Secure Access to User Accounts by Software Puzzle and Digital Images

Bharathi.P[1], Ellammal.R[2], Jenny kalaiarasi.S[3] and Kapila Vani.R.K[4],
[1,2] Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India
[3] Assistant Professor, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India
[4] Assistant Professor , Department of Computer Science and Engineering, Prince Dr K. Vasudevan College of Engineering and Technology, Chennai, India

Abstract

To enhance security over passwords of user login account, username and password combined with the features of text-based and image-based CAPTCHAS for better security. This scheme specified as CAPGP. CaPGP is Call Puzzle as Graphical Password which has four stages of entering passwords. The first stage has username and password as register by individual user which look like normal authentication scheme, but the text-password has special feature of shuffling technique. The second stage is the selection of image from the group of images as his/her own pass-image. Solving a picture puzzle is third stage. Finally, the OTP generation is the last stage. These stages provide security against observation attack and shoulder-surfing attack.

Index Terms—*Graphical password, Pass-image, One-Time Password. Recall-based graphical system, recognition-based graphical system*

I. Introduction

Authenticating a correct user into their login account helps to safe our documents, communication and financial information. Usually authentication done by text passwords and personal identification numbers are deployed on devices and the web. Therefore, this password scheme has several issues such as lack of memorability and security. Sometimes the passwords are hard to remember , So the users reuse the one password for many accounts. Reuse of passwords helps the attackers for easy guessing the passwords across various accounts.

In order to overcome these problems the graphical password system helps to improve the memorability and provide resistance to online guessing attacks. The graphical password system [10] is effective password scheme by selecting an image or portions of image as his/her password. It improves the memorability and decrease error rate in entering a passwords. Graphical passwords avoids online guessing attacks. However graphical passwords have intelligent guessing attack, shoulder-surfing attack[14] and camera-based observation attack. The images used in a system are mostly stored in authentication servers which are easily accessible by attackers. The attackers identify the users graphical password by setting a camera in users work places, the hotspots activated in users place or watching passwords behind users shoulders. These are the problem behind the graphical password scheme.

To avoid the above issues, the new graphical password system along with puzzle technology has been implemented. Hence the system consists of both the text-based and image-based passwords. Authentication starts with entering a username and password here the shuffling technique may be used in entering the username and password according to the users wish. After entering this, the five set of similar images displayed the user select the pass-image among the decoy images. These decoy images confuses the attacker behind the shoulder or camera based attacks. Next step is that user arrange image puzzle this provides the security in a network. Finally OTP has been generated to the users mail account.

This system has been implemented with four stages of authenticating a user such as

1) Entering username and password.

2) Selecting the pass-image from group of similar images.

3) Solving pass-image puzzle.

4) OTP on mail.

These stages enhance a security over network. The shuffling technique of entering username, password and the random generation of similar images presented during log in, therefore these two stages are resistance to shoulder surfing attack and online guessing attacks. Third stage is solving a image puzzle, by arranging a parts of image security is provided in network. Finally OTP generated and send to the users mail account. After completing the four stages of authentication the users entered to their accounts.

This implementation represented as call puzzle as graphical password (CaPGP). CaPGP scheme demonstrates feasibility.

II. RELATED WORK

The survey on graphical password system describes two schemes, which are recall-based and recognition-based [1] schemes. These two schemes are comes under knowledge based authentication[10]. A knowledge based authentication specifies visual authentic password system.

The recall-based scheme based on creation of visual effects in screen and the recognition-based scheme based on pre-selecting the pass-image from the set of image and the user identifying the pass-image during registration.

Passwords are usually vulnerable to online guessing attacks and capture attacks. The graphical password focuses on avoiding both online guessing attacks and capture attacks.

Overview of Recall-based graphical system:

Recall-based graphical password system focuses on draw-metric or reproducing a secret images. these system exposes a entering the password by drawing in visible on screen by this attacks observe or record login page[3] and the area of drawing attacked by screen scrapers. This system improves user’s choice to create their own passwords though it is successful but it attacked by intelligent guessing.

DAS- Earlier recall-based graphical system is Draw-A-Secret. Users draw their password on 2D-grid using mouse while login users draw the password o same path of the grid [1].

BDAS- Background Draw-A-Secret helps the users to draw their password on background image. (2D-grid is replaced by any images)

Pass-doodle system[1] is the system of creating the password by freehand drawing. Pass-shape is another system similar to pass-doodle drawing the password on different shapes or different location. Pass Shapes are similar to pass-doodle during login the user draw the password in different locations on the screen.

Tao and Adams designs a Pass-go scheme allows the users to draw password in intersection points of a grid. The grid line intersection is presented the user draw on those line intersection points. But, this scheme vulnerable to dictionary attack[1].

Overview of Recognition-based graphical system:

Recognition-based systems also known as search-metric system where portfolios of images are provided by the system then the user has to select their pass-image from the portfolio. While login the user has to identify their pass-images among the decoy images. Phishing attacks are avoided here because the user recognizes the correct set of images at registration itself. The set of images file are stored on specific file and this file may attacked the information is known as attacker.

Pass-face is one of the recognition-based scheme allows the users to create their password by selecting an human faces. The system provides a set of human faces for selection of pass-image. A new version of pass faces done by giving a eye-gaze input in a ATM. This helps to improve the ability of choosing users passwords.

Other schemes such as story system, Déjà Vu scheme[1], pass points etc. In this type of scheme the set of images provided for each user from the set the each user select their own pass-image. Story system graphical passwords present the panel of images the user has to select the pass-image in correct order. By selecting the images in a correct the user correlate the images as story this helps the user to remember their passwords in sequence. Still the users have difficulty in remembering the password, so story passwords have only 85% succeeded among the users.

In Déjà Vu scheme provides a portfolio of images, the users select the subset of images as his/her pass-image. To log in, the user has to recognize the pass-image among the decoy images. The system generates a more set of images for different users but the users select the attractive images likelihood that images have similar probabilities with other users. This scheme is resistant to

dictionary attack because the few number of images selected by more users. Attackers are unable identify the images of users because the same image have a different description from each other images in a set.
These two schemes are deployed on various authenticating devices and organization.

Click based graphical passwords system

Click based graphical password provides security by clicking image or portions of image. The existing click based graphical passwords done by clicking a portions[5] of image such as clicking a specific regions of an image. Some click based graphical passwords are pass points, cued click-points, persuasive cued click-points. Click based graphical passwords increases the security by expanding the password space. Password space is choosing the strong passwords in an authentication system. There is some specified click-points based on regions on the stored image in a system. Clicking action as a password is easy for the users other than entering a textual passwords.

Some click based graphical passwords are

A. *Passpoints:* PassBYOP a new graphical password scheme implemented to secure the users passwords against the intelligence guessing attackers. Here the authentication process done using a physical token, the input of pass-image captured using camera token and then the image has shown to the user in live video. The system prompt the user to select any three points on the shown image and these selected points of image made as user password. While login the user select their three pass points. This is a multifactor authentication system where both the physical token and a password of the user need to authenticate. Users are flexible to give their own image input as passwords, by this users does not have restriction to set their passwords. PassBYOP uses a SIFT image processing algorithm which specifies the image features and descriptors. The matching of pass points done using the Euclidean distance between the original image and the entered pass points. Here the database has to maintain more than 1000000 images with accuracy of 80%.The main disadvantage is that every user has to carry a own physical token with them.

B. *Cued click-points:* It is a combination of pass points, pass faces and story system. A password system based on one click-point per image and the next image displayed based on the previous click-point[3]. Likewise the sequence of image displayed based on previous click-points. The user identify every click points for each image. Sometimes the user feels it is hard to remember the each click-point on each image. For example ordered sequence of five images in each image has one click-point click-point of first image specifies the next image. Users receive the immediate response whether he going to the correct login path. Attackers are unable to use hotspots because they have to analyze large set of images and the specific click-points of each image. Any wrong clicks on an image leads to the incorrect path or login fails. The password space for each image is in the range of $1 \leq i \leq 1200$ where $i=1,2,..5$ is image sequence which is next-image selection function f for selecting a distinct image. Every user have to pre-select the initial image by own. Still the shoulder surfing camera based observation is possible because we use only a five image sequence. For each image the system records the pixel coordinates for click points.

C. *Persuasive Cued Click-points :* Persuasive technology[4] has articulated by Fogg motivates the people to select the strong passwords. Persuasive cued click-points is the extension of cued click-points while creating a password the images are shaded except from the viewport. The viewport highlights the parts of an image and positioned randomly to avoid guessing and hotspots from the attackers. Here the user select the click-points password within a highlighted viewport area and the shuffle button is to randomly reposition the viewport. The viewport and shuffling done during a password creation. This system encourages the user to select more random click-points within the viewport area.

Overview on OTP and Image CAPTCHA

One-time password : OTP is a password system generated and used for one login session[13]. OTP is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single session only. OTP overcomes a replay attacks which are dynamically generated at every login session. Another advantage of OTP is that user may use a same password for many system at that OTP helps to prevent from attackers. OTP are generated through short message services, e-mail, and devices.

OTP generation algorithms uses a pseudo randomness concept by generating passwords distinct from previously generated OTP.OTP generation algorithm based on time synchronization and mathematical algorithms.

Text-based and Image-based CAPTCHA's :

CAPTCHAs, which are automated tests which distinguish humans from programs or robots, are used on many web sites to capture spammers in a network

Distorting non-continuous speech of every user taken as Audio CAPTCHAs and it has been deployed in all current schemes, including ones from Microsoft and eBay, which are easily broken.

Visual CAPTCHAs are preventing from spammers in free e-mail accounts. This CAPTCHA generated using EZ-Gimpy and Gimpy-r version[6] .EZ-Gimpy test uses 561 words of dictionary and Gimpy-r uses 4 random letter from 19 letters of dictionary. These two versions are used to distort the text to produce CAPTCHs. Matching of entered password with distorted text takes more time. De CAPTCHAs are inherently weak and, because of the importance of audio for various classes of users.

A new CAPTCHA based on graphical password to overcome a spyware attack[7]. It evaluates an attack that we denote as CAPTCHA smuggling. In many attack the CAPTCHAs are intended to inject on some web applications interactions and networking sites (such as web mail or social networking sites).These intended CAPTCHAs are looks like normal CAPTCHAs . Here a CAPTCHA contains the image along with distorted random string. User select the three pass-image from the portfolio for each pass-image three input sequence are entered to authenticate[6]. After selecting a pass-image the user enter the three input sequence . It is complex process where the login time increases.

Based on our evaluation, still CAPTCHA smuggling attacks are feasible in practice.

Therefore CAPTCHAs are used for some specific simple applications and it provides only less security.

.

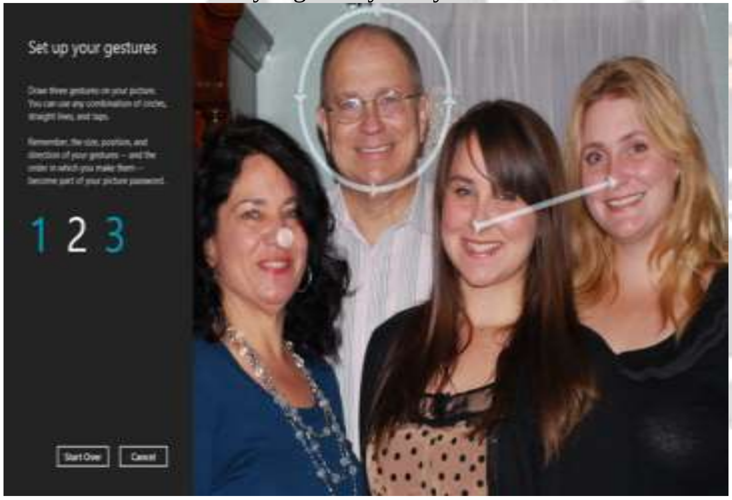
III. CURRENT METHODOLOGY

Touch-screen tablets and mobile are well suited devices for graphical password scheme. Now-a-days PC also deploys the graphical passwords using mouse to create passwords.

The windows 8 is a best example of picture passwords instead of alphanumeric passwords , here we sketch a custom sequence of gestures on top of a picture to verify your identity. Microsoft designs a picture passwords for non-touch systems also ,so the mouse used instead of your fingertips.

User select their own photos stored in a PC and then sketch the series of gestures on the selected photo. Setting up a picture passwords done using locally accessible images within a system. If the user fail to login that is forget the gestures the alternative text password used to log in to your system.

Picture passwords provides a security by tapping, use circles and draw lines over the image, these gestures are harder to guess because of the three way log in to your system.



Set up your gestures

Draw three gestures on your picture. You can use any combination of circles, straight lines, and taps.

Remember, the size, position, and direction of your gestures — and the order in which you make them — become part of your picture password.

Figure 1: Windows 8 picture password scheme

Refer the above figure shows the set up your gestures by

1. Tap anywhere on your picture.
2. Draw a circle anywhere on selected picture.
3. Drag a straight line.

Remember thepostionand the direction of all gesture drew on the image.

Even though the picture passwords fails because users simply forget the gestures they have chosen.

Image Recognition system currently used in CUB, the user register one image out of 12 images shown. When the user log in to the online banking , the pre-selected image displayed along with the 3 other images will be shown to the users and the user will prompt to select his pass-image.If the user select the wrong image more than three times then the questions will asked along with the images .

IV. PROPOSED SYSTEM

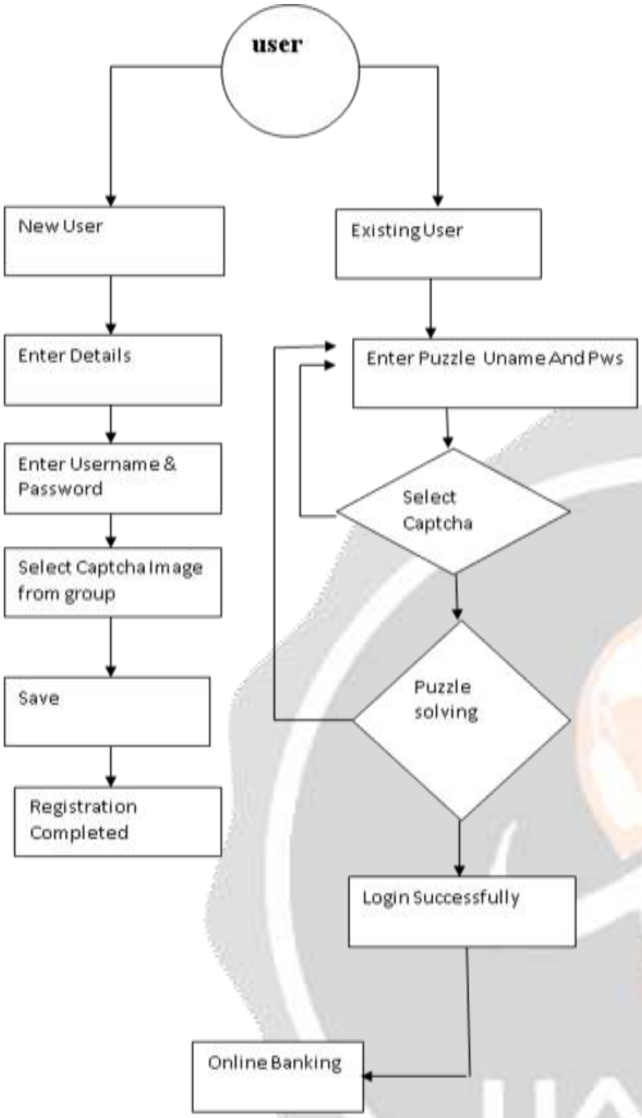


Figure 2: An overview of CAPGP

In this paper, the user register the username, password, pass-image and the puzzle image. Finally OTP has been generated to users mail account. We design a secure access to user accounts on net banking.

1) Stage 1: Registration

In registration process the user has to enter the username, password, E-mail ID and other details. After entering the user details the user register the pass-image in which this image has stored in cloud storage database for every user. The puzzle image also selected and registered to the cloud storage.

After the successful registration, The server provides a secret key for registered user (for example in banking application, the server provides a account number for user).Then the registered images are stored in server database .

2) Stage 2: Login

During login the user enter the username and password. One important feature of entering a username and password avoids shoulder surfing attack. Here shuffling technique involved that is where the user enter the username and password in shuffled manner because of this attacker get confuses. After entering this bubble sort algorithm used to sort the entered the both entered and stored username and password. If the entered and stored password are same then the user proceeded with the further levels of authentication.

3) Stage 3:Selection of pass-image

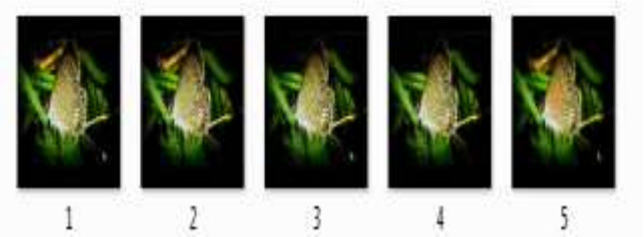


Figure 3:Selection of pass-image

In figure 3 displays the image set identification fot the user where the user has to identify his pass-image from the set. For example the original pass-image of the user is displayed below.

Figure 4:pass-image

The displayed figure 3 image set contains both the pass-image of the user and the duplicate images where all are looks similar. Any person behind you doesn’t easily recognize your pass-image immediately. The user has to select one image from the set. The duplicate images has some pixel variation.

Assume if you are any person behind the user, you closely looking the user movement of selection you can’t recognize the pass-image within 2 seconds.

Attacker guessing can be made for only one attempt. The one attempt of guessing is wrong then the alert message immediately sent to users mail.

4) Stage 4:Solving a image puzzle

After the successful selection of pass-image the user has to solve the image puzzle. The image is divided into four pieces where the four pieces are shuffled and randomly placed.

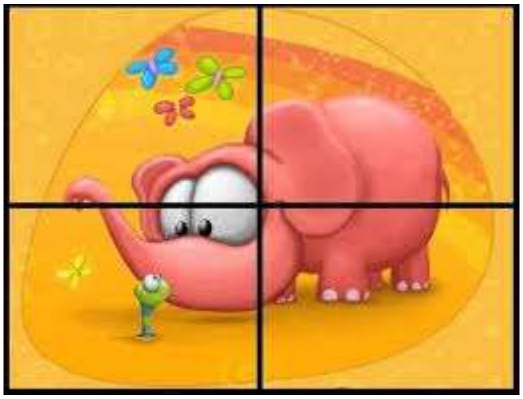


Figure 5:solving a puzzle

The solved puzzle image is submitted, the each pieces of image is checked one by one in the server.This provides security in a network for example the first piece is sent to the server for comparing the original image with the solve image. While tansmission the attacker may watch the image here the 4 pieces of puzzle image sent separately. Identifying the image in a network is too difficult than data.

The AI game programming involved in creation of puzzle image.At every time a new Randomnized display of image puzzle generated. The genetic algorithm used to randominize the puzzle.

5) Stage 5:OTP generation

Finally OTP has been generated to authenticate a user. OTP generated using AES algorithm .AES takes image as input and provides a OTP.OTP uses a MAC based on AES algorithm.

V. CONCLUSION

Efficient password scheme deployed using graphical password and One-Time password. Multi-stage authentication helps to avoid denial-of-service attack. This paper proposes the security on entering the password and a way to improvise this by securing and storing a large amount of images using a Big data concept.

VI. REFERENCES

[1] R. Biddle, S. Chiasson, and P. van Oorschot, “Graphical passwords: Learningfrom the first twelve years,” *ACM Comput. Surveys* vol. 44, no. 4,p. 19, 2012.

[2] “phishing records”,http://timesofindia.indiatimes.com/topic/Phishing

[3] S. Chiasson, P. C. van Oorschot, and R. Biddle, “Graphical password authentication using cued click points,” in *Proc. 12th Eur. Symp. Res. Comput. Security*, 2007, pp.

[4] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. Van Oorschot, “Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism,” *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. Mar./Apr. 2012.

[5] S. Chiasson, A. Forget, R. Biddle, and P. C. Oorschot, “User interface design affects security: Patterns in click-based graphical passwords, *Int. J. Inf. Security*, vol. 8, no. 6, pp. 2009

[6]Gabriel Moy,Nathan Jones,Curt Harkless, and Randall potter,Arete Associates,Sherman Oaks”Distortion Estimation techniques in solving a visual CAPTCHAs”IEEE computer society Conference on Computer Vision and Pattern Recognition(CVPR’04),2004

[7]Haichang Gao,Xiyang Liu,Sidong Wang,Rui Dai”A Graphical password scheme against spyware by using CAPTCHA” Symbosium On Usable Privacy and security (SOUPS) 2009,July

[8]Ahmet Emir Dirik,Nasir Memon,Jean-Camille Birget”Modeling user choice in the PassPoints Graphical password scheme”Symposium On Usable Privacy and Security(SOUPS) 2007.

[9] A. Forget, S. Chiasson, and R. Biddle, “Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords,” in *Proc. SIGCHIConf. Human Factors Comput. Syst.*, 2010 pp.

[10] G. E. Blonder, “Graphical passwords,” U.S. Patent 5 559 961, 1996.

[11] S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birget, “Design and evaluation of a shoulder-surfing resistant graphical password scheme,” in *Proc. Working Conf. Adv. Visual Interfaces*, 2006, pp.

[12] P. C. van Oorschot and J. Thorpe, “Exploiting predictability in click-based graphical passwords,” *J. Comput. Security* vol. 19, no. 4, pp. ,2011

[13]”one-time password”,
https://en.wikipedia.org/wiki/One-time_password.

[14]”what is shoulder surfing”,
http://searchsecurity.techtarget.com/definition/shoulder-surfing.

[15] S.Chiasson, R. Biddle, and P. van Oorschot, “Asecond look at the usability of click-based graphical passwords,” in *Proc. 3rd Symp. Usable Privacy Security,2007 pp.*