ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

GRAPHICAL PASSWORD AUTHENTICATION USING PERSUASIVE CUED CLICK POINT

Iranna A M[1],Pankaja Patil[2]

PG Student, Department of CSE, GIT, Belgaum, Karnataka, India[1]

Assistant Professor MCA Department, GIT, Belgaum, Karnataka, India[2]

Abstract: The main issues of knowledge-based authentication, usually text-based passwords, are well known. Users tend to choose memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. In this paper focuses on the integrated evaluation of the Persuasive Cued Click Points graphical password authentication system, including usability and security. An important usability goal for authentication systems is to support users in selecting better passwords, thus increasing security by expanding the effective password space. In click-based graphical passwords, poorly chosen passwords lead to the emergence of hotspots (portions of the image where users are more likely to select click-points, allowing attackers to mount more successful dictionary attacks). We use persuasion to influence user choice is used in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points**.**

Keywords: Graphical passwords, authentication, persuasive technology, usable security, empirical study.

I.INTRODUCTION

There are many things that are ‘well know’ about passwords; such as that user can’t remember strong password and that the passwords they can remember are easy to guess [1-6].

A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. The task of selecting weak passwords (which are easy for attackers to guess) is more tedious, avoids users from making such choices. In effect, this authentication schemes makes choosing a more secure password the path-of-least-resistance. Rather than increasing the burden on users, it is easier to follow the system’s suggestions for a secure password — a feature absent in most schemes.

We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click- Points (PCCP) [2], [3], and conducted an in lab-lab usability study with 10 participants. Our results show that our Persuasive Cued Click Points scheme is effective at reducing the number of hotspots (areas of the image where users are more likely to select click points) while still maintaining usability. In this paper also analyse the efficiency of tolerance value and security rate. While we are not arguing that graphical passwords are the best approach to authentication, we find that they offer an excellent environment for exploring strategies for helping users select better passwords since it is easy to compare user choices. Indeed, we also mention how our approach might be adapted to text-based passwords.

II. BACKGROUND

Text passwords are the most prevalent user authentication method, but have security and usability problems. Replacements such as biometric systems and tokens have their own drawbacks [8], [9], [10].Graphical passwords offer another alternative, and are the focus of this paper. Graphical passwords were originally defined by Blonder (1996). In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques. In recognition based,a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected during the registration stage. In recall based graphical password, a user is asked to reproduce something that he created or selected earlier during the registration stage. This project is based on recall based Technique.

A. Why Graphical Passwords?

Access to computer systems is most often based on the use of alphanumeric passwords. Though, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

B. Click-Based Graphical Passwords

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. A complete review of graphical passwords is available elsewhere[11]. Of interest herein are cued-recall click-based graphical passwords (also known as locimetric[12]). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues[13] to aid recall. Example systems include PassPoints[14] and Cued Click-Points (CCP)[15].

In PassPoints, a password consists of a sequence of five click-points on a given image (see Figure 1). 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. The usability and security of this scheme was evaluated by the original authors [18,19] and subsequently by others [1, 16, 17]. It was found that although relatively usable, security concerns remain. The primary security problem is hotspots: different users tend to select similar click-points as part of their passwords. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess PassPoints passwords [17]. A dictionary attack consists of using a list of potential passwords (ideally in decreasing order of likelihood) and trying each on the system in turn to see if it leads to a correct login for a given account. Attacks can target a single account, or can try guessing passwords on a large number of accounts in hopes of breaking into any of them.

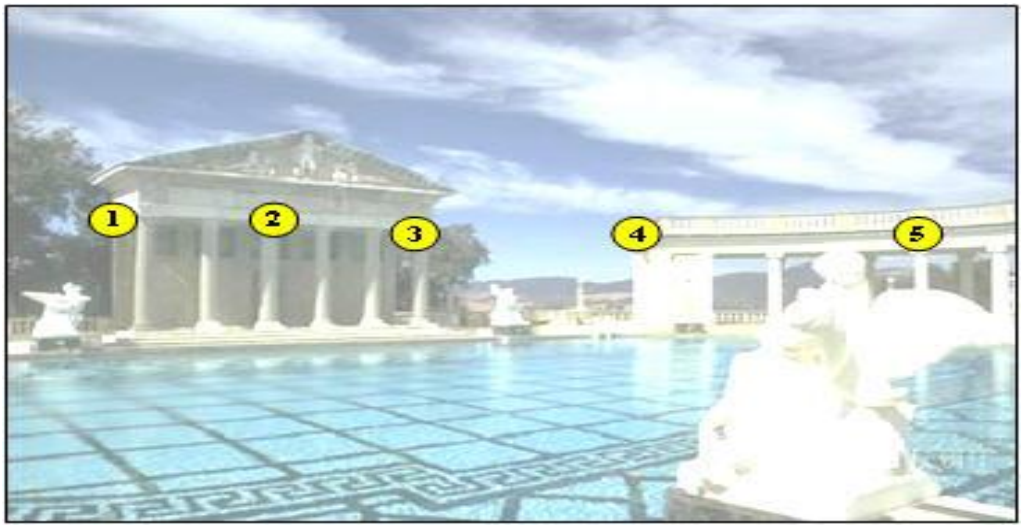

Fig. 1 On PassPoints, a password consists of 5 ordered click- points on the image

A precursor to PCCP, Cued Click Points [7] was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click-point on five different images shown in sequence. The next image displayed is based on the location of the previously entered click-point (see Figure 2), creating a path through an image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click-points results in a different image sequence.

The claimed advantages are that password entry becomes a true cued-recall scenario, wherein each image triggers the memory of a corresponding click-point. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks.

User testing and analysis showed no evidence of patterns in CCP [5], so pattern-based attacks seem ineffective. Although attackers must perform proportionally more work to exploit hotspots, results showed that hotspots remained a problem [2].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

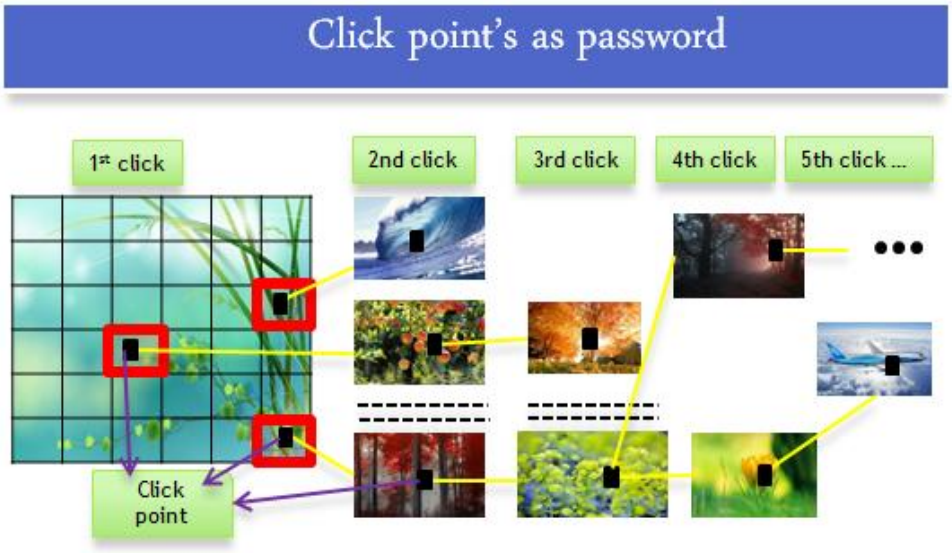

Fig. 2 with CCP, users select one click-point per image. The next image displayed is determined by the current click-point.

C. Persuasive Technology

Persuasive Technology was first articulated by Fogg [20] as using technology to motivate and influence people to behave in a desired manner. Persuasive Technology is the emerging field of "interactive computing systems designed to change people's attitudes and behaviours".

An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed in the next section, our proposed system accomplishes this by making the task of selecting a weak password more tedious and time-consuming. The path-of-least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). As a result, the system also has the advantage of minimizing the formation of hotspots across users since click points are more randomly distributed.

III. PERSUASIVE CUED CLICK POINTS

Previous models have shown that hotspots are a problem in click-based graphical passwords, leading to a reduced effective password space that facilitates more successful dictionary attacks. We investigated whether password choice could be influenced by persuading users to select more random click-points while still maintaining usability. Our goal was to encourage compliance by making the less secure task (i.e., choosing poor or weak passwords) more time-consuming and awkward. In effect, behaving securely became the path-of-least-resistance.

Using CCP as a base system, we added a persuasive feature to encourage users to select more secure passwords, and to make it more difficult to select passwords where all five click-points are hotspots. Specifically, when users created a password, the images were slightly shaded except for a randomly positioned viewport (see Figure 3). The viewport is positioned randomly rather than specifically to avoid known hotspots, since such information could be used by attackers to improve guesses and could also lead to the formation of new hotspots. The viewport's size was intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users were required to select a click-point within this highlighted viewport and could not click outside of this viewport. If they were unwilling or unable to select a click-point in this region, they could press the "shuffle" button to randomly reposition the viewport. While users were allowed to shuffle as often as they wanted, this significantly slowed the password creation process. The viewport and shuffle buttons only appeared during password creation. During password confirmation and login, the images were displayed normally, without shading or the viewport and users were allowed to click anywhere.

Our hypotheses were

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

1. Users will be less likely to select click-points that fall into known hotspots.
2. The click-point distribution across users will be more randomly dispersed and will not form new hotspots.
3. The login security success rates will be higher than to those of the original CCP system.
4. The login security success rates will increase, when tolerance value is lower value.
5. Participants will feel that their passwords are more secure with PCCP than participants of the original CCP system.

Fig. 3 PCCP Create Password interface. The viewport highlights part of the image

The theoretical password space for a password system is the total number of unique passwords that could be generated according to the system specifications. Ideally, a larger theoretical password space lowers the likelihood that any particular guess is correct for a given password. For PCCP, the theoretical password space is $((w \times h)/t^2)^c$where the size of the image in pixels (w * h) is divided by the size of a tolerance square (t^2), to get the total number of tolerance squares per image, raised to the power of the number of click-points in a password (c, usually set to 5 in our experiments).

IV. SYSTEM DESIGN

The system designed consist of three modules such as user registration module, picture selection module and system login module (see Figure 4).

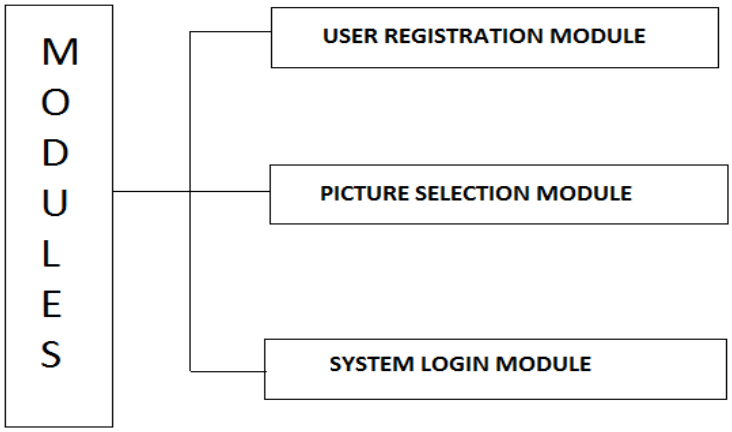

Fig. 4 System design modules

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

In user registration module user enter the user name in user name field and also suitable tolerance value (tolerance value is use to compare registration profile vector with login profile vector). When user entered the all user details in registration phase, these user registration data stored in data base and used during login phase for verification. In picture selection phase there are two ways for selecting picture password authentication.

1. User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices.
2. System defines pictures: pictures are selected by the user from the database of the password system.

In picture selection phase user select any image as passwords and 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. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.

During system login, the 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.

A. User registration flow chart

Below flowchart (see Figure 5) 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 proceed 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.

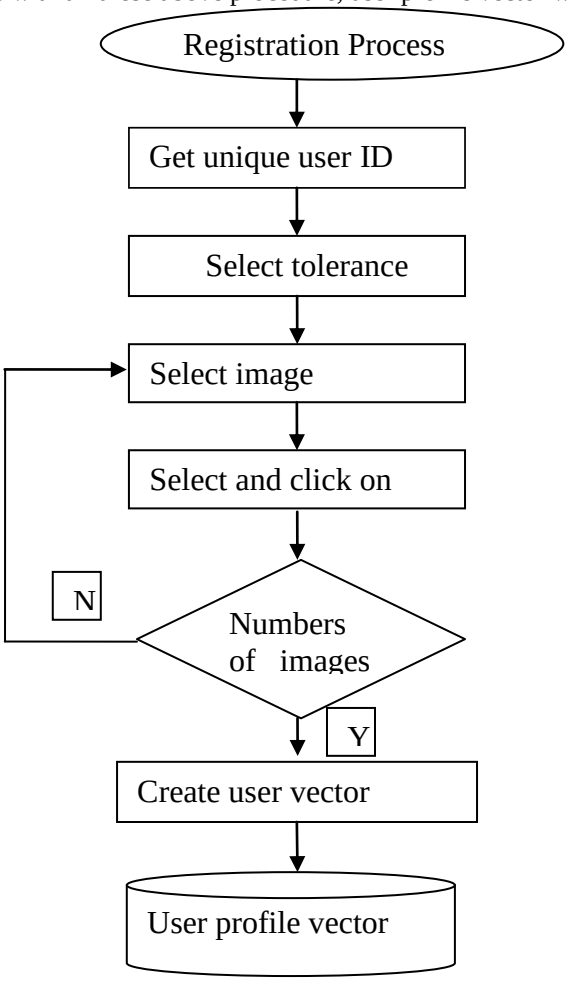

Fig. 5 User registration flowchart

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

B. Login flow chart

In this login procedure (see figure 6), 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.

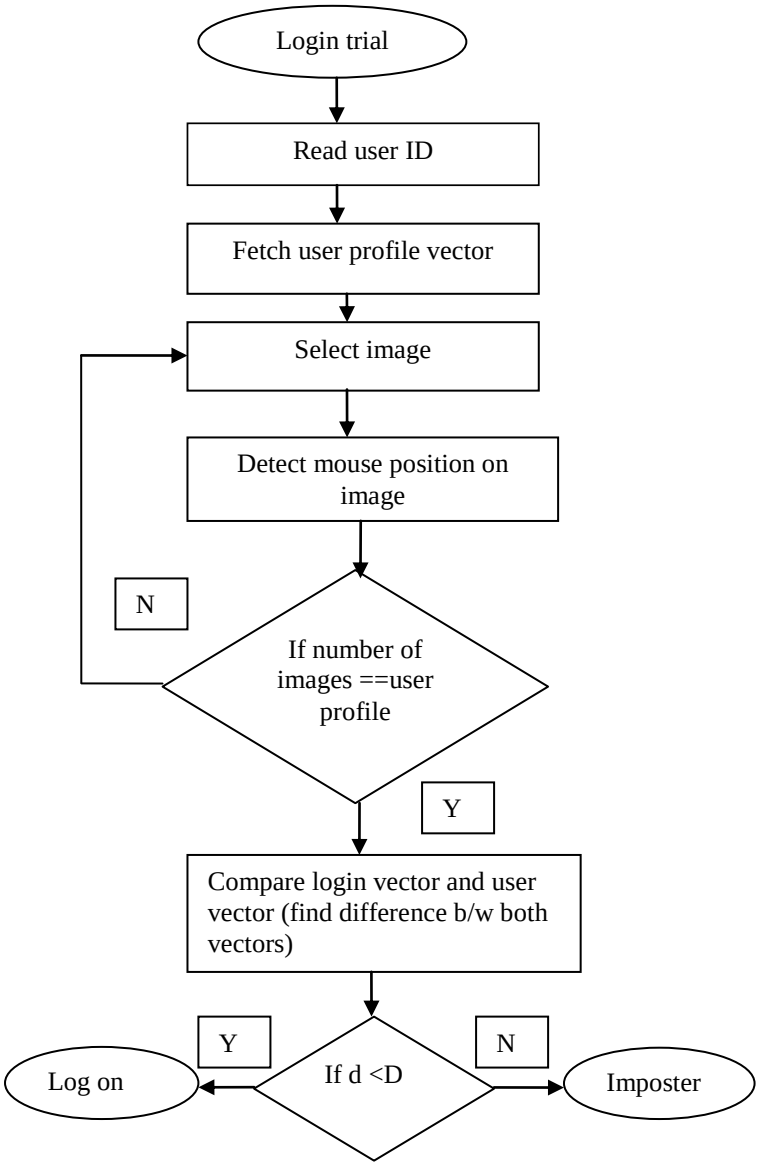

Fig. 6 Login phase flowchart

VI. EMPIRICAL RESULTS AND ANALYSIS

The empirical study 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.

A. Efficiency of the tolerance value

Initially eight participants are considered for the experiment. Each participant has a password which includes clicking on 5 click points in 5 different images. Each image consists of different characters (image details), among

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

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 click points on the images). Once the first participant has logged out, 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 indicates the degree of closeness to the actual click point.
Tolerance region: The area around an original click point 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 number of successful trails for a certain number of trials. the success rates are calculated as the number of trails completed without errors or restarts.
Shoulder surfing: It is the process by which the person standing behind the person entering the password observes the password. It is a type of capture attack. This attack occurs when attackers directly obtain the passwords (or parts thereof) by intercepting the user entered data or by tricking users into revealing their passwords.

The below table 1 shows the result of the tolerance value efficiency of the PCCP method. The results show the graph of the tolerance value against security success rate (see figure 7) and the graph of tolerance value against success rate(see figure 8).

Table I Efficiency of the tolerance value in PCCP method

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

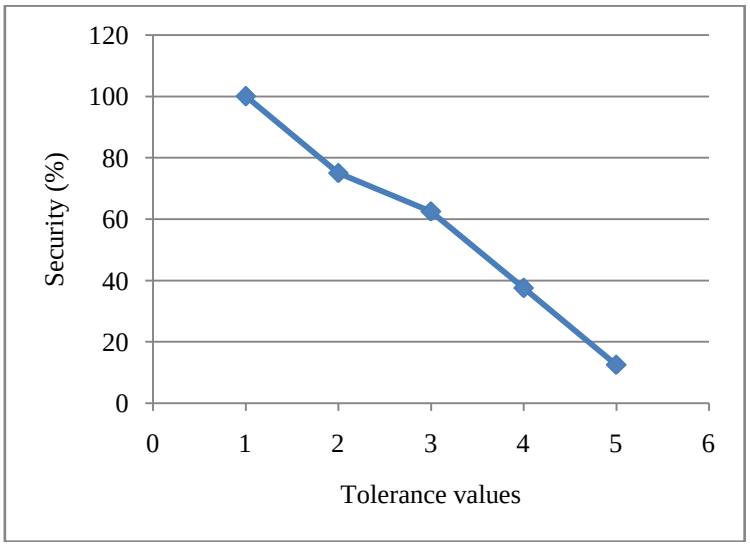

Fig. 7 graph shows that the security increases with the decrease in the tolerance value.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

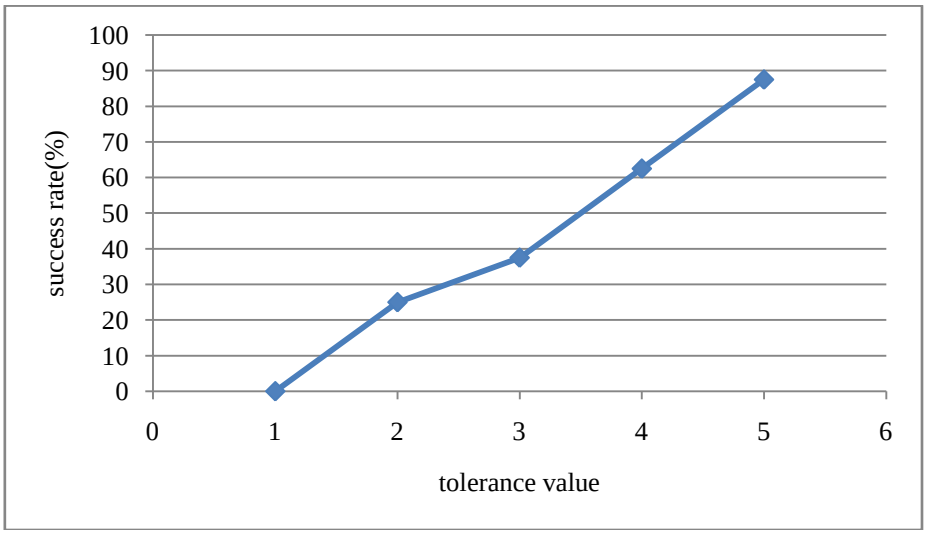

Fig. 8 graph shows that the success rate increases with the increase in the tolerance value

Initially when the tolerance limit was large i.e., 5, seven out eight participants entered the correct password and were able to log in. then when the tolerance limit was reduced to a lower value i.e., to 4, only five out of eight participants were able to log in with the correct password. Later when the tolerance limit was reduced to 3 only three of the eight participants were able to log in and when the tolerance limit was reduced to 2 only 2 of the participants was able to log in. finally when the tolerance limit was reduced to 1 no participants were able to log in successfully. So, the experiment shows that the security level increases with the decrease in the tolerance value, which avoid shoulder surfing problem.

B. Comparison between login Success rate and security success rates of existing CCP and proposed PCCP

Success rates are reported on the first attempt and within three attempts. Success on the first attempt occurs when the password is entered correctly on the first try, with no mistakes. Success rates within three attempts indicate that fewer than three mistakes. Mistakes occur when the participant presses the Login button but the password is incorrect.

Table II PCCP success rates and security success rates compared to CCP

	CCP		PCCP	
	Success rate (%)	Security success rate (%)	Success rate (%)	Security success rate (%)
User1	4/5 (80)	20	3/5 (60)	40
Usre2	3/5 (60)	40	2/5 (40)	60
User3	5/5 (100)	0	4/5 (80)	20
		20 (mean rate)		40 (mean rate)

As shown in Table 2, participants were able to successfully use PCCP. Success rates were calculated as the number of trials completed without errors or restarts, over all trials. In this lab study, initially three participants are

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

considered for the experiment. Each participant has a password which includes clicking on 5 click points in 5 different images and number of trails should be 5 per user. Each image consists of only one click point as a user password. 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.

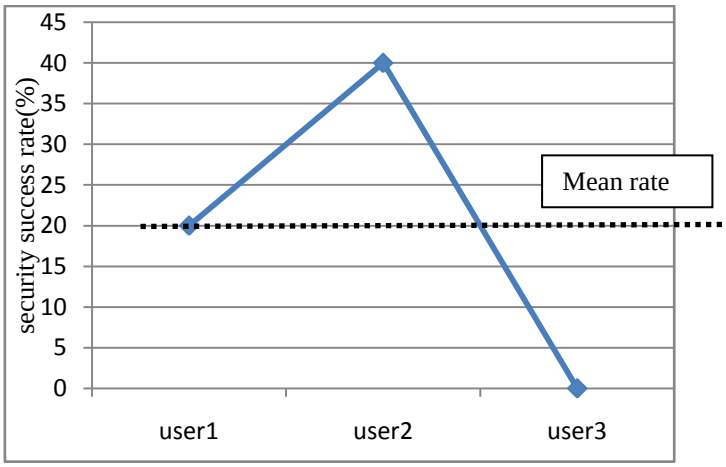

Fig. 9 CCP means rates

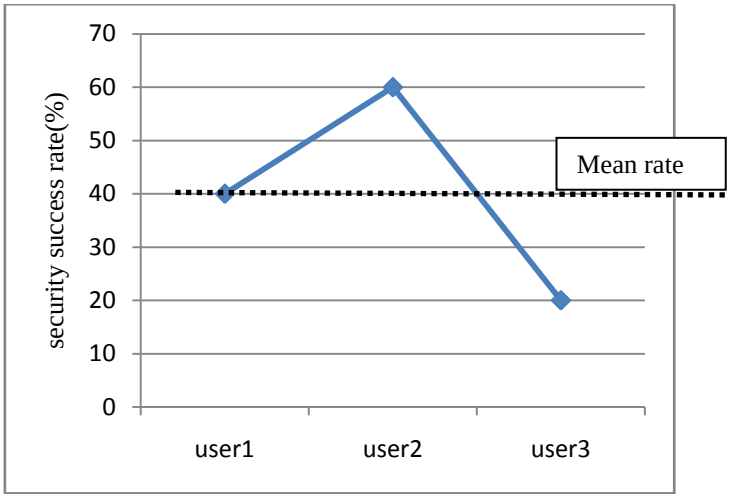

Fig. 10 PCCP mean rate

In comparison, CCP's reported higher success rate then PCCP's but security success rate and mean success rate was lower than the PCCP,s(figure 9 and figure 10) . We suspect that PCCP participants had more difficulty initially learning their password because they were selecting click-points that were less obvious than those chosen by PassPoints and CCP participants. However PCCP participants were ultimately able to remember their passwords with a little additional effort. The experiment shows that security success rate and mean rate of PCCP is very higher than CCP.

C. Speed and time

In general, CPU speed measure by the amount of work that a given CPU can accomplish in a fixed amount of time. speed and time are inversely propositional, means if it take more time to execute the program then CPU speed is slow and vice versa. Times are reported in seconds for successful password entry on the first attempt. For login and recall, we also report the "entry time": the actual time taken from the first click-point to the fifth click-point. According to user opinion during lab study, The PCCP graphical password authentication system will take more time to execute the program compare to text password and pass point. Because it will take more time to select a click point on 5 different images, but it provides more security.

D. Shuffles

During password creation, PCCP users may press the shuffle button to randomly reposition the viewport. Fewer shuffles lead to more randomization of click-points across users. The shuffle button was used moderately. Most

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

participants used a common shuffling strategy throughout their session. They either consistently shuffled a lot at each trial or barely shuffled during the entire session. We interviewed participants to learn about their shuffling strategy. Those who barely shuffled selected their click point by focusing on the section of the image displayed in the viewport, while those who shuffled a lot scanned the entire image, selected their click-point, and then proceeded to shuffle until the viewport reached that area. When questioned, participants who barely shuffled said they felt that the viewport made it easier to select a secure click point. Those who shuffled a lot felt that the viewport hindered their ability to select the most obvious click-point on an image and that they had to shuffle repeatedly in order to reach this desired point.

E. Viewport Details

The viewport visible during password creation must be large enough to allow some degree of user choice, but small enough to have its intended effect of distributing clickpoints across the image. Physiologically, the human eye can observe only a small part of an image at a time. Selecting a click-point requires high acuity vision using the fovea, the area of the retina with a high density of photoreceptor cells. The size of the fovea limits foveal vision to an angle of approximately 1 degree within the direct line to the target of interest. At a normal viewing distance for a computer screen, say 60 cm, this results in sharp vision over an area of approximately $4cm^2$. We chose the size of the viewport to fall within this area of sharp vision.

The viewport positioning algorithm randomly placed the viewport on the image, ensuring that the entire viewport was always visible and that users had the entire viewport area from which to select a click-point. This design decision had the effect of deemphasizing the edges of the image, slightly favoring the central area. A potential improvement would be to allow the viewport to wrap around the edges of the image, resulting in situations where the viewport is split on opposite edges of the image.

F. Variable Number of Click-Points

A possible strategy for increasing security is to enforce a minimum number of click-points, but allow users to choose the length of their password, similar to minimum text password lengths. The system would continue to show next images with each click, and users would determine at which point to stop clicking and press the login button. Although most users would likely choose the minimum number of click-points, those concerned with security and confident about memorability could select a longer password.

F. User opinion and perception

During each trial, participants answered Likert-scale questions correspond to those reported in the previously cited studies A Likert scale is a psychometric scale commonly involved in research that employs questionnaires. It is the most widely used approach to scaling responses in survey research, such that the term is often used interchangeably with rating scale, or more accurately the Likert-type scale, even though the two are not synonymous. The scale is named after its inventor, psychologist RensisLikert. Users rated PCCP favourably (Table 7.4), with all median responses neutral or higher. They felt that PCCP passwords were easy to create and quick to enter, but they remained impartial on their preference between text and graphical passwords. The scores for those questions were reversed prior to calculating the means and medians, thus higher scores always indicate more positive results for PCCP in Table 7.4

Table III Questionnaire responses. Scores are out of 10

Question	Mean	Median
I could easily create a graphical password	8	8
Logging on using a graphical password was easy	6.4	7
Graphical passwords are easy to remember	6	6
I prefer text passwords to graphical Passwords	4.9	5
Text passwords are more secure than graphical passwords	6	6.2
I think that other people would choose different points than me for a graphical password	7.2	7
With practice, I could quickly enter my graphical password	8.3	8

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

VI. SECURITY

An authentication system must provide adequate security for its intended environment; otherwise it fails to meet its primary goal. The classification of attacks on knowledge-based authentication into two general categories: guessing and capture attacks.

A .Guessing Attacks

In successful guessing attacks, attackers are able to either exhaustively search through the entire theoretical password space, or predict higher probability passwords (i.e., create a dictionary of likely passwords) so as to obtain an acceptable success rate within a manageable number of guesses. We now consider how these could be leveraged in guessing attacks.

Pattern-Based Attack

One of the proposed attacks on PassPoints is an automated pattern-based dictionary attack that prioritizes passwords consisting of click-points ordered in a consistent horizontal and vertical direction (including straight lines in any direction, arcs, and step patterns), but ignores any image-specific features such as hotspots. The attack guesses approximately half of passwords collected in a field study on the Cars and Pool images (two of the 17 core images) with a dictionary containing 2^{35} entries, relative to a theoretical space of 2^{43}.

Given that PCCP passwords are essentially indistinguishable from random for click-point distributions along the x- and y-axes, angles, slopes, and shapes (see technical report such pattern-based attacks would be ineffective against PCCP passwords.

Hotspot Attack with All Server-Side Information

PassPoints passwords from a small number of users can be used [21] to determine likely hotspots on an image, which can then be used to form an attack dictionary. Up to 36 percent of passwords on the Pool image were correctly guessed with a dictionary of 2^{31} entries.

To explore an offline version of this attack, assume in the worst case that attackers gain access to all server-side information: the username, user-specific seed, image identifiers, images, hashed user password, and corresponding grid identifiers .The attacker's task is more difficult for PCCP because not only is the popularity of hotspots reduced, but the sequence of images must be determined and each relevant image collected, making a customized attack per user. An online attack could be thwarted by limiting the number of incorrect guesses per account.

Hotspot Attack with Only Hashed Password

Suppose attackers gain access only to the hashed passwords, for example, if the passwords and other information are stored in separate databases. Offline dictionary attacks become even less tractable. The best attack would seem to involve building a guessing dictionary whose entries are constructed from the largest hotspots on random combinations of images.

B .Capture Attacks

Password capture attacks occur when attackers directly obtain passwords (or parts thereof) by intercepting user entered data, or by tricking users into revealing their passwords. For systems like PCCP, CCP, and PassPoints (and many other knowledge-based authentication schemes), capturing one login instance allows fraudulent access by a simple replay attack. We summarize the main issues below.

Shoulder Surfing: All three cued-recall schemes discussed (PCCP, CCP, and PassPoints) are susceptible to shoulder surfing although no published empirical study to date has examined the extent of the threat. Observing the approximate location of clickpoints may reduce the number of guesses necessary to determine the user's password. User interface manipulations such as reducing the size of the mouse cursor or dimming the image may offer some protection, but have not been tested. A considerably more complicated alternative is to make user input invisible to cameras, for example, by using eye tracking as an input mechanism.

Malware: Malware is a major concern for text and graphical passwords, since key logger, mouse logger, and screen scraper malware could send captured data remotely or otherwise make it available to an attacker.

Social Engineering: For social engineering attacks against cued-recall graphical passwords, a frame of reference must be established between parties to convey the password in sufficient detail. One preliminary study [22] suggests that password sharing through verbal description may be possible for PassPoints. For PCCP, more effort may be required to

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

describe each image and the exact location of each click-point. Graphical passwords may also potentially be shared by taking photos, capturing screen shots, or drawing, albeit requiring more effort than for text passwords.

C. Survey on Security Analysis

Given that hotspots and click-point clustering are significantly less prominent for PCCP than for CCP and PassPoints, guessing attacks based on these characteristics are less likely to succeed. Taking into account PCCP's sequence of images rather than a single image offers further reduction in the efficiency of guessing attacks. For capture attacks, PCCP is susceptible to shoulder surfing and malware capturing user input during password entry. However, we expect social engineering and phishing to be more difficult than for other cued-recall graphical password schemes due to PCCP's multiple images.

VII. CONCLUSION

An important usability and security goal in authentication systems is to help user's select better passwords and thus increase the effective password space. We believe that users can be persuaded to select stronger passwords through better user interface design. As an example, we designed Persuasive Cued Click-Points (PCCP) and conducted a usability study to evaluate its effectiveness. We obtained favorable results both for usability and security.

PCCP encourages and guides users in selecting more random click-based graphical passwords. A key feature in PCCP is that creating a secure password is the "path-of-least-resistance", making it likely to be more effective than schemes where behaving securely adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots, avoid shoulder surfing problem and also provide high security success rate, while still maintaining usability.

ACKNOWLEDGMENTS

We thank the participants of our lab study for their time andValuable feedback. Parts of this paper appeared earlier in publications [1], [2], [3], [4], [5],[16],[17],[18].

REFERENCES

[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," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.
[3] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Bddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security CCS), Nov. 2009.
[4] E. Stobert, A. Forget, S. Chiasson, 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.
[5] 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.
[6] 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.
[7] 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.
[8] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.
[9] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.
[10] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.
[11] 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.
[12] 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," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 128-152, 2005.
[13] E. Tulving and Z. Pearlstone, "Availability versus Accessibility of Information in Memory for Words," J. Verbal Learning and Verbal Behavior, vol. 5, pp. 381-391, 1966.
[14] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.
[15] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005.
[16]. Golofit, K. Click Passwords Under Investigation. ESORICS 2007. LNCS 4734, 343-358, 2007.
[17] Thorpe, J. and van Oorschot, P.C. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security Symp. 2007.
[18]. Wiedenbeck, S., Birget, J.C., Brodskiy, A., and Memon, N. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. Symp. on Usable Privacy and Security (SOUPS) 2005.
[19]. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., and Memon, N. PassPoints: Design and longitudinal evaluation of a graphical password system. Int. Journal of Human- Computer Studies 63, 102-127, 2005.
[20] B. Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, 2003.
[21]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.
[22] P. Dunphy, J. Nicholson, and P. Olivier, "Securing Passfaces for Description," Proc. Fourth ACM Symp. Usable Privacy and Security (SOUPS), July 2008.