IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 63-69
www.iosrjournals.org

M-Wallet Security using Cued Click Points

Miss. Deepika Mhetre, Miss. Komal Murkute, Miss. Vishranti Kale,
Miss. Apurva Kabra, Prof. Sonali Madankar
Under Guided
(IT Dept., PVPIT, Pune, India)
IT Dept., PVPIT, Pune, India)

Abstract: *The main goal of this paper is to provide higher level of security by using graphical password authentication scheme. Text passwords are easily broken by various intruders and may hack all confidential information of user. User often create memorable passwords that are easy for attackers to guess, but strong system –assigned passwords are difficult for user to remember. So we are making use of alternative method where graphical images are used as passwords as human brains are better at recognizing images than text. The main goal of our work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult password to guess so that various security threats like brute force attacks, dictionary attacks, social engineering attacks ,shoulder surfing attacks can be successfully removed.*

Keywords: *Authentication, graphical passwords, guessing attacks, computer security.*

I. Introduction

Various graphical password schemes have been proposed as alternative to text-based passwords. Many research and experience have shows that text-based passwords have usability as well as security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text. Graphical passwords are intended to reduce the memory burden on users and coupled with a larger full password space offered by images ,more secure passwords can be produced and user will not resort to unsafe practices in order to cope. Primitive methods suffered from an innumerable number of attacks which could be imposed easily.Unfortunately, text passwords are broken mercilessly by intruders by several methods such as dictionary attack, shoulder surfing attack, social engineering attack etc. So to overcome these problems advanced methods have been proposed using graphical as passwords such as Cued Click-Points (CCP).

II. Related Work

2.1. Password Systems

Graphical passwords were first described by Blonder [6]. Since then, many other graphical password schemes have been proposed. Graphical password systems can be classified as either recognition-based (image based scheme, cued recall-based (image based scheme) or pure recall-based (grid based scheme)

2.1.1 Recognition Based

Dhamiji and Perring [4] proposed a graphical authentication scheme based on Hash Visualization Technique .In their system, user is asked to select certain number of images from a set of random pictures generated by a program and later user will be required to identify pre-selected images in order to be authenticated. Drawback of this system is that the server needs to store the seeds of the portfolio images of each user in plain text also the process is very time consuming for the user.

Akula and Devisetty's [2] algorithm is similar to Dhamija and Perring technique. The images will be converted into hashing code using SHA-1 technique to give more secure and less memory. This technique produces 20 byte output. Both the above algorithms have tendency to reduce Shoulder surfing attacks.

Hong,[3] proposed another shoulder surfing resistant algorithm. This technique allows the user to select their own codes to pass-objects variants. This method force the user to memorize many text strings and therefore suffer from the many drawbacks of text based passwords.

"Passface" [5] is a technique developed by Real User Corporation. In this, the user will be asked to select four images of human faces from a face databases their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures. But this technique took longer than text passwords and therefore was used less frequently by users and hard for user to remember faces.

2.1.2 Recall based techniques:

Based on Blonder's [6] original idea , Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image as shown in Figure.To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points.

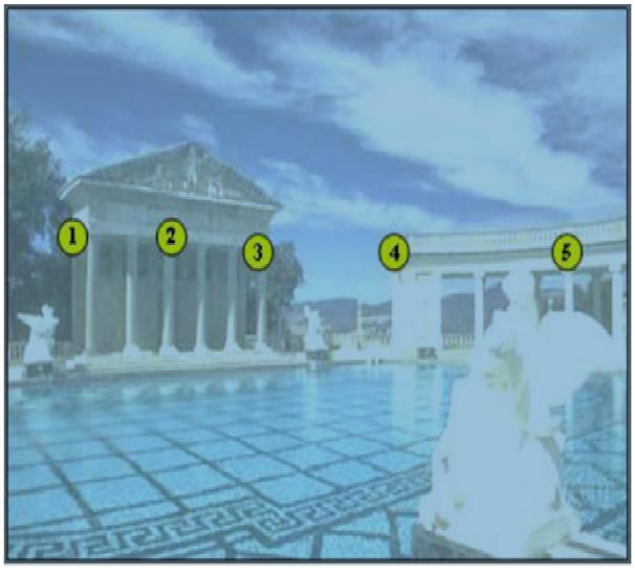

Figure 1: Pass Points

III. Proposed System

3.1 Cued Click Points (CCP)

CCP was developed as an alternative click based graphical password scheme where users select one point per image for five images. The interface 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 next 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. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image 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.

IV. Project Work

4.1 Project Workflow

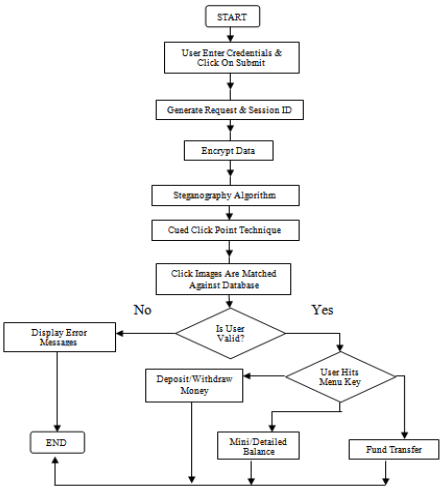

Figure 2: Workflow of Proposed system

1. User enters user ID and Password
2. Data is Encrypted using AES and send to the server
3. Server Checks the credentials in database and returns result
4. Server send SMS on users mobile phone
5. Client wait for an incoming SMS
6. If SMS is for valid IMEI no then user is shown with CCP images
7. User gets 5 images in sequence for authentication
8. Each image is divided into 4*4 matrix and user has to select one point per image and advances to the next image
9. If valid user then user gets the banking menu.

4.2 Project Implementation

The project illustrated in this paper is entirely base on the idea of graphical password. We are developing a login technique that can be used in various applications like banking, facebook, mobile applications etc. where security of data is major concern.. Here the aim of our work is to provide 2-levels of security for transaction in mobile banking application. Confidential files and data are kept secure with this login technique as we are making use of 2-levels of security. First, we are making use of steganography technique for sending userid and password to the server by using steganography encoded images from client mobile phone. Second, we are going to implement CCP technique for authentication. Project includes registration process, CCP selection process, accessing Banking menu.

4.2. 1.Registration Process (SERVER)

When we run application, a login form pops up allowing user to enter userid and password. The form consist of login button.

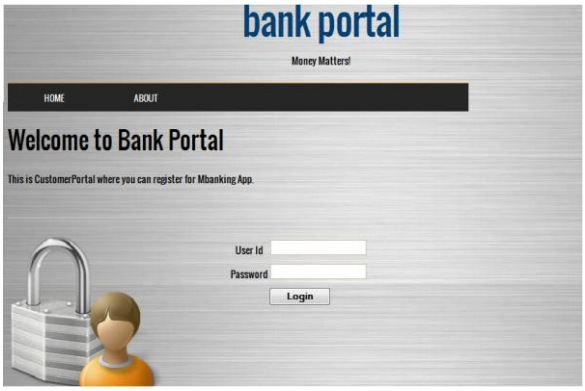

Figure 3: Login Screen

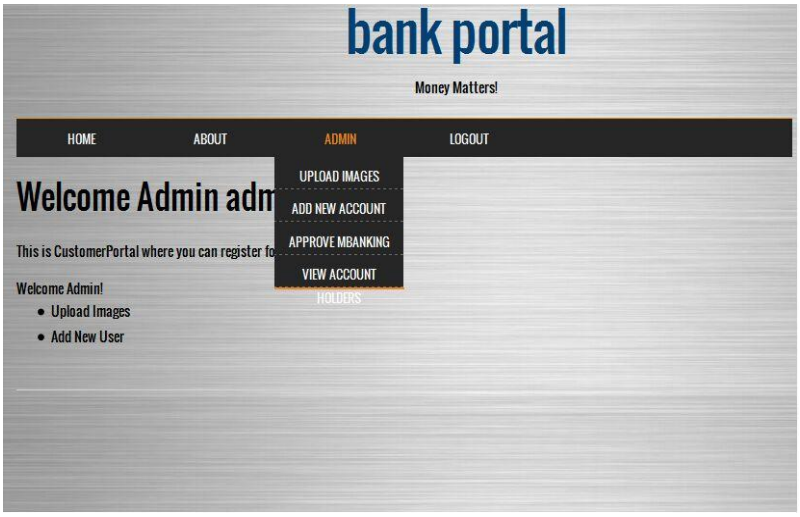

Figure 4: Menu Screen

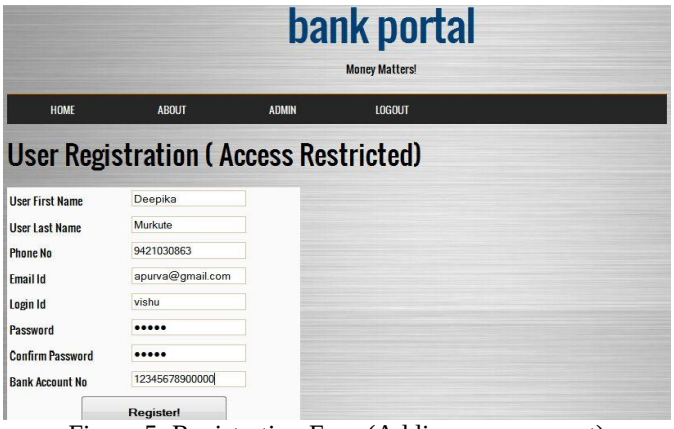

Figure 5: Registration Form(Adding new account)

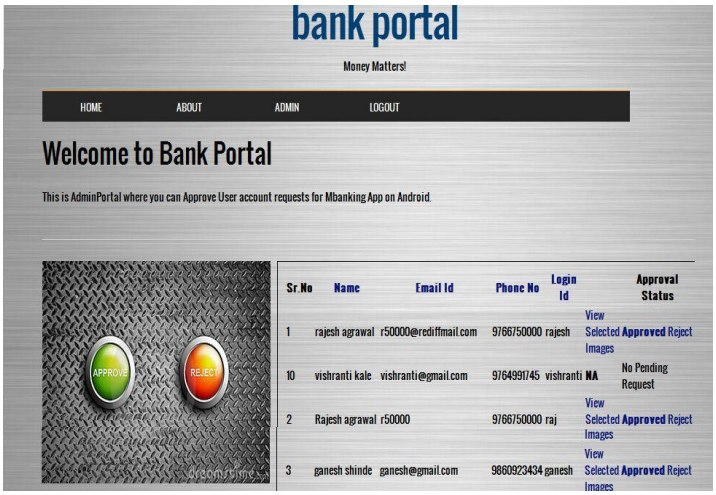

Figure 6: View or Approve Mbanking.(Managing account).

If the user is registered user then after entering valid userid and password user will advances to next phase of project. If the user is not registered then user has to fill banking application form to access Mbanking. After entering all mandatory fields user will assign userid and password. This user credentials are required to access Mbanking application on user's mobile phone. After click on register button user will be able to login with his/her userid and password and perform further process of ccp selection.

4.2.2 CCP Selection Process

Figure 7: User login.

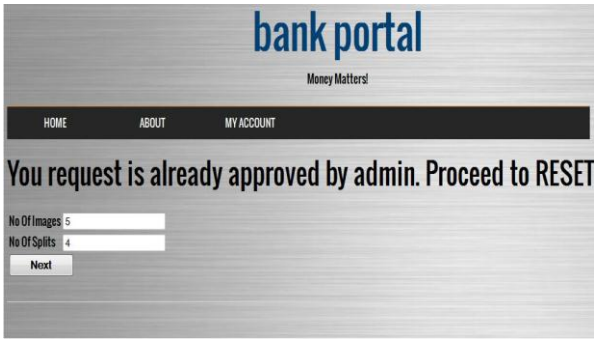

Figure 8: User chooses no of images and Splits.

Figure 9: image selection process

Figure 10: CCP selection process

After entering user id and password user will display his/her own portal. At this point user has to select only 5 images and click on confirm button. Then all these 5 images will be displayed in grid format and user needs to select one click point per image. After selecting all 5 click points access request for accessing banking menu on his/her android phone has been raised.

If admin approves this request then user will be able to use banking menu on his/her android phone.

4.2.3 User Registration (CLIENT)

When admin approves request then user will be able to access banking menu on phone. First of all Mbanking app will be installed on android phone for valid user only. User need to enter same userid and password on mobile. This credentials are matched against database and if valid user will be shown with banking menu.

Figure 11: Mobile login

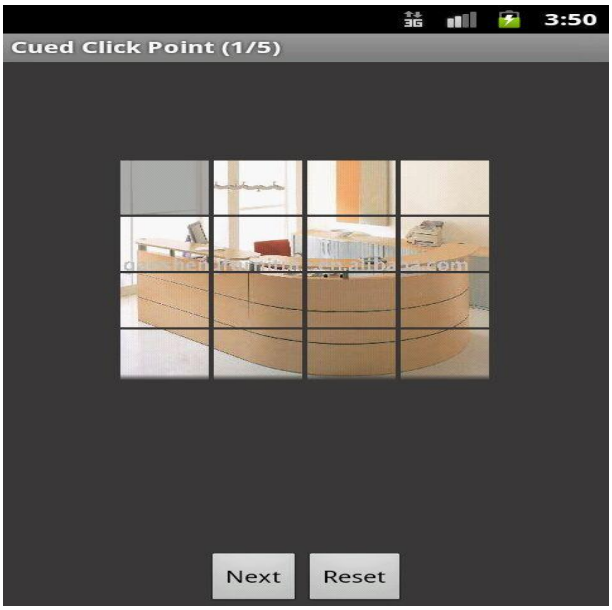

Figure 12: CCP Authentication on mobile.

Figure 13: Banking Menu (After successful CCP authentication).

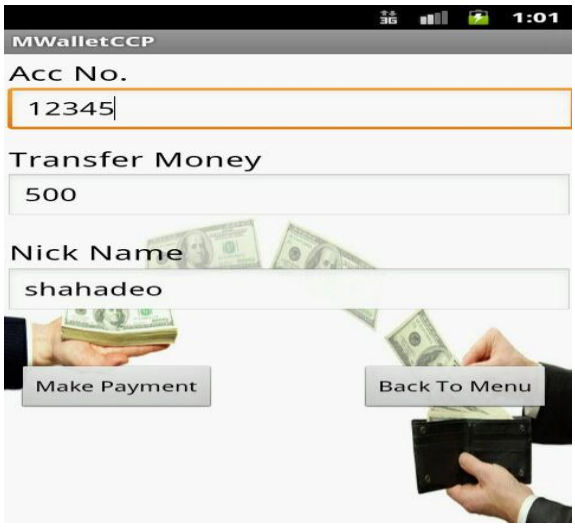

Figure 14:Required option will be taken place.

If username and password are valid then user will be shown with ccp selection form. At this point User has to select Same click point per image that is selected at Registration time. If all click points are correct then user will be shown with banking menu and able to perform all banking transactions like fund transfer, minimum statement of accounts, change password or update profile.

If any of the click point enter is invalid then next image displayed will be the random image so that unauthorized user cannot understand where is actual mistake and banking menu will not be displayed.

V. Conclusion

The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over PassPoints in terms of usability. Being cued as each images shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image.CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images.

In this way, we provide 2 levels of security. First we are making use of Steganography for sending user id and password on server. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect.

Acknowledgements

The authors would like to thank project guide Prof. Sonali Madankar and H.O.D. Prof. V. S. Nandedkar, PVPIT, Pune (India),for their guidelines and involving in research.

References

[1] Chippy. T and R.Nagendran**, "**DEFENSES AGAINST LARGE SCALE ONLINE PASSWORD GUESSING ATTACKS BY USING PERSUASIVE CLICK POINTS," in International Journal of Communications and Engineering Volume 03– No.3, Issue: 01 March2012.

[2] S. Akula and V. Devisetty, "Image Based Registration and Authentication System", in Proceedings of Midwes Instruction and Computing Symposium, 2004.

[3] S. Man, D. Hong and M. Mathews, "A Shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management." Las Vegas, NV, 2003.

[4] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[5] Real User Corporation: Passfaces. www.passfaces.com

[6] G. E. Blonder. Graphical passwords.United States Patent 5559961, 1996.