Authentication Using Persuasive Cued Click Points

M .Swathi, M. V. Jagannatha Reddy
[1]((IInd MTech, MITS, Madanapally

[2](Associate Professor, Dept Of CSE, MITS,Madanapally

Abstract— In this paper the most efficient authentication method persuasive cued click points is used. Generally the users create passwords by using textual character, but by using these text passwords there are many drawbacks. Users create memorable passwords that are easy for hackers to guess, but strong passwords are very difficult to remember. So we introduced a new technique ,authentication using persuasive cued click points. By using this method, we can secure the passwords. Generally human brain is good in remembering picture than textual character. In this paper, we work with persuasive cued click points and password guessing resistant protocol. The main goal of this paper is, to reduce the guessing of passwords and select passwords to guess that are more difficult. By using the persuasive cued click points, we can successfully avoid security threats like brute force attacks, dictionary attacks, shoulder surfing, social engineering, spy ware and malware**.**When logging in if the user draws the correct gesture using mouse the user will treat as an authenticated user.

Index Terms— Authentication, image passwords, password guessing resistant protocol, persuasive technology.

1. INTRODUCTION

Authentication plays an important role in protecting information against unauthorized access. Most of the people preferred text passwords to secure information. Text based passwords are not suitable for the applications that enforce security through access control mechanism. Authentication based on text passwords has major drawbacks. Graphical password schemes have been used in place of text passwords. By using graphical password we can provide security for our valuable information. According to Psychology, human brain is better at recognizing and recalling pictures rather than text. Graphical passwords are based on this human characteristic. The advantages of using graphical passwords are the reduction of memory burden on users, larger password space and more secure passwords .Graphical password schemes are categorized in to pass points, cued click points, persuasive cued click points

In presentation paper, explore on the efficient click based graphical password scheme known as persuasive cued click points (PCCP). A password consists of the image is dimmed except for a small selected area that is randomly positioned on the image. Users must select a click-point with in the selected area. If they are unable to select a point in the current image, they may use the shuffle button to randomly reposition the image. PCCP offers both improved usability and security. Users could quickly create and re-enter their passwords. We compared PCCP to text passwords. PCCP passwords are good to remember than text passwords, and comparing to other two related graphical password systems, we can reduce the hotspots in PCCP passwords and in remaining two graphical password systems, there are some drawbacks. Graphical passwords have also been applied to Bank applications and mobile devices

2. BACKGROUND

There are some authentication methods they are

1. Token based authentication
2. Biometric authentication
3. Knowledge based authentication

2.1 Token Based Authentication

Token based techniques such as keycards, bank cards and smart cards are used. Using these techniques or methods is not much safe. If the cards are stolen then the data may be misused by others.

2.2 Biometric Based Authentication

In this type of authentication, Biometric based techniques are fingerprints, iris scan, facial recognition are used. The major draw back of this technique is that the identification process is slow

2.3 Knowledge Based Authentication

In this knowledge based authentication, text based password and picture based passwords are used. These are again divided into two categories

2.3.1 Recognition Based Technique

Using recognition based technique; user is presented with a set of images in the database. By using this it is time consuming process and memory will be wasted in the system

2.3.2 Recall Based Graphical Technique

Using recall based technique user can select the password as image, based on user's selection. There are three types of techniques and we will discuss them in next section.

3. RELATED WORK

Text passwords are the most popular user authentication method, but have security and usability problems. Alternatives such as biometric systems and tokens have their own drawbacks. Graphical passwords offer another alternative method that we focus in this paper.

3.1.Click-based graphical passwords:

Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information. In this click based graphical passwords there are three possible techniques. Those are

- Pass Points
- Cued Click Points
- Persuasive Cued Click Points

Pass Points:

In Pass Points, the passwords consist of a sequence of fiveclick points on a particular image. User may select any pixels in the image as click-points for their passwords. When users are login, they repeat the sequence of clicks in the correct order, within a system-define tolerance sequence square of the original click-point that is shown in Figure1. By using this technique there are some drawbacks. Security is weak and the hackers can easily to guess the passwords. Hackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess Pass Points passwords.

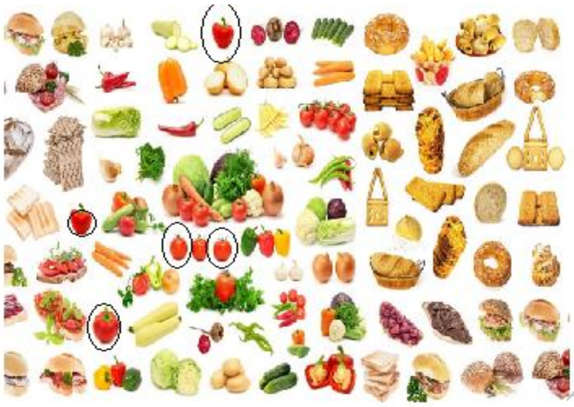


Figure1: User creates a pass point password by selecting five click points on the image

Cued click points:

Cued Click Points (CCP) was developed as an alternative click based graphical password scheme where users select one click point per image until selected images. The monitor displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image. The coming image displayed to users is based on a deterministic function of the point which is currently selected. It now 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 during login, the coming image will also be incorrect. Unknown or hacker is who was saw an unrecognized image will know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

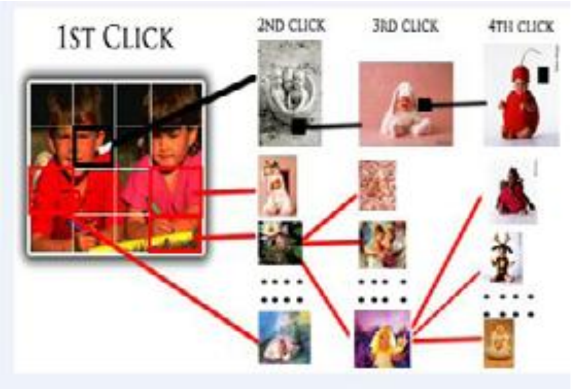


Figure 2: A user's navigation path through a sequence of images to form a password in CCP. Users click on one point per image and the current click-point determines the next image displayed.

Persuasive cued click points(PCCP)

During password creation, generally the image is dimmed except for a small view port area that is randomly positioned on the image. Users must select a image password(click point) within the current image. If they are unable or unwilling to select a point in the current image, they may use the Shuffle button to randomly reposition the image. The view port guides users to select more random passwords that are less likely to include hotspots(are shown in figure3). 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 will take lot of time and more tedious process.

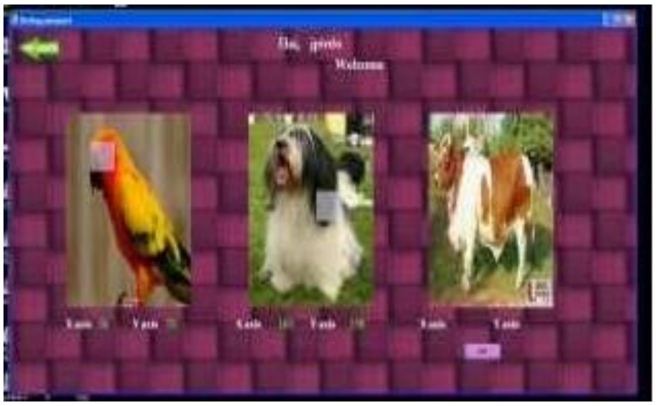


Figure3: Screen shot of the PCCP Create Password Interface with the view port highlighting a portion of the image

4. Persuasvive Cued Click Points(PCCP)

We investigated that the system could influence users to select more random click-points while maintaining usability. The main goal is user is selecting a better passwords or strong passwords. We are not giving chance to hackers to guess the passwords so we are choosing the persuasive cued click points; it is very safe path of least resistance.

There are many drawbacks are there in other two graphical passwords that is pass points and cued click points. In the pass points the user will click five points per image so it is very easy to guess the passwords and coming to cued click points for user it is very difficult to remember the password because a single pixel per image to select as password. So PCCP passwords are convenient for users.

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 aim age password (click point) within the current image. If they are unable or unwilling to select a point in the current image, they may use the Shuffle button to randomly reposition the image. The view port guides users to select more random passwords that are less likely to include hotspots(are shown in figure3). 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 later password entry, the images are displayed normally, without shading or the view port, and users may click any whereon the images.

The theoretical password space for a password system is the total number of unique passwords that could be generated according to the system specifications. Generally 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, to get the total number of tolerance squares per image, raised to the power of the number of click-points in a password.

By using this PCCP we can avoid the hackers who are guessing the passwords. We propose a new condition for this paper that is "Increment number of failures", user can enter their password only five times, if more than he/she cannot enter into their achieved document or file. If user exceeds number of attempts then inform user that password was incorrect and to retry. We are sending security code to the user, by using this code he/she can re-enter their password. If in case again user can attempt wrong password then block the future attempts.

4.1. Selection of image

The system creates user profile vectors there are two types of vectors are there those are Master vector and Detailed vector. In this paper we are using detailed vector by using this formula we can select the image.

Detailed Vector - (Image, X-coordinates, Y-coordinates)
As an example of detailed vector
Detailed Vector
(Image**, x-coordinates, y-coordinates)**

I1 (123,678)
I2 (176,134)
I3 (450,297)
I4 (259,525)

By usage this we select the image. When we create the password it will store in the database. By using this X-COORDINIATES and Y-COORINATES we can select the image these coordinates will help us to remember the passwords

4.2 Euclidian Distance

Once the user can create the password then user can login to the system, then system calculate the Euclidian distance between two vectors **p** and **q** is given by the formula?
Where p is login vector and q is the profile vector

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + .. + (p_n - q_n)^2}$$

$$d(p,q) = \sum_{i=0}^{n} (p_i - q_i)^2$$

Above formula is calculated the distance if the distance d less than a tolerance value then it are according to the application.

4.3 Algorithms for image registration

Registration algorithm
Registration(user_id)

- Sequence_number:=1;
- While sequence_number is less than 3 do
- Generate a random number between 111 to 1111 (total images in the database),let be the image_number:
- Retrive the random image with image_number from the data base and show it to the user;
- Draw a virtual grid over the image;
- Wait for the user to select the region;
- Calculate the parameters;
- Store the parameters with sequence_numberimage_number and user_id in the database;
- Sequence_number:=sequence_number+1;

4.4Defense Against Algorithm

- Defense against algorithm(user_id);
- IF (user_id .value.length<6) then do
- Alert("Your username must be atleast6 letters please try again");
- Return user_id;
- Else

- Select your image password which are stored in database;
- IF image is not equal to selected image(which are stored in database)
- Alert("your password entries did not match please try again");
- Else
- Alert("you are successfully login ……thank you……..");
- End IF;
- End IF;

5. SYSTEM ARCHITECTURE

We propose to reduce the guessing attacks as well as encouraging users to select more random, and problematic passwords to guess. The system work merges persuasive cued click points and password guessing resistant protocol. There are two processes are there those are

- User registration process
- User login process

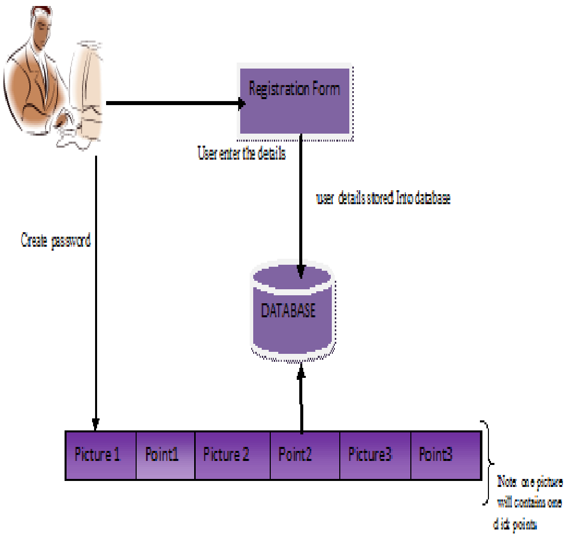
User Registration Process

Input : The User will enter the details and select pictures for password

Output :The user will receive a positive message from the system i.e. successfully registered.

System behavior:

The details entered by the user in registration phase will be saved into database along with the picture and click points. The systems ensure that all the fields are filled and no one picture is left out. In case of any field Missing system will generate a negative message.



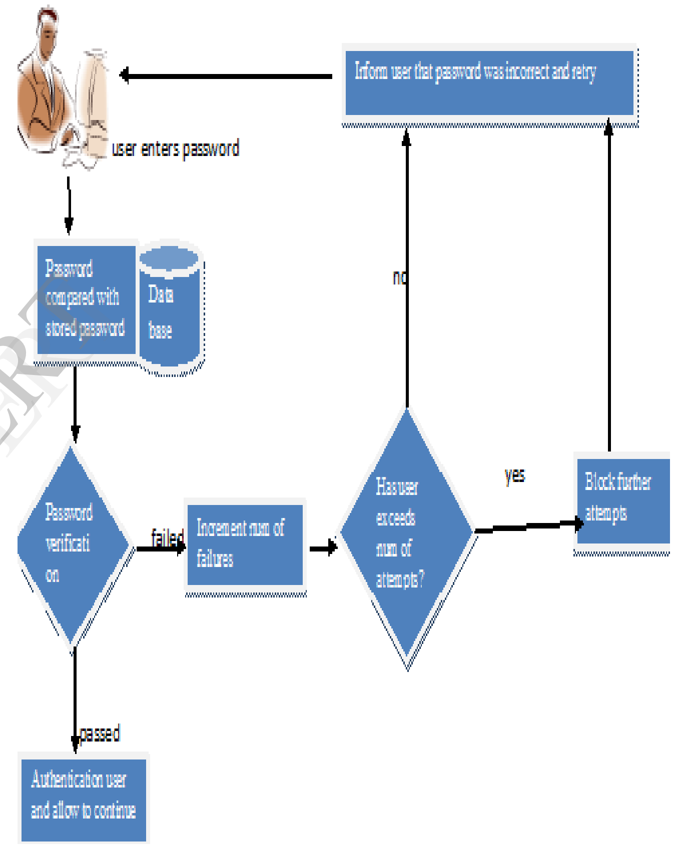
User Login Process

Input : The user provides the username and verify. The correct username give first image for password and continues to last image.

Output :The authentication confirmed message and open up the user account

System Behavior :

The system verifies the username with the login name from the registration phase. If the username exists then the system will load the first image from the database. The user click on the image and the system verified the point with the database if the point matches then next image will be displayed for password so on up to last image. Final click points verified and open up the user system or user account.


Inform user that password was incorrect and retry
user enters password
Password compared with stored password
Data base
no
Password verificati on
failed
Increment num of failures
Has user exceeds num of attempts?
yes
Block further attempts
passed
Authentication user and allow to continue

System Architecture

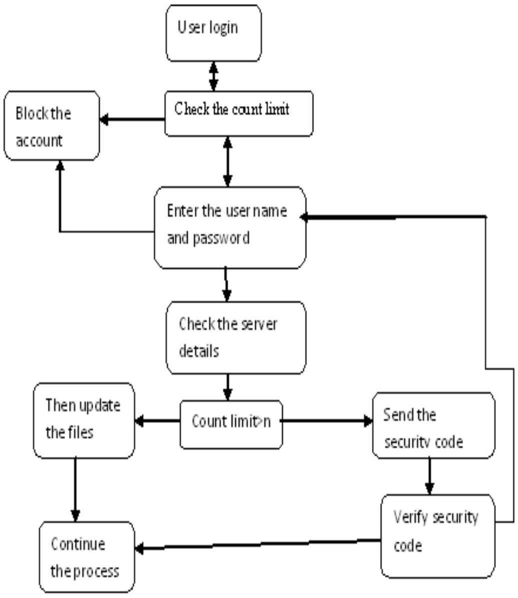


Figure: System Architecture

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 there login page, if user name and password is wrong again login the password then starts the count limit. If count limit>=5 then system send security code to user’s mobile. By using this code user can re-enter the password ,otherwise we will declare he is a legitimate user or fake process then legitimate user will be unable to enter the other mails. By using this method, we can reduce the hackers to guess the passwords.

This paper proposes a click-based graphical password system. During password creation, there is a small view port area that is randomly show on the image. Users must select a image password(click-point) within the current image. If they are unable or unwilling to select a point in the current image, they may use the Shuffle button to randomly reposition the image. The view port guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. By using this method we can easily reduce the brute force attack, dictionary attack, social engineering and Shoulder-surfing.

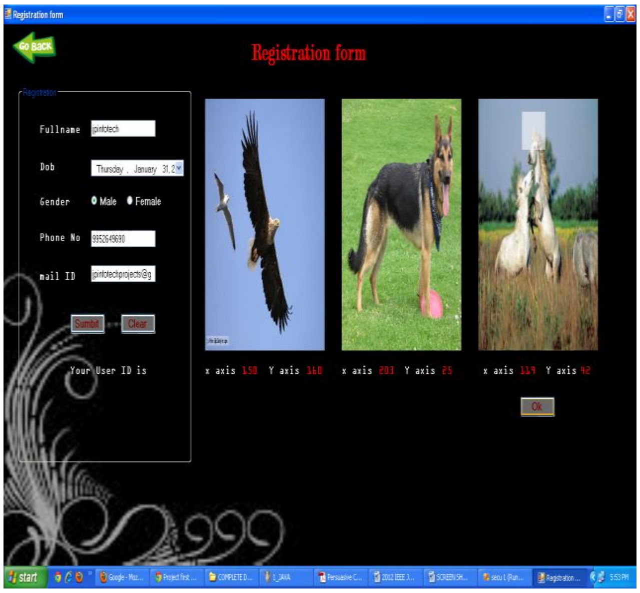
6. Detailed Description of Method Graphical Password Authentication Using Persuasive Cued Click Points

Persuasive cued click points(PCCP) is a proposed alternative to pass points and cued click points. In PCCP, users click one point on each of c=3 images rather than on three click points on one image. If offers cued recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point.

As shown in Figure.3,each click results in showing a next image, in effect leading users down a ”route” as they click on their sequence of points. An incorrect click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the subsequent images, they could create a new password involving different click points to get different images. If a user enters as wrong password, then the sequence of images from that point onwards,
It will be display incorrect and thus the login attempt will fail. For an hacker who does not know the correct sequence of images, this cue will not be helpful.

Expected Results:

- The user will enter the details and select pictures for password
- The user will receive a positive message from the system i.e. successfully registered.
- The user provides the username and verify. The correct username give first image for password and continues to last image.
- The authentication confirmed message and open up the user account



Registration form

Registration

Fullname jpintotech

Dob Thursday , January 31, 2

Gender ○ Male ● Female

Phone No 9952649690

mail ID jpintotechprojects@g

Sumbit Clear

Your User ID is

x axis 150 Y axis 160

x axis 203 Y axis 25

x axis 119 Y axis 42

Ok

7. Conclusion

In this paper, a persuasive cued click points authentication is are introduced. By using this persuasive cued click points, we can reduce easily dictionary attack and brute force attacks. In exiting system, we can use text characters as passwords by using these text characters the hackers are easily identify the text passwords so by reducing the guessing passwords we introduced (PGRS) persuasive graphical resistance protocol by using these we can reduce the hackers to guess the passwords. By using this PCCP users can create difficult passwords.

This paper proposes a new Password Guessing Resistant Protocol (PGRP) is, derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from legitimate users in most cases user can make several failed login attempts before being challenged with an Automated Turing Tests (ATTs). This ATT continue to be an effective, easy to deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users. This proposed system also provides protection against key logger spy ware. Since, computer mouse is used rather than the keyboard to enter our graphical password this protects the password from key loggers.

By using this PCCP and PGRP we can avoid the hackers who are guessing the passwords. We propose a new condition for this paper that is “Increment number of failures”, user can enter their password only five times, if more than he/she cannot enter into their achieved document or file. If user exceeds number of attempts then inform user that password was incorrect and to retry. We are sending security code to the user, by using this code he/she can re-enter their password. Again user can attempt wrong password then block the future attempts.

REFERENCES

[1] SoniaChiasson,Member, IEEE, Elizabeth Stobert,Alain Forget, RobertBiddle,Member, IEEE, and P.C. vanOorschot,Member, IEEE “Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, volume 03-No.3.Issue 01 March 2012

[2] Sonia Chiasson, P.C. vanOorschot,and RobertBiddle, “GraphicalPasswordAuthenticationUsing Cued Click Points” ESORICS, LNCS 4734,pp.359-374,Springer-VerlagBerlinHeidelberg2007.

[3]A.Salehi-Abari,J.Thorpe,and P.van Oorschot,“On purely automated attacks and click-basedgraphicalpasswords,” inAnnual ComputerSecurityApplicationsConf.(ACSAC),2008.

[4] ZhiLi, QibinSun, Yong Lian, andD.D. Giusto,,,Anassociation-basedgraphical passworddesign resistant to shoulder surfing attack‟,InternationalConferenceonMultimediaandExpo(ICME),IEEE.2005

[5] S.Akula andV.Devisetty,"ImageBasedRegistration and Authentication System," inProceedings ofMidwes InstructionandComputingSymposium,2004.

[6]S.Chiasson,E.Stobert,A.Forget,R.Biddle,andP.van Oorschot, “Persuasive cuedclick-points: Design,implementation, andevaluation of a knowledge-based authentication mechanism,”SchoolofComputerScience, CarletonUniversity,Tech.Rep.TR-11-03,February2011.

[7] P. C. van Oorschot andJ. Thorpe,“Exploiting predictabilityinclick-basedgraphicalpasswords,”Journalof ComputerSecurity,vol.19,no.4,pp.669–702,2011.

[8] 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