Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.1049 – 1056

RESEARCH ARTICLE

Robust Authentication Based Graphical Passwords Mechanism

Nikhil Tarkeshwar Ambade[1], Prof. Dr. Arati Dixit[2]

[1]M.E. student, Department of Computer Engineering PVPIT, Shavitribhaiphule Pune University, India

[2]Professor, Department of Computer Engineering PVPIT, Shavitribhaiphule Pune University, India

[1] Nikhil.ambade50@gmail.com; [2] Adixit98@gmail.com

Abstract— In alphanumeric text based passwords, users try to create memorable passwords that are usually easy for attackers to capture, and strong system-assigned passwords are difficult for users to remember. Text passwords are the most popular user authentication mechanism which faces variety security problems. Other techniques such as biometric systems and tokens have their own drawbacks. Graphical password is another alternative to text. Different existing graphical password techniques were studied and analysis. Existing PCCP graphical password technique provides better security but have accessibility problem. The system assign viewport in persuasive technique help users to select stronger password but may take several clicks to get desired portion which is considerably slows the systems password creation process. Proposed system overcomes the drawbacks of Persuasive cued click point (PCCP) technique by providing better user accessibility. Proposed work provides better security while maintaining accessibility.

Keywords— Graphical password, Authentication, Text passwords, Security, Usability.

I. INTRODUCTION

A password is a string of characters or word used for user authentication to make identity or access approval to gain access to a resource, which should be kept secret from unauthorized those not allow access. Authentication is the act of confirming the truth of an attribute of a piece of data. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. The purpose of authentication schemes is to allow access only by legitimate users. Authentication methods can be divided into Token based authentication, Biometric based authentication and Knowledge based authentication.

Token based authentication method uses tokens such as key cards, bank cards and smart cards to provide security. Token-based Authentication systems also use knowledge based techniques to improve security.

A Biometric based authentication technique uses fingerprints, iris scan, or facial recognition. This technique uses hardware which is expensive and the identification process can be slow and unreliable. Thus, this type of technique provides the highest level of security.

Knowledge based techniques include both text-based and picture-based passwords. Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information which reduced memory burden that will facilitate the selection and use of more secure or less predictable passwords, discourage users from unsafe coping practices.

One of the main drawbacks in text-based password is the difficulty of remembering it. Studies have shown that users tend to choose short and easy passwords [2]. But, these passwords can also be easily guessed or

attacked. Text based password scheme is lacking the above essential points. Generally the text based passwords follow the difficult guidelines like password should be at least 8 characters long, it should not be easy to relate to the user, it should not be a word that can be found in a public dictionary, it should combine upper and Lower case letters and digits. Because of these guidelines the text based password scheme has many problems and difficulties which the user will have to face, like user may forget the password if it is too long.

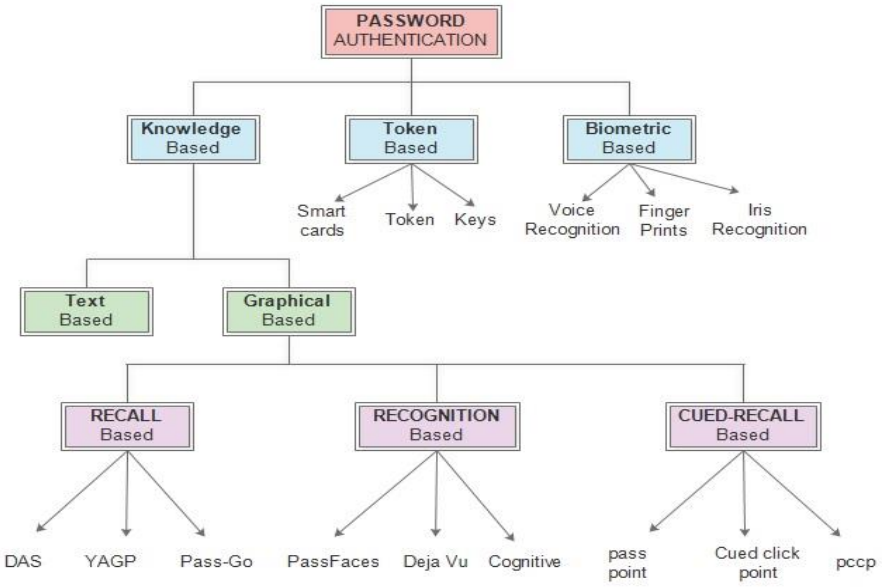

Figure 1: Categories of password authentication.

II. **RELETED WORK**

The problems of text based password are stolen the password, forgetting the password, and weak password. So there is need to have a strong authentication method which secure all our applications. Traditionally, conventional passwords have been used for authentication but they are known to have security and usability problems. Graphical password have been proposed as a alternative to text-based password, motivated by the fact that humans can remember pictures better than texts. Graphical passwords can be broadly categorized according to the memory task involved in remembering and entering the password are recall, recognition, and cued-recall [1].

A. Recall-based graphical password systems

In recall based graphical system the user has to reproduce something that user selected earlier during the registration stage. In this graphical password scheme retrieval is done without memory prompts or cues. Draw-A-Secret (DAS) is a recall based graphical system which allows users to use a set of gestures drawn on a grid to authenticate. The user's drawing is mapped to a grid & co-ordinate pairs used to draw the password in order. Background Draw a Secret (BDAS) is an extended form of DAS. The same grid is used as the original Draw a Secret, but a background image is simply shown over the grid. Passdoodle is another recall based system allows users to create a freehand drawing as a password (see Figure 2-c). It is similar to DAS. It uses more complex matching process without a visible grid and characteristics such as pen color, number of pen strokes, and drawing speed.

Figure 2: Recall-based system (a) Draw-A-Secret [11] (b) BDAS [12] (c) Passdoodle [12]

B. Recognition -based graphical password system

In Recognition based systems user must recognize their images from a portfolio of images. Recognition based techniques involve identifying previously selected images. The user must only be able to recognize previously seen images and not able to generate them unaided from memory. In Passfaces [9] recognition based system users preselect a set of human faces (see Figure 3-a). In Story system users first select a sequence of images for their portfolio. To log in, users must identify their portfolio images from among decoys. Users must select images in the correct order. Users were instructed to mentally construct a story to connect the everyday images in their set. In Déjà vu [10] system (see Figure 3-c) users select and memorize a multiple random art images from a larger sample for their portfolio. To log in, users must recognize images belonging to their pre-defined portfolio from a set of decoy images.

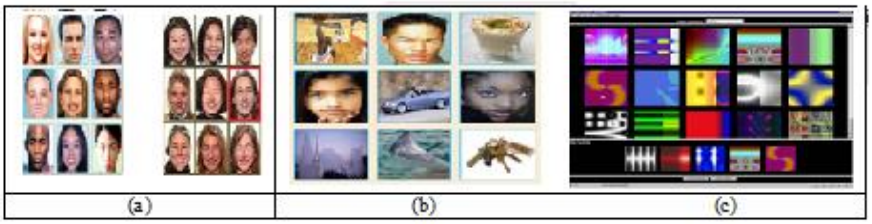

Figure 3: Recognition-based system (a) Passfaces [1] (b) Story system [1] (c) Déjà vu [1]

C. Cued-recall graphical password system

In a cued recall system, the user is provided with a hint to recall his password where user identify and target previously selected locations within one or more images. The images itself act as memory cues to aid recall. This feature intended to reduce the memory load on users and is an easier memory task than pure recall.

In pass point technique, password contains sequence of click points on a given image. The image is divided into tolerance squares. Users can select any points on the image as password in any order during registration stage. To login to the system the users have to correctly click on the same points in the image in correct order which is in the same tolerance squares as entered in the registration stage. The main drawback of this technique is pattern attack and brute force attacks are possible [5].

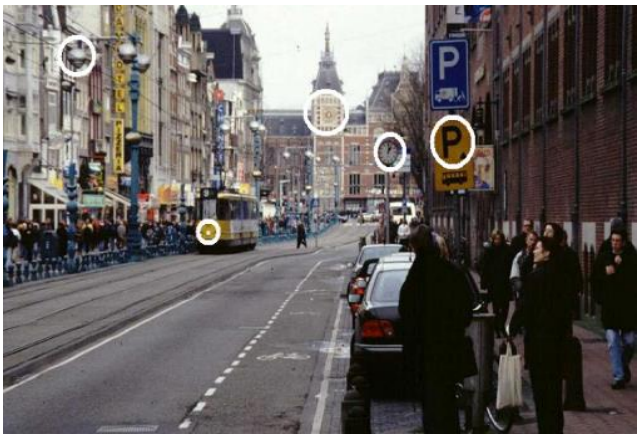

Figure 4: Pass Points

In Cued Click-Points (CCP) method users have to click on one point per image on five different images shown in sequence. To create a different password users have to click on different click points in different images. User testing and analysis [6] showed no evidence of patterns in CCP, so pattern-based attacks seem ineffective. Attackers must perform more work to exploit hotspots (attractive portion of image), results showed that hotspots remained a problem.

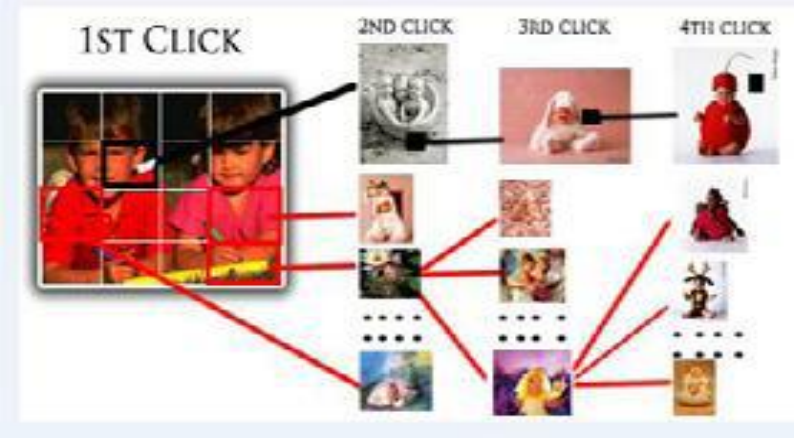

Figure 5: Cued Click-Points

III. EXISTING SYSTEM

Persuasive cued click point (PCCP) [7] work like CCP, but during registration the images are slightly shaded except for a small selected area (viewport). PCCP is designed to persuade users to select more random passwords. PCCP encourages users to select less predictable passwords. A password consists of the image which is shaded except for viewport that is randomly positioned on the image. Users select a click-point within this viewport or may press a "shuffle" [3] button to randomly reposition the viewport until a suitable location is found. The Persuasive Cued Click Points scheme is effective at reducing the number of hotspots while still maintaining usability. This system has the advantage of reducing the formation of hotspots across users since click points are more randomly distributed at the time of password creation users may shuffle as often as desired but it slows the process of password creation.

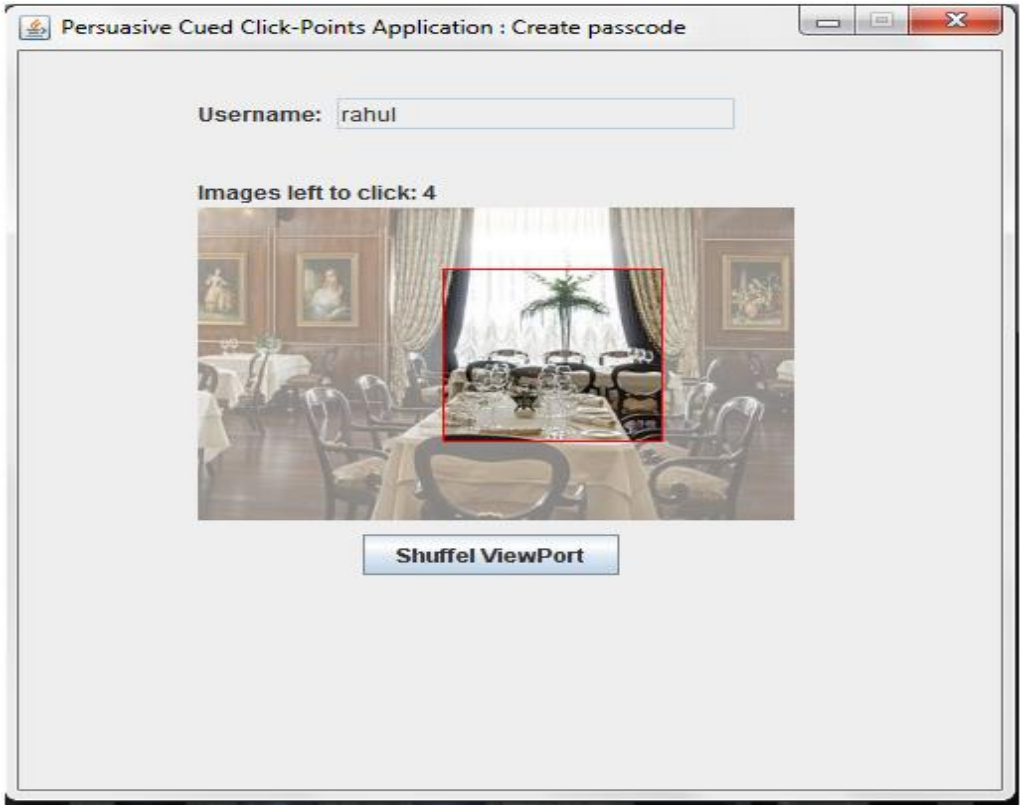

Figure 6: Persuasive cued click point

IV. **PROPOSED WORK**

Persuasive Technology influences user to select more difficult password for secure authentication. PCCP is a good technology but has accessibility problems. At the time of password creation users may shuffle as often as desired but it slows the process of password creation, it can take many clicks to shuffle view port on user wanted area which leads to increase in password creation time. In PCCP technique system generated view port indicate less attractive portion of image, but if user want to choose his click on less attractive part or on his/her wanted area users may get bored by clicking on shuffle button several time to get it.

Proposed system is mainly the **P**ersuasive **C**ued **C**lick **P**oints **T**wo **V**iew ports (PCCP-TV) based graphical password scheme having system assigned and user defined. In this, the process of click points is done for 6 numbers of images, in order to increase the security. First a Randomly generated viewport is assign by the system which guide user to select strong and memorable password. One random blocks of the image is selected as viewports (system generated viewport) and second block is move as a cursor (user defined viewport), rest of the image is blurred. System generated viewport can be shuffled to desired position, but this shuffling may take several clicks. So we provide user choice viewport which size is smaller than system generated viewport. We suggest users to select password within system generated viewport by giving message on screen while creation. By providing small viewport on the image we try to maintain the usability. Users may now select at anywhere on the images. This propose scheme look likes CCP scheme in which users can select password at any point on the image, But it differs with CCP because we provide both system generated and user defined viewport and suggest user to select password on system generated viewport.

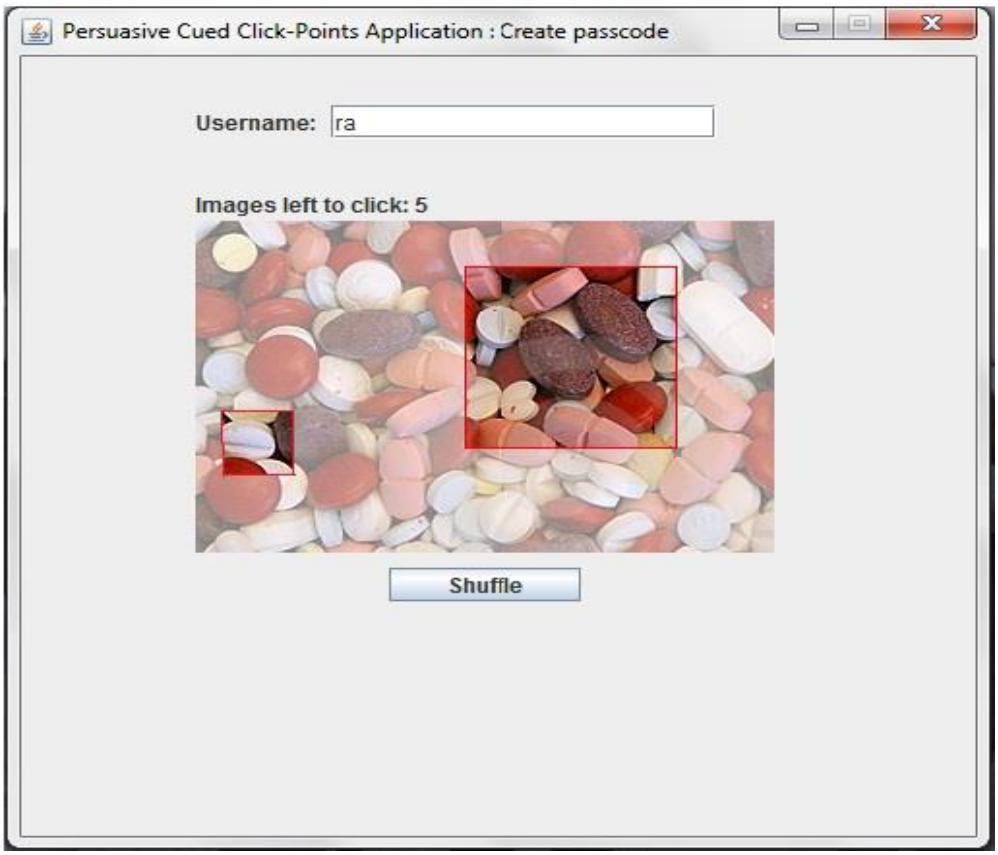

Figure 7: Persuasive cued click point with two viewports

A. Variations in Proposed Scheme

The propose scheme is divided into two sub schemes where user choice viewport is in different size. The following figure shows both schemes where figure 8 (a) have a viewport size one forth (25×25 pixel) of system generated viewport (100×100 pixel). Figure 8 (b) have a user choice viewport size 20×20 pixel.

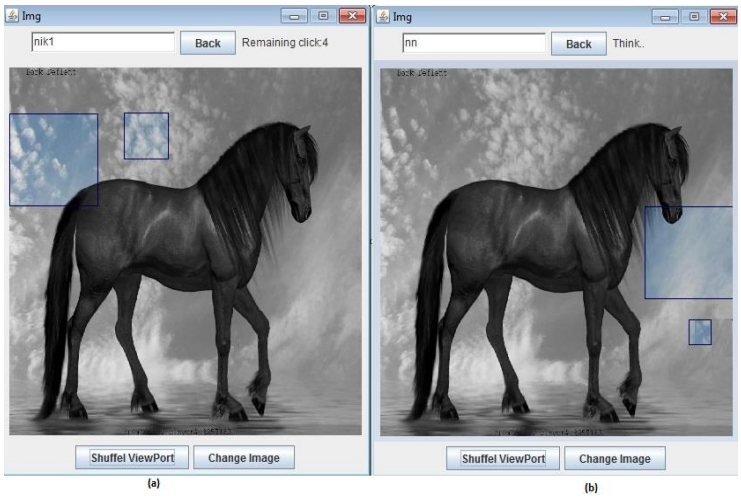

Figure 8: PCCP with TV having different user choice viewport size.

For identify the better technique among above, Five user study was conducted which will be discuss in result section.

B. Password creation Process

User must enter the unique user name. The first image is always same. User can select password from system generated viewport or by using user define viewport. The viewport is appears only at registration process. User may shuffle the system generated viewport to select password or use small viewport as mouse cursor. This process is repeated for 6 numbers of images. To increase the complexity, the number of images is 6 to be selected and given a click point as password.

C. Login Process

During login, the user must enter the user name first, if it present in database then only user can able to select the image. Both viewports and shuffle button will not appear at login process. User must select the same sequence of images which he/she selected during registration process. If first click point is correct then only user can able to see the next image, if not he will get wrong image. With this sequence, the process is done for 6 images.

V. **RESULTS**

Success rates are the number of trials completed without errors or restarts. Time for password creation and login affects the success rate of system. We conducted 3 user studies of the proposed techniques for both PCCP and PCCP-TV techniques. We gave three attempts to each user for creation process and found that existing system takes longer time as compare to proposed system:

	Password creation	time in second	
	PCCP	PCCP-TV (a)	PCCP-TV (b)
User 1	21-60 s	15-43 s	17-54 s
User 2	16-52 s	10-19 s	16-33 s
User 3	18-93 s	12-21 s	19-89 s

Table1: Time for password Creation process in both techniques.

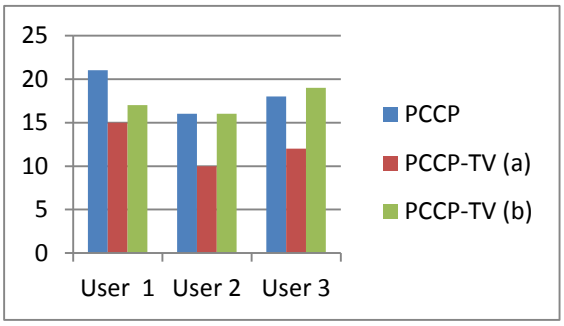

Figure 9: 3 User study shows that PCCP-TV systems takes less password creation time as compares to PCCP.

This user study shows that proposed scheme is more robust than existing one while maintaining the security. As per results the PCCP-TV (a) is more robust scheme. But when the security point of view arise user want to choose PCCP-TV (b) scheme.

VI. CONCLUSION

This paper for graphical passwords schemes shows that people are better at remembering picture passwords than text based passwords. Existing PCCP graphical password technique provides better security but have accessibility problem. Proposed system overcomes the drawbacks of PCCP technique by providing new user choice viewport. Proposed work provides better security while maintaining accessibility.

REFERENCES

1. R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM ComputingSurveys (to appear), vol. 44, no. 4, 2012.

2. XiaoyuanSuo, Ying Zhu, G. Scott, Owen, "Graphical Passwords: A Survey", Department of Computer Science, Georgia State University.

3. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud." Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems".International Journal of Human-Computer Studies, 2005.

4. "Christopher Mallow "Authentication Methods and Techniques".

5. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon."PassPoints: Design and longitudinalevaluation of a graphical password system". International Journal of Human-Computer Studies, 63(1-2):102 127, 2005.

6. S. Chiasson, P. C. van Oorschot, and R. Biddle."Graphical password authentication using Cued ClickPoints". In European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007.

7. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot."Inuencing users towards better passwords: Persuasive Cued Click-Points". In Human Computer Interaction (HCI), The British Computer Society, September 2008.

8. M. Mannan, T. Whalen, R. Biddle, and P. van Oorschot."The usable security of passwords based on digital objects: From design and analysis to user study". Technical Report TR-10-02, School of Computer Science, Carleton University, 2010.

9. Passfaces Corporation. The science behind Passfaces.White paper, http://www.Passfaces.com/ enterprise/resources/white_papers.htm, accessed July 2009.

10. R. Dhamija and A. Perrig. “Deja Vu: A user study using images for authentication”. In 9th USENIX Security Symposium, 2000.

11. T. Pering, M. Sundar, J. Light, and R. Want.“Photographic authentication through untrusted terminals”. Pervasive Computing, January - March 2003.

12. D. Weinshall. “Cognitive authentication schemes safe against spyware (short paper)”. In IEEE Symposium on Security and Privacy, May 2006.

13. S. M. Bellovin and M. Merritt. “Encrypted key exchange: Password based protocols secure against dictionary attacks”. In IEEE Symposium on Research in Security and Privacy, 1992.

14. P. Dunphy and J. Yan. “Do background images improve Draw a Secret" graphical passwords?” .In14th ACM Conference on Computer and Communications Security (CCS), October 2007.

15. D. Davis, F. Monrose, and M. Reiter. “On user choice in graphical password schemes”.In 13th USENIXSecurity Symposium, 2004.

