Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme

P. R. Devale, Shrikala M. Deshmukh, Anil B. Pawar

Abstract - Now a days, graphical password is used as an alternative to text-based passwords, biometric and tokens. We use Graphical passwords because peoples can remember images better than the text. The Graphical passwords are divided into three categories: click-based graphical password, choice-based graphical password and draw-based graphical password. In this paper, we combine the features of these three methods. Our proposed system is mainly the combination of Persuasive Cued Click Points and click-draw based graphical password scheme (CD-GPS). In this, users first choose an ordered sequence of 5 images and then select single image to click-draw their secrets. On remaining 4 images we select click points using features of PCCP (viewport and shuffle button). At the time of login images appear as per the decided sequence. For login user should click on the images for which we used features of PCCP for password creation and user should draw a secret on the previously selected image. By adding feature of secret drawing to PCCP , attackers fails to know that there is use of secret drawing technique on a image in between these images, unfortunately if they knows about secret drawing, they don't get exact idea that on which image secret has to done .Our proposed system provides higher security than other techniques.

KEYWORDS: Authentication, Graphical Password, images, security.

I. INTRODUCTION

In early days, text based passwords are used for authentication. Text based passwords are nothing but string of characters. For text passwords, peoples always creates password which is easy to remember but these passwords are easy for attackers to break. For more security, users use strong system assigned passwords which will be difficult for users to remember [1] [17].Biometric and tokens are used as an alternative to text based passwords but has its own drawbacks such as it requires extra hardware so these methods are costly.

As an alternative to all these methods, graphical passwords are used because psychology studied that human brain can recognize images better than the text [5].Graphical passwords are of three types: Click based graphical password scheme, choice based graphical password scheme and draw based graphical password scheme.

Pass-Points:

Pass-Point comes under click based graphical password scheme. In Pass-Points password consists of sequence of 5 different click points on a single image. The main disadvantage of this scheme are HOTSPOTS [11] [12] and pattern formation attacks [13] [14].

Manuscript received on May, 2013.

P.R.Devale, Prof.P.R.Devale is the Head of Information Technology Department in the College of Engineering, Bharati Vidyapeeth, Pune, India.

Shrikala Madhav Deshmukh, has completed B.E.(I.T.) & pursuing M.Tech(I.T.) in College of engineering,Bharati Vidyapeeth,Pun, India.

Anil Baburao Pawar, has completed B.E(I.T) & pursuing M.E.(C.N.) at SIT,Lonaval, India.

Cued Click Points:

Cued Click Points comes under click-choice based graphical password scheme. Cued Click Points [1] [15] was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Instead of five click-points on one image, CCP uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point. One best feature of Cued Click Point is that the message of authentication failure is displayed after the final click-point, to protect against incremental guessing attacks. But this technique has several disadvantages like false accept (the incorrect click point can be accepted by the system) and false reject (the click-point which is to be correct can be reject by the system).In this system pattern formation attack is reduced but HOTSPOT remains since users are selecting their own click-point [10].

Persuasive Cued Click Points:

Persuasive Cued Click Points comes under click-choice based graphical password scheme. By adding a persuasive feature to CCP [1] [15], PCCP [1] encourages users to select less predictable passwords, For password creation PCCP uses terms like viewport & shuffle. To avoid known hotspots the viewport is positioned randomly. The most useful advantage of PCCP is attackers have to improve their guesses.

Click Draw based Graphical Password Scheme:

There are mainly two steps in this scheme:

1. Image selection
2. Secret drawing. [2]

In first step, an image is selected amongst various images in the image pool. In second step, secret is drawn on the selected image. It has the advantage that in this technique there is not necessity to remember the sequence of clicks. But this system has disadvantage that attackers can guess the image on which secret is done and what type of secret is done.

In this paper we proposed a system in which we combine the features of PCCP & Click Draw Based Graphical Password Scheme. In this project the first step is to select 5 images from the image pool of 20 images. After that in second step we select single image from previously selected 5 images. On this image we have to draw a secret by considering the coordinates & for remaining 4 images we use features of PCCP i.e. by using viewport & shuffle button to create password. This is simply the password creation process of PCCP with secret draw technology. At the time of login images appear as per the decided sequence. For login user should click on the images for which we used features of PCCP (i.e. viewport and shuffle button) for password creation and user should draw a secret on the previously selected image.

Our proposed scheme has various advantages such as it will be hard for attackers to guess the password because using feature of PCCP, pattern formation attacks and hotspots will be removed using viewport & shuffle button. By adding feature of secret drawing to PCCP, attackers fails to know that there is use of secret drawing technique in between these images unfortunately if they knows about secret drawing, they don't get exact idea that on which image secret has to done .The one more advantage is that the message of correct password or incorrect password is displayed after the click on last image, by this feature it will hard for attackers to find on which image their guess is correct or incorrect. So by this our proposed scheme will provide higher security in authentication.

II. BACKGROUND

Previously various Graphical Password techniques were introduced. Some of the techniques are given below,

Pass-point Scheme

S. Wiedenbeck et al. [6] [8] [9] proposed pass-point graphical password scheme in which on a given image password consists of a sequence of 5 different click points. For password creation user selects any pixel in the image as a click-points and for login the user has to enter the same series of clicks in correct sequence within a system defined tolerance square of original click-points.

The problem with this scheme is the HOTSPOTS [11][12](the area of an image where user more likely to select the click-point) and it is easy for attackers to guess the password because user forms certain patterns[13][14] in order to remember the secret code which results pattern formation attacks are easily possible. Thus the pass-point system suffers from these two major disadvantages. To overcome these disadvantages next technique is to be implemented.

Fig 3: Pass-Points [10]

Cued Click Points

Cued Click Points [1] [2] [15] was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Instead of five click-points on one image, CCP uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point; it creates a path through an image set. Creating a new password with different click-points results in a different image sequence.

One best feature of Cued Click Point is that the explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks.

But this technique has several disadvantages like false accept (the incorrect click point can be accept by the system) and false reject (the click-point which is to be correct can be reject by the system).In this system pattern formation attack is reduced but HOTSPOT remains since users are selecting their own click-point [10].

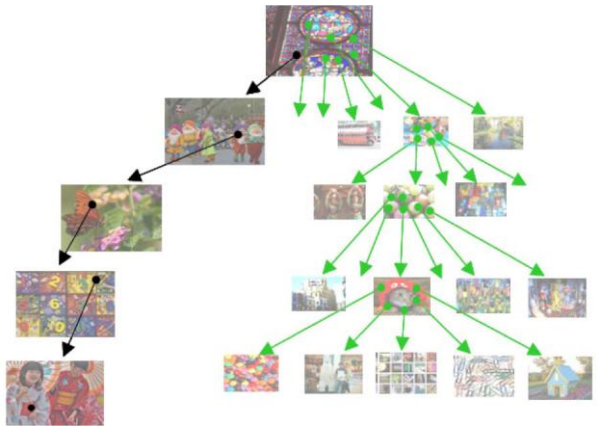


Fig. Cued Click Points

Persuasive Cued Click Points

For creating Persuasive Cued Click Points persuasive feature is added to CCP.PCCP [1] encourages users to select less predictable passwords. For password creation PCCP uses terms like viewport & shuffle. When users creating a password, the images are slightly shaded except for a viewport as shown in the fig. to avoid known hotspots the viewport is positioned randomly. The most useful advantage of PCCP is attackers have to improve their guesses. Users have to select a click-point within the highlighted viewport and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport [1].At the time of password creation users may shuffle as often as desired but it slows the process of password creation. Only at the time of password creation, the viewport & shuffle button appears. After the password creation process images displayed normally without the viewport & shuffle button. Then user has to select correct click on particular image. PCCP is a good technology but has security problems. Fig. shows the password creation process including viewport & shuffle button.

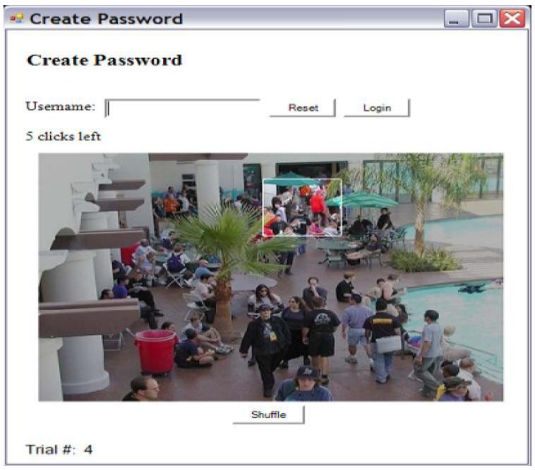


Fig. password creation in PCCP. Highlighted area is viewport (pool image is taken from [16], [1])

CLICK-DRAW BASED GRAPHICAL PASSWORD SCHEME

The purpose of click-draw based graphical password scheme (CD-GPS) [3] is to enhance the image-based authentication in both security and usability. There are mainly two steps in this scheme:

1. Image selection
2. Secret drawing.

1. Image selection

In CD-GPS, the first step is the image selection. In this step users have to select several images from an image pool. Suppose there are N1 images in the image pool, then at first users should select n ∈ N1 images from the image pool in an order and remember this order of images like a story. Users should further choose k ∈ n image from the above selected n images. k is nothing but the single image on which we have to draw secret. [3]

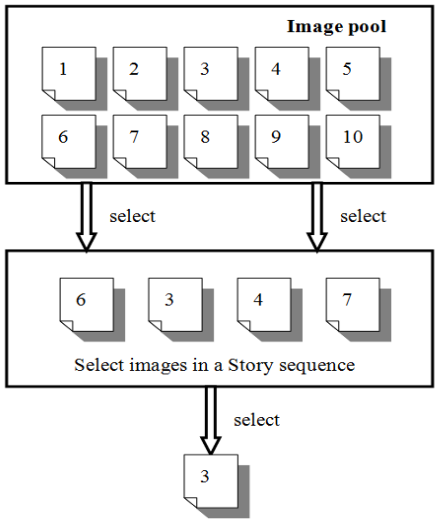


Fig. image selection in click draw based graphical password scheme [3].

As shown in Fig, there are total 10 images in the image pool i.e.N1 images. Users should first select 4 images from the image pool in story-sequence i.e. n images (e.g., {6, 3, 4, 7}).Then users should further select 1 image i.e. k image (e.g., {3}) from the above 4 selected images to draw the secret.

2. Secret drawing.

This is the second step comes after the image selection. In this step users can freely click-draw their secrets. For constructing secret drawing users use series of clicks

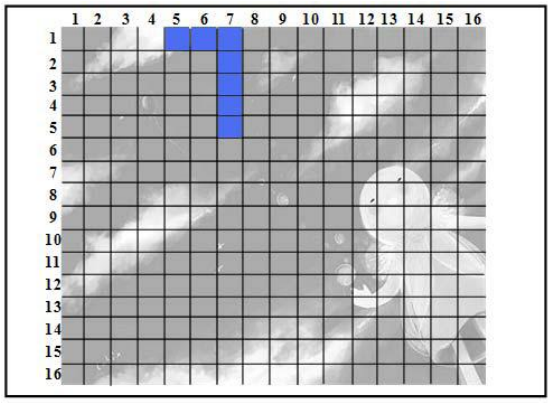


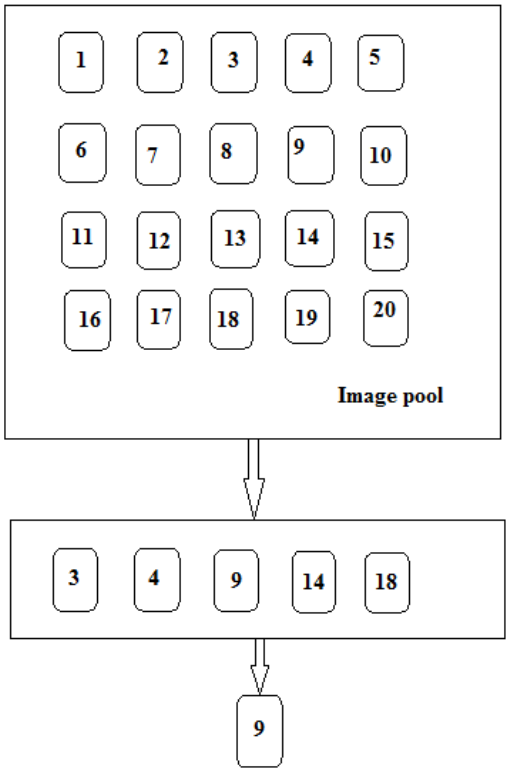
Fig. user draws number “7” as the secret

As shown in above fig. the image is divided into a 16×16 table. Users can use the coordinate numbers for remembering their drawings. In above fig. user draw number “7” as the secret,

Which consists of coordinates (1, 5), (1, 6), (1, 7), (2, 7), (3, 7), (4, 7) and (5, 7). In this technique there is not necessity to remember the sequence of clicks. During the authentication, users should re-draw their secrets accurately in the correct coordinates on the image [3].

III. PROPOSED SYSTEM

In this paper we proposed a system in which we combine the features of PCCP & Click Draw Based Graphical Password Scheme.

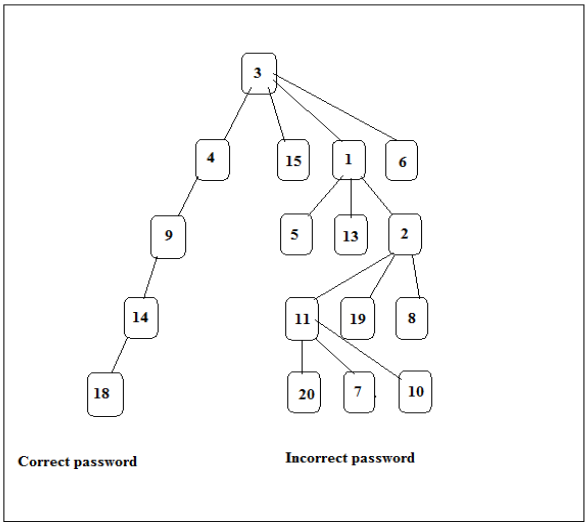


As shown in above fig. there is an image pool of 20 images(1 to 20) from which in the first step we simply select 5 images(3,4,9,14,18).After that in second step we select single image(9) from previously selected 5 images.

So, on the image number 9 we have to draw a secret by considering the coordinates & for remaining 4 images (i.e.3, 4, 14, 18) we use features of PCCP i.e. by using viewport & shuffle button we are required to create password on these 4 images. This is simply the password creation process of PCCP with secret draw technology.

After password creation, during login as shown in following fig at first image 3 will be displayed, if we click on the correct click point of that image then image 4 will be displayed but if one can failed to click on the correct click point of image 3 then several other images will be displayed. Same for image 4, if user clicks at correct click point then image 9 will be displayed otherwise several other images from the image pool will be displayed. Then on image 9 we have to draw a secret because previously in password creation we selected that image for secret drawing. If we draw correct secret on image 9, image 14 will be displayed otherwise several other images from image pool will be

displayed. On image 14 user have to click at correct click point which is decided at password creation process using viewport & shuffle button, if it is correct then image 18 will be displayed otherwise several other images from image pool are displayed. When user clicks at correct click point on image 18, then it displays that "Your password is correct" & it will authenticate the user. When user fails to click at correct point on last image then it will display that "You have entered incorrect password. Try again."



IV. CONCLUSION

Our proposed scheme has various advantages such as it will be hard for attackers to guess the password because using feature of PCCP pattern formation attacks and HOTSPOTS will be removed using viewport & shuffle button. By adding feature of secret drawing to PCCP, attackers fails to know that there is use of secret drawing technique in between these images, unfortunately if they knows about secret drawing, they don't get exact idea that on which image secret has to be done .The one more advantage is that the message of correct password or incorrect password is displayed after the final click only, by this feature it will hard for attackers to find on which image their guess is correct or incorrect. So by this our proposed scheme will provide higher security in authentication.

REFERENCES

[1] Sonia Caisson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget,Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE "Persuasive Cued Click Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012

[2] Sonia Chiasson1,2, P.C. van Oorschot1, and Robert Biddle2 "Graphical Password Authentication Using Cued Click Points" 1 School of Computer Science, Carleton University, Ottawa, Canada 2 Human-Oriented Technology Lab, Carleton University, Ottawa, Canada(chiasson,paulv)@scs.carleton.ca, robert biddle@carleton.ca

[3] Yuxin Meng "Designing Click-Draw Based Graphical Password Scheme for Better Authentication" 2012 IEEE Seventh International Conference on Networking, Architecture, and Storage

[4] Karen Renauda Department of Computing Science, University Of Glasgowkaren@dcs.gla.ac.uk "Quantifying the Quality of Web Authentication Mechanisms A Usability Perspective"Journal of Web Engineering, Vol. 0, No. 0 (2003) 000–000_c Rinton Press.

[5] Nelson, D.L., U.S. Reed, and J.R. Walling. Picture Superiority Effect. Journal of Experimental Psychology: Human Learning and Memory 3, 485-497, 1977.

[6] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, and N. Memon. "PassPoints: Design and longitudinal evaluation of a graphical password system". International Journal of Human Computer Studies, 2005.

[7] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. Proceedings of the Eighth USENIX Security Symposium, pages 1–14, 1999.

[8] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Toler-ance and Image Choice," Proc. First Symp. Usable Privacy and Se-curity (SOUPS), July 2005.

[9] Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme," Proc. Third ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[10] Ms. Uma D.Yadav and Mr. P. S. Mohod,"Enhancement of Knowledge Based Authentication Mechanism using Graphical Password via Persuasion" JOURNAL OF COMPUTER SCIENCE AND ENGINEERING, VOLUME 17, ISSUE 2, FEBRUARY 2013

[11] K. Golofit, "Click Passwords under Investigation," Proc. 12th European Symp. Research in Computer Security (ESORICS), Sept. 2007.

[12] A. Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme," Proc. Third ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[13] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387-398, 2009.

[14] A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "On Purely Automated Attacks and Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2008.

[15] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.

[16] PD Photo, PD Photo Website, http://pdphoto.org, Feb. 2007.

[17] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.

Prof.P.R.Devale is the Head of Information Technology Department in the College of Engineering, Bharati Vidyapeeth, Pune. He has completed M.E.(computer) & pursuing PHD.

Miss. Shrikala Madhav Deshmukh has completed B.E.(I.T.) & pursuing M.Tech(I.T.) in College of engineering,Bharati Vidyapeeth,Pune.

Mr.Anil Baburao Pawar has completed B.E(I.T) & pursuing M.E.(C.N.) at SIT,Lonavala.