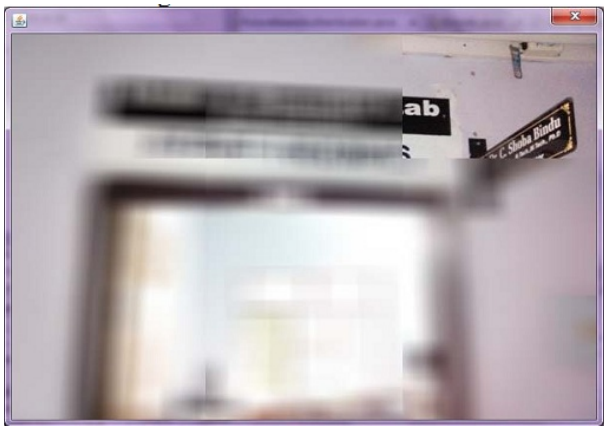

Fig 3: Activation at the block at preprocessing time.

5.2 Registration Phase

In this phase a new user needs to create user id and t allocate set of images for selection of click points in order to create passwords. Here we use single click method for selecting click points

5.2.1 Single Click Method

This method is applied on only in the activated portion of the image. Once it is applied on the image, it generates the coordinate values(x, y) of click points. And it is stored in temporary variables. To calculate tolerance area of click points it uses centered discretizationalgorithm [7] with the input of those temporary variable values. Finally this results(username, images, and tolerance values) stored in database.

5.3 Login Phase

In this phase, whenever user id internal processor check whether the id is valid or not. If valid then corresponding images are displayed. On this user have to select click points by using single click method and double clicks method.

In single click method, it takes empty values whenever a user uses a single click for selecting the click point and these values are sent to the processing phase.

5.3.1 Double Click Method:

It takes coordinates values of click points and is stored temporarily in a variable and these values are sent to processing phase. Mostly an attacker focuses on single click method for selecting click point rather than double click in the login phase. This will reduces the shoulder surfing issue.

5.4 Processing Phase

We can compute tolerance area of click points which is obtained from login phase using centered discretization algorithm [7]. Now we should compare this result with the values stored in database. If the values are matched we can concluded that the entered user is an authorized otherwise the entered user is an unauthorized user.

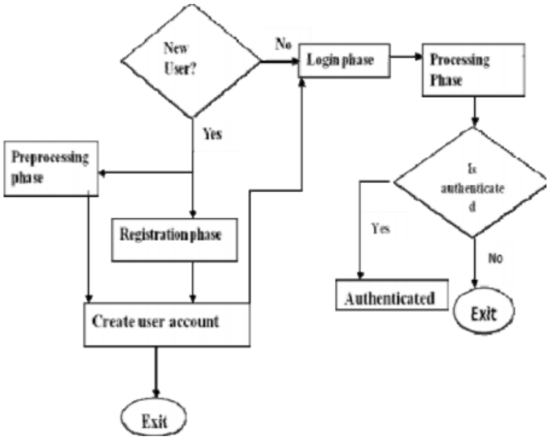

Fig 4: Represents the flow of IPCCP.

6. Usability and Security Analysis

The proposed improved persuasive cued click point is compared with PCCP in terms of usability and security functionalities.

6.1.Usability

The usability functionality can be measured based on two factors, they are: success rate and password generation time.

Success rate: it can be calculated based on successful login of a user. User faces some minor difficulty during the registration phase due to blurring on the image because they face some difficulty to identify the image. It is user-friendly after completion of login phase.

Table 1: Login times for both IPCCP and PCCP

	Successful user password creation	Successful login
IPCCP	33/35(94%)	31/35(88%)
PCCP	32/35(91%)	30/35(85%)

Almost two schemes performed well over the success rate but proposed scheme slightly tends to be good over PCCP

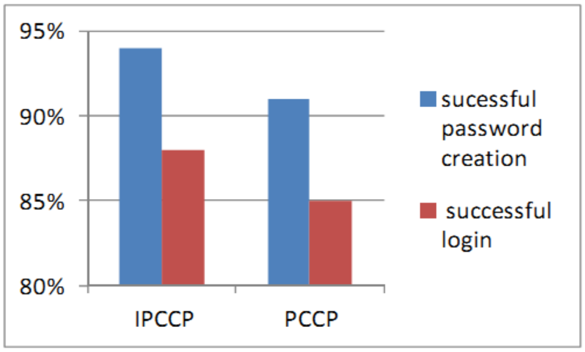

Fig 5: Comparison of success rate of two schemes.

Password generation time: In PCCP, system activates some area of image for selecting click points. If the user does not satisfy with that activated area there is a flexibility to change that area by the user. This flexibility causes hotspot problem and increases time for password creation. To mitigate these issues IPCCP uses invariant view port area.

Table 2: time taken by each phase for both IPCCP an PCCP

	IPCCP		PCCP	
	Password Creation Phase	Login Phase	Password Creation Phase	Login Phase
Time taken for 5 click points	38.2	16.2	50.7	16.2
Time taken for single click points	35.9	7.8	36.2	7.8

From table 2, it can be learnt that the two schemes shows a significant time variation at registration phase, whereas, during the login phase both the schemes take almost the same time.

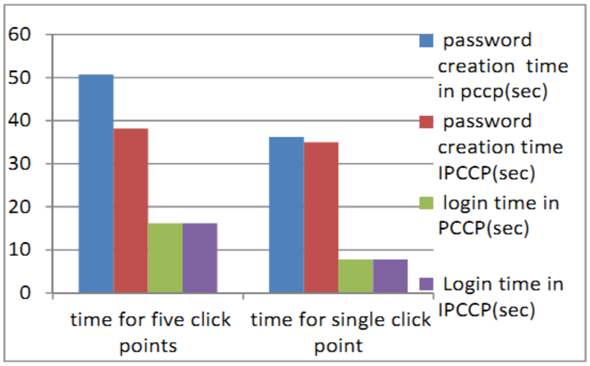

Fig 6: Comparison of password creation and login time of two schemes.

7. Security

The security can be achieved by reducing the hotspots and the shoulder surfing problem.

Hotspots: One of the main goals of this work is to prevent hotspot problem. For achieving this, we divide the image into block in the form of square matrix. The matrix size up to 6*6 so that we can get more blocks. Once an image is divided into more blocks there is a less chance for hotspot issue in the generated block.

Table 3: Hotspot percentage for both IPCCP and PCCP

	In PCCP	In IPCCP
Probability of selected point to be a hotspot in percentage	13%	8%

Both PCCP and IPCCP through put are very good in the case of hotspot removal. But our proposed work gives some more good result.

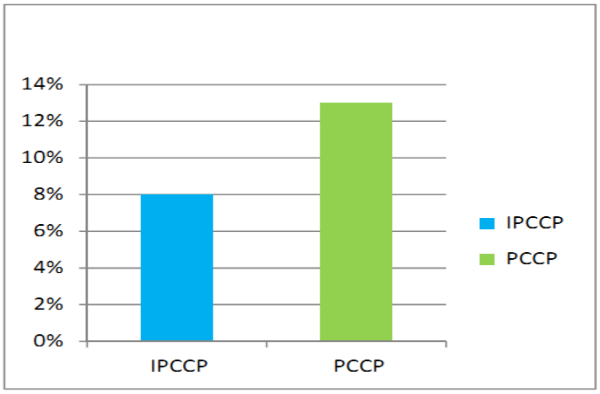

Fig 7: Comparison of hotspot occurrence percentage of two schemes.

Shoulder surfing problem: IPCCP provides more security by reducing shoulder surfing problem. Earlier in PCCP, it uses a single click method for selecting click points in the login phase. Where as in IPCCP, it uses bothsingle click and double clicks method randomly for the selection of click points in login phase. So that it is very hard to predict the exact click point method used in the password.

8. Conclusion

Authentication relies on usability and security issues and its responsibilities are to provide strong passwords with less memory effort and to make an application more secure from vulnerabilities. Earlier pass-points overcome usability issues but suffered with security issue because all points are on the same image. Later CCP was designed for eliminating these problems by using more number of images.

However these techniques did not overcome hotspot problem completely. To remove these issues a new methodology PCCP was introduced but it completely failed in the case of shoulder surfing problem. IPCCP is the enhancement of PCCP and is designed to encourage the users to select more random click points and provides a method to remove the shoulder surfing problem. IPCCP is comparison reveals that IPCCP is better than PCCP in the aspect of usability and security.

The major advantage of persuasive cued click point scheme is its large password and it helps in reducing number of hotspots in the image compared to existing click based graphical password systems. Therefore it provides better security. Randomness of the system is very high in comparison to both single-image multi-point based technique and multi-image single point based techniques. The system offers features based matching instead of point based matching. Thus physical password does not store the image points. There by securing the password to a great deal.

The system allows user to select first image at the time of authentication, thereby eliminating the need of exposing the gallery for every images. It is though for the impostors to remember the first image and view port. Thus systems are better equipped to deal with false acceptance and shoulder is surfing attacks. This method can be further improved by incorporating better image features than color features. Texture descriptor could be used for complex images.

References

[1] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, The Design And Analysis Of Graphical Passwords, Proceedings of the 8th USENIX Security Symposium Washington, D.C., USA, August 23–26, 1999.

[2] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes.In 13th USENIX Security Symposium, August 2004.

[3] S. Chiasson, R. Biddle, and P. van Oorschot.A second look at the usability of click-based graphical passwords.In the proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), July 2007.

[4] Susan Wiedenbeck, Jim Watersa, Jean-Camille Birget, Alex Brodskiy, NasirMemon, PassPoints: Design and longitudinal evaluation of a graphical password system, Int. J. Human-Computer Studies 63 (2005) 102–127.

[5] Sonia Chiasson1,2, P.C. van Oorschot1, and Robert Biddle , Graphical Password Authentication Using Cued Click Points, April 10, 2007.

[6] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and Paul C. van Oorschot, Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism, MARCH/APRIL 2012.

[7] S. Chiasson, J. Srinivasan, R. Biddle, and P. van Oorschot.Centered discretiza-tion with application to graphical passwords.InUSENIX Usability, Psychology, and Security (UPSEC), April 2008.

[8] X. Suo. A design and analysis of graphical password. Georgia State University, August 2006.

[9] S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical password authentication using Cued Click Points”, in European symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359-374.

[10] A. De Angeli, L. Coventry, G. Johnson, and K. Renaued, “ Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systrms,” Journal of Human-computer Studies, vol. 63, no. 1-2, pp.128-152, 2005.

[11] E.Tulving and Z.Pearlstone, “Availability versus accessibility of information in memory for words,” Journal of Verbal Learning and Verbal Behavior, vol.5, PP. 381-391,1966.

[12] S.Wiedenbeck, J.Waters, J.Birget, A. Brodskiy,and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” Journal of Human-computer Studies, vol. 63, no. 1-2, pp. 102-127,2005.

[13] K. Golofit, “click passwords under investigation,” in 12th European Symposium on Research in Computer security (ESORICS), LNCS 4734, September 2007.

K.C. Sreedhar is currently working as assistant professor in C.S.E department QIS College of Engineering and Technology, Ongole, AP,India. He received his M.tech from JNT University, Hyderabad in 2012. His research interests include datamining and computer networks. He has around 6 years of teaching experience for under graduate and post graduate students.

M. Aswini is currently studying M.Tech in the steam of C.S.E in QIS College of Engineering and Technology, Ongole, AP, India. Her research interests are interests nclude data mining and computer networks.