# Authentication Using Graphical Passwords-PCCP

K.Suesh Kumar Reddy[1], K.Venkataramana[2]
[1] M.Tech(CSE) Student Scholar, Department of CSE, KMMITS, Tirupati, INDIA,
sureshreddy117@yahoo.com
[2]Head, Dept. of CSE, KMMITS, Tirupati, INDIA
ramanakv4@gmail.com

*Abstract:* **The graphical passwords have been designed to try to create passwords more brilliant and easier for people to use and more secure. Using a graphical password, users click on images rather than type alphanumeric characters. Authentication means we are provide security for our valuable information, files, data and passwords. User interacts with computer by using passwords. The most important concept behind the paper entitled Authenticate using graphical passwords-PCCP is the systems to support users in selecting improved passwords. So present days we are using dissimilar graphical passwords are used to security reason that is Image, Thumb impression, digital Signatures, mobile passwords, etc. used as passwords. Instead of using textual character we are using Graphical passwords. Graphical passwords essentially use Image, Thumb impression, digital Signatures, mobile passwords, etc. used as graphical system passwords-PCCP. There are various graphically Image, Thumb impression, digital Signatures, mobile passwords, etc. used as passwords are there those are Authentication using graphical passwords.**

**Keywords: Authentication, image passwords, Persuasive Cued Click Points (PCCP), password guessing resistant protocol.**

## I. INTRODUCTION

The most frequent computer authentication system is for a user to submit a user name and a text password. The vulnerabilities of this system have been famous. One of the major problems is the difficulty of remembering passwords. Graphical password schemes have been proposed as a potential alternative to text-based schemes, annoyed incompletely by the information that humans can remember pictures better than text; psychological studies supports such assumption. A variety of graphical password schemes have been proposed as alternatives to text-based passwords. The research has shown that text-based passwords are loaded with both usability and security problems that make them less than attractive solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text.

A graphical based password is one capable alternative of textual passwords. 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 and 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.

## II. BACK GROUND OF PCCP

Previous models have exposed that hotspots are a problem in click-based graphical passwords, foremost to reduced efficient password space that facilitates more booming dictionary attacks. We investigated whether password preference could be influenced by persuading users to choose more random click-points while still maintaining usability. Our goal was to support compliance by making the less secure task (i.e., choosing poor or weak passwords) more time-consuming and awkward. In effect, behaving powerfully 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 harder to select passwords where all five click-points are hotspots. Particularly, when users formed a password, the images were somewhat shaded apart from the randomly placed viewport. Persuasive Cued Click Points (PCCP) can be viewed as a combination of Pass Points (PP), Cued Click Points (CPP), and Story. A password consists of one click-point per image for a series of images. The subsequently image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. PCCP offers both improved usability and security. Users could quickly create their password. Another feature of Persuasive cued click point is the immediate implicit feedback (Knowledge based feedback) telling the correct user whether their latest click-point was correctly entered.

### ***A.*** *Persuasive Cued Click Points On Images*

PCCP encourages and guides users in selecting more random click-based graphical passwords. The major aspect in PCCP is that generate a secure password is the path-of-least- resistance, make it expected to be more efficient than schemes where behaving securely adds an additional load on users. The advance has confirmed successful at reducing the structure of hotspots, keep away from shoulder surfing problem and furthermore provide high security success rate, while still maintaining usability. We believe that users can be persuaded to select stronger passwords through better user interface design. For example, we considered Persuasive Cued Click-Points (PCCP) and conducted a usability study to evaluate its efficiency. We obtained positive results mutually for usability and security. Persuasive Cued Click Points is a proposed alternative to Pass Points and Cued Click Points. As shown in Figure 2, each click results in showing a next-image, in effect leading users down a "path" as they click on their series of points. An incorrect click leads down a wrong path, with an unambiguous indication of authentication failure only after the last click. Users can select their images just to the extent that their click-point dictates the subsequently image. If they hate the resulting images, they could generate a fresh password concerning different click-points to get different images.

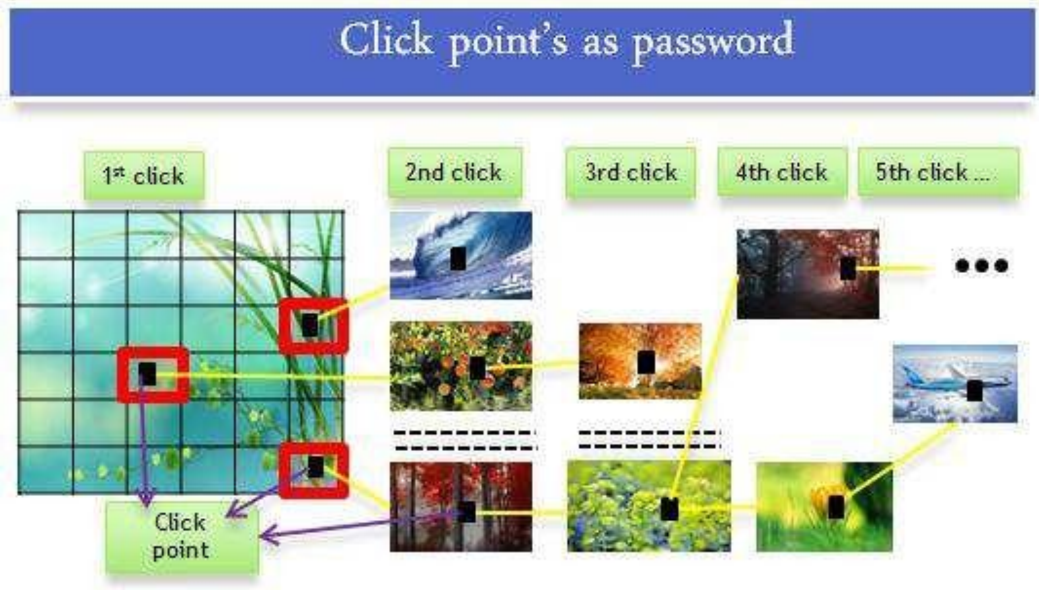


*Figure 2: PCCP passwords as a choice-dependent path of images.*

During password creation, the first image can be selected by the user from the system. We will find out the X and Y co-ordinates of the click-point. For each click-point in a subsequent login attempt, this number is retrieved from the database and used to determine whether the click-point falls within the tolerance (correct region or correct X and Y coordinates) of the original point. The number of images would quickly become quite large increasing exponentially. When computing the next-image index, if any is a repeat, we can select a distinct image using load picture button. A user's initial image is selected by the system based on user characteristic such as username.

## III. PRELIMINARY SECURITY ANALYSIS

Proposed authentication scheme needs to be evaluated in terms of feasible threats. We initiate by clarifying our objective scenario for CCP and the particular assumptions made regarding the system. We propose that CCP be implemented and deployed in systems where offline attacks are not potential and wherever attack will be made against an online system that can limit the number of guesses made per account in a given time period. If the username, the image series and the click-points are experimental through shoulder-surfing then an attacker has all of the information needed to break in to the version as is the case with PassPoints and most other password system. A compromised computer is also a threat because malware may capture the login information and relay that information elsewhere. A few alternatives exist to increase the effective password space for CCP.

## IV. OVERVIEW OF IMAGE PASSWORDS

There has been a great deal of hype for Image, Thumb impression, digital Signatures, mobile passwords since two decade due to the fact that primitive's methods suffered from an innumerable number of attacks which could be imposed simply. Here we will progress lose the classification of authentication methods. We focus on the most common computer authentication method that makes use of text passwords. Unfortunately, these passwords are broken means such as dictionary attacks, shoulder surfing attacks and social engineering attacks. To moderate the problems with established methods, highly developed methods have been proposed using graphical as passwords.

### *A. Graphical password as secure as text based password*

Very little research has been done to study the difficulty of cracking graphical passwords. Since the graphical passwords are not broadly used in practice, there is no description on valid cases of breaking graphical passwords. Here we examine some of the feasible techniques for breaking graphical passwords and try to do a comparison with text-based passwords. Easily hackers are identify the text passwords because there are only110 key words are there instead of that we can use graphical password there are many pixels are there per image so hackers are difficult to identify the Image, Thumb impression, digital Signatures, mobile passwords. Image, Thumb impression, digital Signatures, mobile passwords are an alternative to text passwords; user is easily to remember an image (or parts of an image) instead of a word. Three click-based graphical password schemes: Pass Points and two variants named Cued Click-Points and Persuasive Cued Click-Points. In CCP and PCCP, a user clicks on a single point on each of five images, where each image (except the first image) is dependent on the previous click-point. By using these PCCP we can provide the authentication for user's passwords and valuable information.

### *B. The major design and implementation issues of graphical passwords*

***Security*** we have briefly examined the security issues with graphical passwords.
***Usability:*** One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. Beginning of user studies are accessible in some research papers seem to support. But, present user Studies are still very restricted, connecting only a small number of users.
***Reliability:*** The major design issue for recall-based methods is the reliability and accuracy of user input detection. In this category of process, the inaccuracy tolerances have to be set carefully – overly high tolerances may lead to many false positives while overly low tolerances may lead to many false negatives.

### *C. Recall based techniques*

In this section we discuss recent two types of click based graphical password techniques

- Pass Points
- Cued Click Points

***Pass Points:*** Based on Blonder's original idea Pass Points is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel based image. To login, a user must click within some system-defined tolerance region for each click- point

***Cued Click Points:*** Cued Click Points was developed as an alternative click based graphical password scheme where users select one point per image for five images. The edge displays only single image at a time; the image is replaced by the next image as soon as a user selects a click point. The method determines the subsequently image to display based on the user's click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is presently chosen. It is currently presents a one to one cued recall scenario where each image triggers the user's memory of the one click point on that image(are shown in figure2). Secondly, if a user enters an incorrect click-point through login, the subsequently image displayed will also be wrong. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the presented user studies are extremely restricted and there is not yet convincing evidence to support this argument.

## V. SYSTEM DESIGN

### *A. Input Design*

The input design is the link between the information system and the user. It comprise the developing requirement and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The input is designed in such a way so that it provides security and ease of use with retain the privacy. The input design measured the following things:

What data should be given as input?
How the figures should be arranged or coded?
The dialog to direct the working people in providing input.
Methods for prepare input validations and steps to follow when inaccuracy occur.

*Objectives:*

1. Input Design is the process of converting a user-oriented description of the input into a computer-based method. This plan is significant to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large amount of information. The objective of scheming input is to make data entry easier and to be open from errors. The data access display is considered in such a way that all the data manipulates can be performed. It as well provides record screening services.
3. When the data is entered it will check for its authority. Information can be entered with the assist of screens. Suitable messages are provided as when required so that the user will not be in maize of time. Thus the purpose of input plan is to generate an input design that is simple to follow.

### *B. Output Design*

A quality output is one, which meets the requirements of the end user and presents the information obviously. The system results of processing are communicated to the users and to other system during outputs. In the output design the information is to be displaced for immediate need and also the inflexible output. It is most significant and direct source information to the user. The proficient and sharp output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in a structured well thought out manner; the right output must be developed while ensuring that every output element is considered so that people will find the system can use simply and efficiently. When analysis designs computer output, they should recognize the definite output that is required to meet the necessities.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.
Convey information about past activities, current status or paper ions of the future.
The signal significant events, opportunities, problems, or warnings.
Trigger an action.
Confirm an action.

## VI. SYSTEM ARCHITECTURE

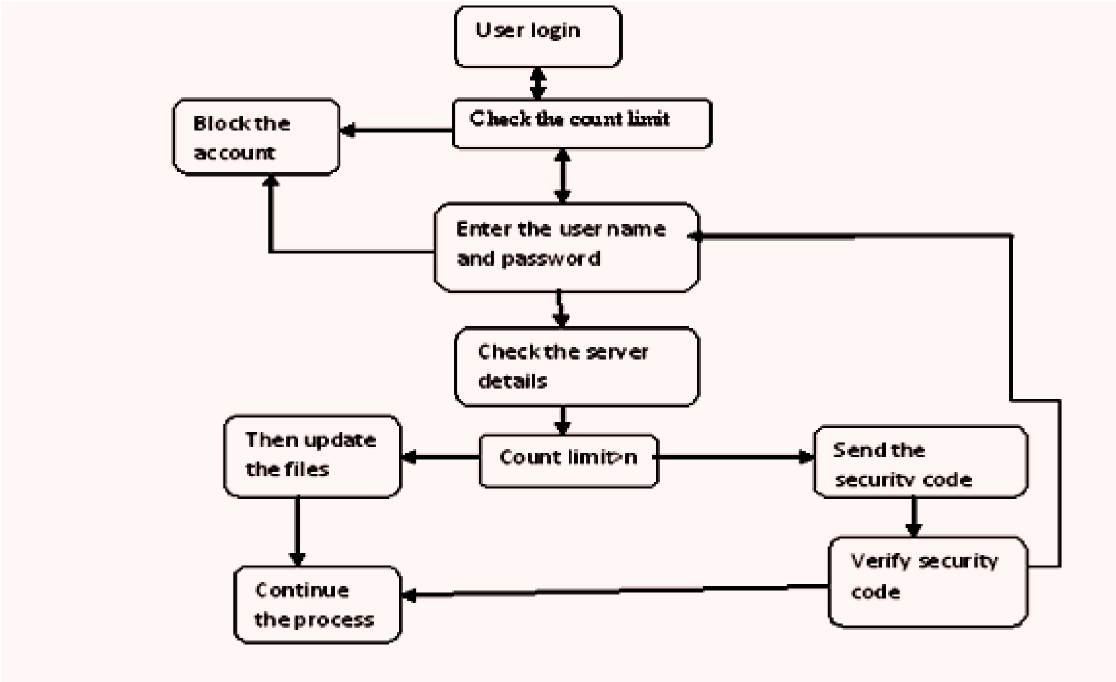


*Figure 3: Architecture of the user login system*

The above figure shows that when user login system will check whether the user is already login or new user, if already login user means check count limit or new user means check stop list, after entering user checking count limits if username and password is correct then the user enter in to their login page, if user name and password is wrong again login the password then starts the count limit.

## VII. CONCLUSION

The proposed Persuasive Cued Click Points scheme shows assure as an utilizable and memorable authentication mechanism. By taking improvement of users' ability to identify images and the memory trigger related with seeing a new image, PCCP has advantages over PassPoints in terms of usability. Being cued as every image is exposed and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. In our little comparison group, users robustly preferred PCCP. We consider that CCP offers a more secure option to PassPoints. PCCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then perform hotspot analysis on every of these images. The system's flexibility to enlarge the overall number of images in the system allows us to randomly increase this workload. The effort merges persuasive cued click points and password guessing resistant protocol. The major objective of this paper is to reduce the guessing attacks as well as encouraging users to select more random and difficult passwords to guess.

## REFERENCES

[1] A.Salehi-Abari,J.Thorpe,and P.van Oorschot,"On purely automated attacks and click- based graphical passwords," in Annual Computer Security Applications Conf.(ACSAC),2008.
[2] Design, implementation, and evaluation of a knowledge-based authentication mechanism," School of Computer Science, CarletonUniversity, Tech.Rep.TR-11-03, February 2011
[3] Dhamija, R. and Perrig, A. Déjà Vu: User study using images for authentication. In *Ninth Usenix Security Symposium* (Denver, CO, USA, Aug. 14-17, 2000).
[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] G. Niranjana and Kunal Dawn, "Graphical Authentication Using Region Based Graphical Password", International Journal of Computer Science and Informatics, vol-2, issue-3,pp 6-11,.2012.
[6] Journal of Human- Computer Studies 63, 102-127, 2005.

[7] Khalil Shihab," A Backpropagation Neural Network for Computer Network Security", Journal of Computer Science 2 (9): 710-15, 2006.
[8] P. C. van Oorschot andJ. Thorpe,"Exploiting predictability in click- based graphical passwords", Journal of Computer Security,vol.19, no.4, pp.669–702,2011.
[9] S.Akula and V.Devisetty,"Image Based Registration and Authentication System," in Proceedings of Midwes Instruction and Computing Symposium, 2004.
[10] 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.
[11] S.Chiasson,E.Stobert,A.Forget,R.Biddle,andP.van Oorschot, "Persuasive cued click- points:
[12] Sonia Chiasson, P.C. van Oorschot,and Robert Biddle, "Graphical Password Authentication Using Cued Click Points" ESORICS, LNCS 4734,pp.359-374,Springer Verlag Berlin Heidelberg 2007.
[13] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., and Memon, N. PassPoints: Design and longitudinal evaluation of a graphical password system. Int.
[14] ZhiLi, QibinSun, Yong Lian, andD.D.Giusto,,,Anassociation-based graphical password design resistant to shoulder surfing attack,International Conference on Multimedia and Expo(ICME),IEEE.2005