International Journal of Computer Applications Technology and Research
Volume 4– Issue 9, 633 - 639, 2015, ISSN: 2319–8656

Evaluation of a Knowledge Based Authentication Mechanism through Persuasive Cued Click Points

Y.Sravana Lakshmi
Computer Science and Engineering
BVSR Engineering College
Chimakurthy, India

Abstract: Authentication is the first line of defence against compromising confidentiality and integrity. Password protection is a security process that protects information from unauthorized user. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of very high security, in the sense of being from an expanded effective security space. We use persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-point. This paper presents an integrated evaluation of the persuasive cued click-points graphical password scheme, including usability and security evaluations, and implementation considerations. It reflects a proposed system which uses graphical password using knowledge based authentication mechanism. Users select their images for any click points and for one click point display the next image having a specific relational order. The use of inclusive exclusive principal can be applied to find the minimum or maximum number of images required to form the image sequence reducing shoulder surfing problem.

Keywords: Cued Click-Points; Graphical password authentication; Inclusive- Exclusive principal; Shoulder surfing; Knowledge-based authentication.

1. INTRODUCTION

Beginning around 1999, a multitude of graphical password schemes have been proposed, motivated by the promise of improved password memorability and thus usability, while at the same time improving strength against guessing attacks. Like text passwords, graphical passwords are knowledge-based authentication mechanisms where enter a shared secret as evidence of their identity. Graphical passwords are of three types:

- Click based graphical password scheme
- Choice based graphical password scheme
- Draw based graphical password scheme

According to person psychology, humans are able to memorize pictures simply. Users are creating unforgettable passwords like text and symbols passwords that are easy for crack hackers to guess, but strong system-assigned passwords are difficult for users to remember. Computer security systems should also consider the human factors such as ease of a use and accessibility. Present secure systems undergo because they typically ignore the importance of human factors in security. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory load on users, coupled with a larger full password space offered by image, Thumb impression, digital signatures, mobile passwords, more secure passwords can be produced and users will not resort to insecure practices in order to extent.

The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. A password authentication system should encourage strong passwords while maintaining memorability. Rather than increasing the burden on users, it is easier to follow the system's suggestions for a secure password a feature lacking in most schemes.

The approach to create the first persuasive click-based graphical password system, Persuasive cued click-points (PCCP) and conducted user studies evaluating usability and security. This systematic examination provides a comprehensive and integrated evaluation of PCCP, covering both usability and security issues, to advance understanding as in prudent before practical deployment of new security mechanisms. The images act as memory cues to aid recall. Example systems include Pass points and Cued Click-Points.

In Passpoints, passwords consist of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click points. Although Paasspoints is relatively usable security weaknesses make passwords easier for attackers to predict. Hotspots are the areas of the image that have higher likelihood of being selected by users as password click points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess Passpoints passwords. Users also tend to select their click points in predictable patterns. By adding a persuasive feature to CCP, PCCP, encourages users to select less predictable passwords, and makes it more difficult to select passwords where all five click points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a viewport. The viewport is positioned randomly, rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots.

The viewports size is intended to offer a variety of distinct points but still cover only an acceptable small fraction of all possible points. Users must select a click-point within this highlighted viewport and cannot click outside of the viewport, unless they press the shuffle button to randomly reposition the viewport. While users shuffle as desired, this significantly slows password creation. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images.

Password capture attacks occur when attackers directly obtain passwords by intercepting user entered data, or by tricking users into revealing their passwords. For systems like PCCP, CCP, and Passpoints, capturing one login instance allows fraudulent access by a simple replay attack. An alternative to increasing the number of images is to use larger images but crop them differently for each user. Hotspot analysis would be more difficult for attackers because the coordinates of hotspots could not be directly applied across accounts. If furthermore, each user receives a different pool of images, an attacker would need to collect these data on a peer-user basis when launching an attack.

To overcome all these existing defects we provide an authentication scheme in which the user choice of selecting the password scheme plays a vital role. This method also provides a more secure password scheme. The use of persuasive technology persuades the user choicer of selecting the password. The graphical passwords use a click based authentication scheme. The persuasive cued click point's method uses the concept of persuading the user to select the password. Here the prediction of password is difficult for the hackers as it is generated in a random manner.

2. PROPOSED SYSTEM

The user will provide an option of selecting the hotspots in an image. The successive selection of the exact hotspots will enable the user to move the next successful images. For login into the system, the user will provide an option of selecting the hotspot in the continuous 5 images. After reaching the successful login attempt the user will be allowed to access the application. Storing the images in a secure database through file stream data type is one of the options used to secure the images instead of storing the images in the server. Users will be provided an option of selecting the images to create the authentication page which is not included in the existing system. Possibility of monitoring the hotspots by the nearby user is possible. To avoid the same the password with matrix formation is one of the complex password schemes in the world. This option is been added in this paper.

Advantages:

Integrated evaluation of the password scheme in graphical manner.
Users will be provided an option of selecting the images to create the authentication page.

2.1 Persuasive Cued Click Points

For creating persuasive Cued Click points persuasive feature is added to CCP.PCCP encourages users to select less probable passwords. For password generation PCCP uses requisites like viewport & shuffle. When users making a secrete word, the images are a little monochromic except for a viewport for to avoid known hotspots the viewport is positioned casually. The most useful benefit of PCCP is hackers have to improve their presumptions. Users have to choose a clickable area within the highlighted view port and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport. At the time of password creation users may shuffle as often as desired but it slows the process of password generation. Only during the password generation, the viewport & shuffle buttons are displayed. After the secrete word generation process, graphical images are presented to users casually without the viewport& shuffle button. Then user has to choose exact clickable area on particular image. Now a day's PCCP is a best technology but has security problems. Using this method HOTSPOT problem is reduced, but this method is difficult to remember the exact clickable area.

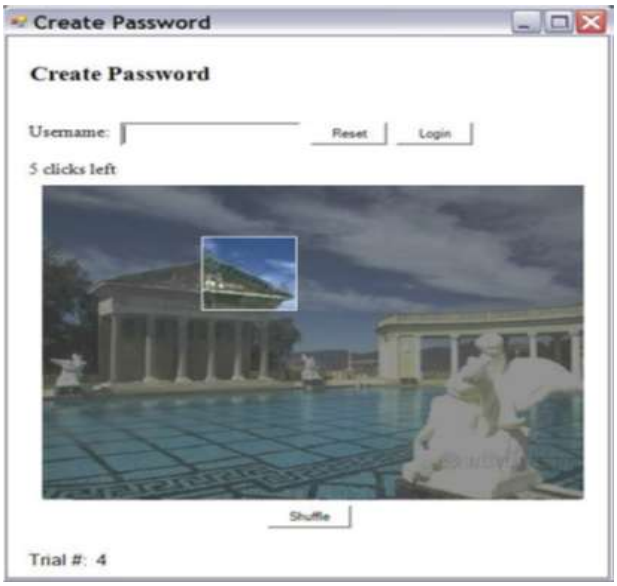

Figure 1. Persuasive Cued Click-Points. During password creation, users select a click-point from the highlighted viewport or press the shuffle button to relocate the viewport.

3. SYSTEM DESIGN

The system designed consist of three modules such as registration module, picture selection module and system login module (see Figure 2).

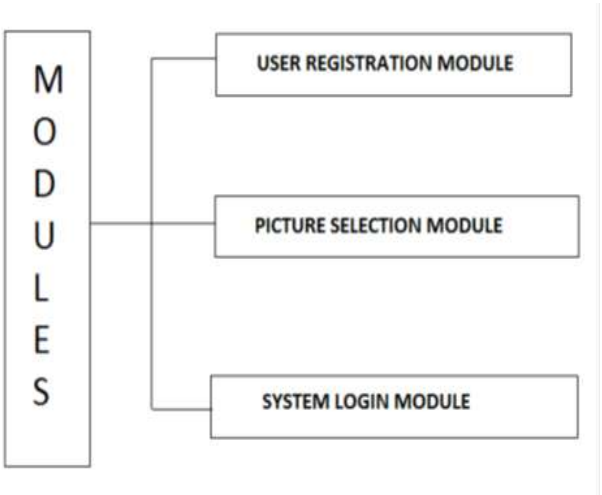

Figure 2. System design modules

3.1 User Registration Flow Chart

Below flowchart (see figure 3) shows the user registration procedure, this procedure include both registration phase (user ID) and picture selection phase. The process flow starts from registering user id and tolerance value. Once user completes all the user details then precede to next stage, which is selecting click points on generated images, which ranges from 1-5. After done with all these above procedure, user profile vector will be created.

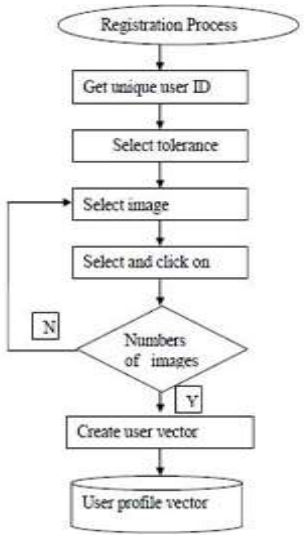

Figure 3. User registration flow chart

3.2 Login Flow Chart

In this login procedure (see figure 4), first user enters the unique user ID as same as entered during registration. Then images are displayed normally, without shading or the viewport, and repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. After done with all these above procedure, user profile vector will be opened.

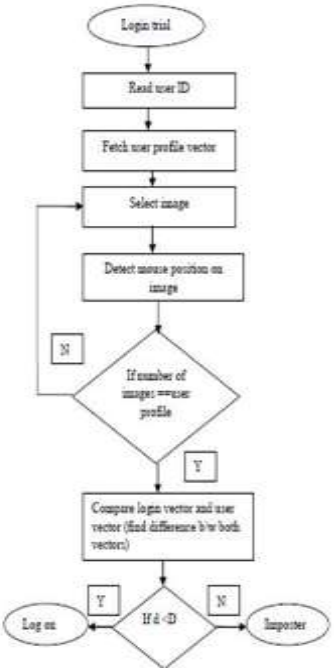

Figure 4. Login phase flowchart

4. MODULES

4.1 Authentication Scheme Module

In this module, the user will be permitted to provide their valid credentials to login in to the system. Before finalizing the validation of the user, they need to cross two level of boundaries. The first check will be the matrix validation. Once the user provides valid data, he will be allowed for the second check. In the second check users will be checked for the valid hotspot of the images. He will be permitted to view his profile page. If more than a stipulated time, the user has tried the login. In that case, the user will be blocked permanently and it can be overcome by the admin.

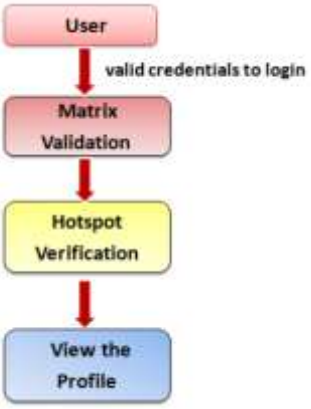

Figure 5. Authentication Scheme Module.

4.2 Matrix Verification Module

In this module, the user needs to enter the correct username. After entering, an 8*8 matrix is formed and it's displayed to the user. The user needs to verify the color combinations in the matrix. Based on the intersection of the input value provided by the user during registration, the matrix will be manipulated and the user needs to provide the exact intersection points are valid; he will be authorized user, so that he will be allowed for the second level of validation.

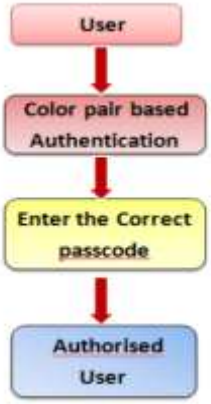

Figure 6. Matrix Verification Module.

4.3 Hotspot Verification Module

In this module, users will be provided with an image. If the user clicks the correct hotspots, then he will be the authorized user to access the application. If the user clicks the fake hotspots, then he will not be the authorized user to access the application.

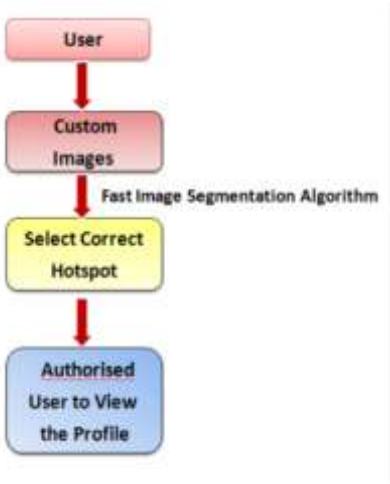

Figure 7. Hotspot Verification Module

5. GRAPHICAL PASSWORD METHOD USING KNOWLEDGE BASED AUTHENTICATION

Graphical password considers there are five images. There are five click points on one image. The next image displayed is based on the relation on the location of the previously entered click point creating a path through an image set. Users select their images for any click points and in return for once click point another click point and again it will display next image having relational order of second image click point and so on. In PCCP limitations all images could be reused at each stage in the password for every user. This strategy has the highest probability of collision where a user clicks on an incorrect click-point.

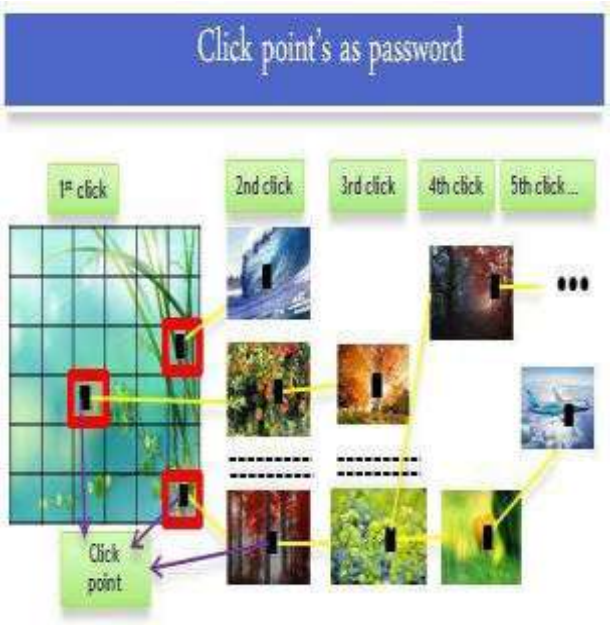

Figure 8. PCCP passwords as a choice-dependent path of images.

Using PCCP implementation, there is a possibility that images are reused for a given user. While this poses a potential usability concern, the likelihood of this happening is correspondingly low with enough images. In this technique reused images are not used for different users. If any image sequence is selected by a user then same image sequence is not available for any other user. This means same image sequence is not used by two different users for the authentication. It is proposed to select different image sequences according to a specific relational order. Due to this when the user clicks on the image, the possibility of any collision is minimized. This probability can be reduced or nearly eliminated if the overlap of images is reduced between password stages by increasing the number of images in a users set. An alternative for increasing the no. of images is to use larger images. We can make a different set of images for each user, because hotspot analysis would be more difficult as suggested in PCCP.

6. EVALUATION OF PERFORMANCE AND RESULTS

6.1 Evaluation of Performance

In this evaluation of performance chapter we evaluated the usability of PCCP: with CCP through performance measures. The distributions contain all user-chosen click points for the given scheme for graphical passwords that were, at smallest amount, effectively re-entered at least once during login. In the Figure 9, this random distribution would appear as a curved diagonal line. In comparison, the PCCP graph shows that in the worst case, half of all click-points are confined within the most popular 0.00075 percent of hotspots within the distribution, while in the best case 0.00200. This indicates that CCP click-points have a flatter distribution and thus an attack dictionary based on hotspots should be less effective for CCP than for the other schemes. This analysis focused on individual click-points, not complete passwords. A key feature in PCCP and CCP is that creating a harder to guess password is the path of smallest resistance, likely making it more useful than schemes where secure behavior adds an extra problems on users. The approach has proven successful at reducing the formation of hotspots and patterns, thus growing the good space.

6.2 Results

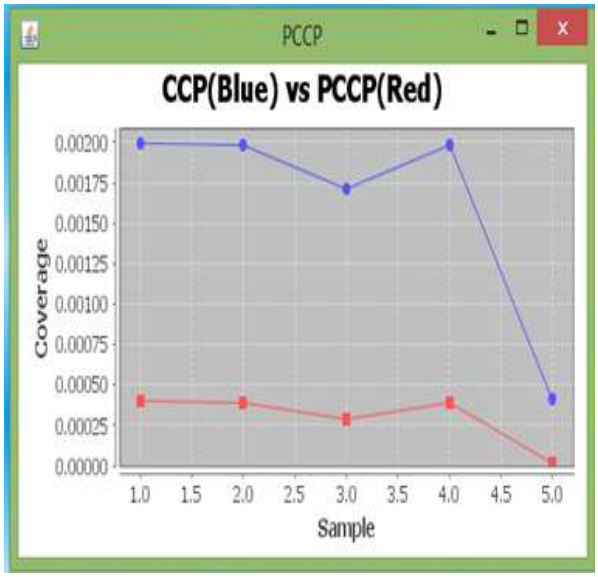

Figure 9. Cumulative frequency distribution of hotspot coverage for CCP&PCCP

Table 1. Input parameters of CCP and PCCP for calculating coverage ratio

Images	Height	Width	Click Area	View Port Height	View Port Width	PCCP Coverage Ratio	CCP Coverage Ratio
Image 1	177.0	284.0	10*10	100	100	0.00039575	0.00198934
Image 2	168.0	300.0	10*10	100	100	0.00039368	0.00198413
Image 3	210.0	278.0	10*10	100	100	0.00028341	0.00171292
Image 4	168.0	300.0	10*10	100	100	0.00039368	0.00198413
Image 5	387.0	620.0	10*10	100	100	0.00001737	0.00041677

Equations used in coverage ratio calculation:

Image click ratio (10 10) (height width)

View port ratio (100 100) (height width)

PCCP coverage ratio image click ratio view port ratio

CCP coverage ratio image click ratio

In this Figure .9, the performance of the CCP and the performance of PCCP measure the coverage results in the number of input samples. The number of input samples are shown in the X axis and the coverage of the result are measured in Y axis. The CCP and PCCP measure the coverage result in the number of input samples; it shows that the proposed CCP coverage is most important result in the samples. CCP's segments were the longest and within range of the random distributions. Given that no other spatial patterns are apparent for PCCP. This proposed work suspects that these shorter segments are an artifact of the viewport positioning algorithm, which vaguely favored more focal areas of the image.

Image click ratio is measured based on the width and height in the original image. The height and width was changed according to the image was used in the application. In this proposed work we, measured the image click ratio for each and every image used in the project work. If we taken 5 images the image ratio is measured to five images. The viewport is situated randomly, rather than explicitly to avoid known hotspots, since such statistics might allow hackers to improve guesses and could lead to the formation of new hotspots. The viewports size is anticipated to proposal a variety of distinct points but still cover only an acceptably small fraction of all possible points. View port ratio is calculated based on the rectangle boundary was selected in the image; their corresponding height and width are selected measure the view port.

7. TASKS

Ease of login is the most frequently examined task, but is only one of many. Ideally, usability should be explored along several dimensions. For usability, essential elements to measure and report include: time to create a password, and time to login: memorability (typically through success rates and number of errors made during login over an extended period): and interference, by testing with a normal password load (as opposed to with only one password at a time).

Password Initialization

Authentication systems require initialization. A graphical password can either be assigned or user selected. In PCCP the middle ground between allowing user choice and system assigned passwords led to passwords nearly indistinguishable from random on the measures examined. Further works needed to evaluate the effect on long-term memorability.

Login

Login should be quick and simple since it is the most common task completed by users of an authentication system. Memorability issues are important when discussing login performance, as memorability is a main factor determining login success. Most graphical password studies to date required users to remember only one password at a time, whereas in real life users must remember many passwords and may get them confused. With authentication, interference occurs when remembering a password for one system impairs the users memory of a password for another system. This may be of particular concern with graphical passwords since exposure to similar images from multiple concurrent passwords or from password resets may aggravate the problem.

Password reset and password change

The tasks of resetting or changing passwords are not typically examined during usability testing of new graphical password schemes, but these are often required in practice when users forget passwords. The process may involve the user interacting only with the system, or may require contact with help desk personnel. System configuration and design of password reset and password change mechanisms can impact memorability, interference, and security of the system. For example, if the users are presented with the same, or similar, images as in previous graphical passwords, they may be more likely to confuse the memories of passwords or to reuse passwords. This suggests that reuse of password images should be avoided, and also argues against images being uploaded by users. Most authentication systems must allow password changes. The usability and security concerns are similar to password reset, except users can complete the task themselves without requiring a temporary password, entering their current graphical password as authentication.

Portable login

Unless restricted to specific environments users of graphical password systems may need to log in from different physical devices or locations. Usability issues to consider include whether the system is suitable for access from devises having different screen sizes or resolutions, and whether local bandwidth constraints impact performance. Moreover, portable login may require a modified login process or completion of additional tasks; these should also be considered and tested.

Shoulder-surfing

`Shoulder-surfing is targeted attack exacerbated by the visual aspect of graphical passwords. As users enter login information, an attacker may gain knowledge about their credentials by direct observation or external recording devices such as video cameras. High resolution cameras with telephoto lenses and surveillance equipment make shoulder-surfing a real concern if attackers target specific users and have access to their geographic location. Several existing graphical schemes believed to be resistant or immune to shoulder-surfing have significant usability drawbacks, usually in the time and effort required to log in, making them less suitable for everyday authentication. Multi-touch tabletop interfaces support novel approaches offering shoulder-surfing resistant properties. For some graphical

[passwords, multiple successful logins must be observed to deduce the full password. Passwords in other schemes can be recovered from one successful login.

8. SECURITY

An authentication system must provide adequate security for its intended environments; otherwise it fails to meet its primary goal. A proposed system should at minimum be evaluated against common attacks to determine if it satisfies security requirements. We classify the types of attacks on knowledge-based authentication into two general categories; guessing and capture attacks. In successful guessing attacks, attackers are able to either exhaustively search through the entire theoretically password space, or predict higher probability passwords so as to obtain an acceptable success rate within a manageable number of guesses.

Password capture attacks involve directly obtaining the password, or part thereof, by capturing login credentials when entered by the user. Shoulder-surfing, phishing, and some kinds of malware are common forms of capture attacks. In shoulder-surfing, credentials are captured by direct observation of the login process or through some external recording device such as a video camera. Phishing is a type of social engineering where users are tricked into entering their credentials at a fraudulent website recording user input. Malware uses unauthorized software on client computers or servers to capture keyboard, mouse, or screen output, which is then parsed to and login credentials..

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 dividing into more blocks there is a less chance for hotspot issue in the generated block.

Table 2. 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.

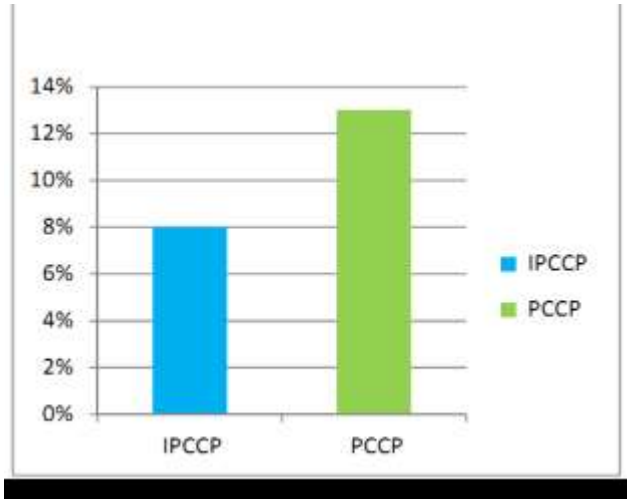

Figure 10. Comparison of hotspot occurrence percentage of two schemes.

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 both single 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.

9. RESULTS AND ANALYSIS

The study and analysis of normal point (CCP) and persuasive cued click point (PCCP) was designed to explore ways of increasing the efficiency of tolerance value and also conducted lab study for comparison between login success rate and security success rate of existing CCP's and proposed PCCP's.

Efficiency of the tolerance value

Initially eight participants are considered for the experiment. Each participant has a unique password which includes clicking on 5 click points in 5 different images. Each image contain of different characters, among which the participant needs to click on any one point of his choice to make it a click point in the series. Similarly the participant select a click point each of the images. Then, the participant logs in with that password, meantime the other participants are made to stand in a group behind the participant who is entering the password and are made to peek in over the shoulder of the participant and observe his password. The first participant has logged out once, the other [participants are asked to enter the same password which they have observed of the first participant.

Tolerance value: It is the value which defines the degree of closeness to the actual click point.

Tolerance region: The area describes an original click point is accepted as correct since it is unrealistic to expect user to accurately target an exact pixel.

Success rate: It is the rate which gives the names of successful trails for a certain number of trails, the success rates calculated as the number of trails given completed without errors or restarts.

Table 3. Results of tolerance value efficiency of the PCCP method

No	Tolerance value	Success rate	Percentage of success rate	Security (in percentage)
1	5	7/8	87.5	12.5
2	4	6/8	75.8	37.5
3	3	3/8	37.8	62.5
4	2	2/8	25	75
5	1	0/8	0	100

10. CONCLUSION

Published research in the area of graphical passwords currently lacks consistency, making it different to compare or reproduce results. A closer look at individual systems has typically revealed less security than promised; matching historical early experience in other areas usually repaired with maturity. The main purpose of authentication schemes is to allow system access only by legitimate users. To thoroughly evaluate the security of a graphical password proposal, and to facilitate comparison with alternatives, all standard threats and known attacks should be analyzed, with convincing arguments o how a scheme precludes them.

We expect tomorrow's ideal graphical password systems may have many of the following desirable characteristics, reecting lessons learned from proposals to date.

1. Theoretical password space meeting the security policy of the intended domain.

2. Avoidance of exploitable reductions in security due to user choice of passwords, e.g., through persuading password choice towards attar distributions.

3. At least mild resistance to different types of capture attacks including shoulder surfing and key logging, through variable response design.

4. Cues aiding memorability, design features minimizing password interference.

5. Usability as close as possible to, or better than, text passwords.

6. Implicit feedback to legitimate users, when passwords are multi-part.

7. Leveraging of pre-existing user specific knowledge where possible, rather than having users memorize entirely new and/or random information.

The major advantage of persuasive cued click point scheme is its later 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 signal point based techniques. A common security goal is password based authentication systems is to maximize the effective password space. In this paper we have brought the color matrix formation method, so that even though the hotspots viewed by the neighboring user while entering the account will not be easy for the users to enter into the others user account. The key feature of PCCP is that creating a harder to guess password is the path of least resistance, likely making it more effective than schemes where secure behavior adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots and patterns, thus increasing the effective password space.

11. REFERANCES

[1] S.Chiasson, R. Biddle, and P.van Oorschot, "A Second Look at the usability of Click-Based Graphical Passwords," Proc. ACM symp. Usable Privacy and Security (SOUPS), July 2007.

[2] S.Chiasson, A.Forget, R. Biddle, and P.van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click-Points," British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.

[3] S.Chiasson, A. Forget, E.Stobert, P.van Oorachot, and R.Biddle, "Multiple Password Interference in text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security CCS, Nov.2009.

[4] P.C.van Oorschot and J.Thorpe, "Exploiting Predictability in Click-Based Graphical Passwords," J.Computer Security, vol.19, no.4, pp.669-702, 2011.

[5] 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", IEEE Transactions on Dependable and Secure Computing, Vol.9, No.2, March/April 2012.

[6] R.Biddle, S.Chiasson, and P.van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," to be published in ACM Computing Surveys, vol.44, no.4, 2012.

[7] E.Stobert, A.Forget, S.Chiason, P.van Oorschot, and R.Biddle, "Exploring Usability effects of Increasing security in Click-Based Graphical Passwords," Proc. ANN. Computer Security Applications Conf. (ACSAC), 2010.

[8] A.E. Dirik, N.Memon, and J-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp.20-28.

[9] (2010, Feb.). The Science behind Passfaces [Online].

Available:http://www.realuser.com/published/SceienceBehindPassfaces.pdf

AUTHORS PROFILE

Y.Dasradh Ram Reddy working as Associate Professor in C.S.E department BVSR Engineering College, Chimakurthy, A.P, India. He has done his M.Tech and PhD in Computer Science Engineering. He has around 12 years of teaching experience for UG and PG students.

Y.Sravana Lakshmi is currently studying M.Tech in C.S.E in BVSR Engineering College, Chimakurthy, A.P, and India.