International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 9, September 2014 **ISSN 2319 – 4847**

Innovative Graphical Passwords using Sequencing and Shuffling Together

Rashmi Wable[1], Dr.Suhas Raut[2]
N.K. Orchid College of Engineering and Technology, Solapur

ABSTRACT

Graphical authentication technology is to make the method usable and secure for the user. Pictures are easier to remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures. The main security reason for graphical password is harder to guess or broken by brute force, and also if the numbers of images are more then, complexity and security provided for system is very efficient. In this paper graphical password is developed for android mobile system. This type of system does not exist in android and the theme will give more security for mobile. The two methods cued click points and persuasive click points have their own advantages and disadvantages. Here is taken an effort to remain advantages and disadvantages by proposing a third methodology that combines both of them together and this will surely increase complexity by including more images. Major goal of this paper work is to reduce the guessing attacks as well as encouraging users to select more random password with multiple images.

Keywords:-Android mobile system, Graphical password

1.INTRODUCTION

In the present graphical password system which are mainly made for remote desktop application here in this paper effort taken to make it for android mobile system. Graphical passwords basically use images or representation of images as passwords. At the same time we try make the password more complex which will be difficult to hack. The system provides complexity for it will make the system more safe and secure. The previous techniques cued click points and persuasive cued click points consist of sequencing and shuffling we tried to make this sequencing and shuffling together in this methodology. The second thing address in this to prove the existence of biases toward certain types of images in graphical authentication tokens chosen by users; and to characterize such biases if they do exist. There has been a great deal of hype for graphical passwords since two decade due to the fact that Primitive's methods suffered from an innumerable number of attacks which could be imposed easily. In this method will have authentication methods .To start with focus on the most common computer authentication method that makes use of text passwords .Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. In this existing system password it is very easy to hack the text password system. In graphical password for android mobile we have provided selection of number of images as per user's requirement and number of splits gives for images will be define by user on the server. Then on client side user will select the clicks as per defined on the server side if clicks are right then it will show login successfully otherwise if clicks are wrong then it will show wrong images and login cannot be successful. Security is maintained by having server and client system and each and every user can select their images and clicks separately.

2.RELATED WORK

There are many different techniques present in graphical password technology. Passfaces technique is easier to remember compared to textual passwords [12]. It is the combination of attractive password faces but it also takes too much longer time than password faces. The next scheme consist of passobjects scheme but it consist of 1000 objects on the login process and this make display more crowded and making it difficult to find the pass objects and if number of objects is reduced the size of password space will become smaller and it become easier to crack and guess. The repeating process several times by clicking or rotating it randomly and this become confusing and time consuming since it consist of two many pass objects. The Dhamija and Perrig password system Based on Blonder's 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 [3]. To log in, a user must click within some system-defined tolerance region for each click-point. This acts as a cue to help users remember their password click-points and for this sequence of click points provided. And if you click on wrong sequence then click points will get blocked. This drawback of the pass point system that clicks points will get blocked. But as per security point of view it is the strong system but finding click points sequence is time consuming task so innovative graphical password system will help user to come out from this drawback and surely this will provide

more security also. In cued click point technique which is a next graphical password scheme where users select one point per image for five images but it is sequence defined with combination of number of images in the defined sequence of cue. The interface of click point displays only one image at a time and then image will get replaced by the next image. But it is necessary that point should be correct and after that only it will get correct sequence of cue. The next technique is persuasive cued click point consist of concept of shuffling. For accepting password user must select click point within view port area. If user unable to find the view port then user can press the shuffle button. But this is time consuming task to find the click point in the shuffle button so the new technique defined in this paper will help to overcome from these disadvantages will surely make system safe and secure.

3.DESIGN AND IMPLEMENTATION

The proposed system consists of the Client Server architecture and design part of the system includes diagrams of server and client class diagram. Server part consists of collection of all images plus registered click points also. The server has the authority to store all information of the user also user creation and deletion is done on the sever side only. The server part of the system then created a separate login for the user and assigned each username and password. Then the user will login by username and select particular images user want to select also give no of splits how much the user wants to give and then select the splits area user want on one image or number of images after all this selection the user will confirm the clicks and logout and then Administrator will approve the request. After approving the request from the Admin now user can login on the mobile by first establishing connection with the server then can login with their username, and then images will be shown to the user whatever user selected on the server side then by clicking appropriate images clicks users can get successfully logged on the mobile device. The database of the server mainly stores registration information of the user and also a number of images stored and also its clicks. The client side of the system that is the mobile device has registration activity on the server side and also again image selection and Theme clicks selection activity after following all this activity only then the client can successfully login into the mobile device.

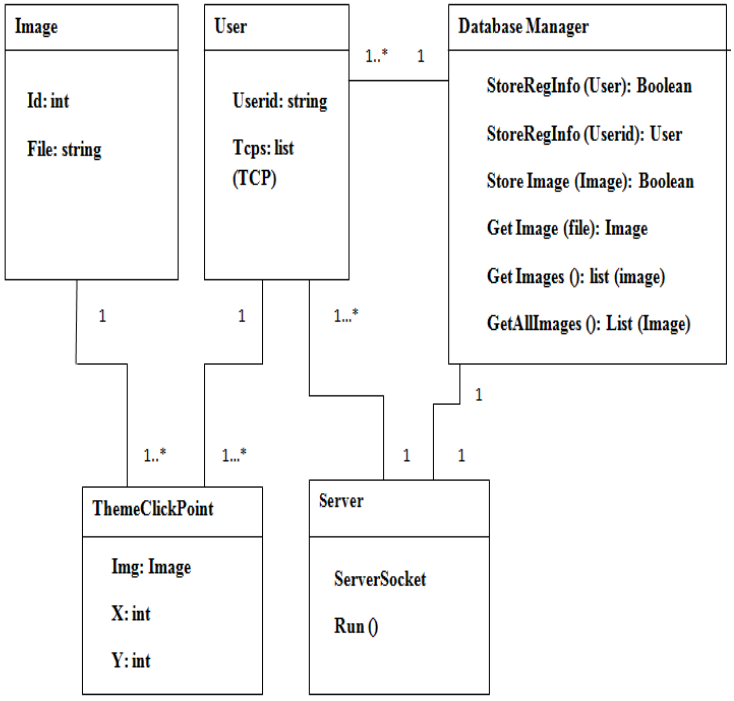

Figure 1: Server class diagram

The existing graphical password scheme where a password consists of an ordered sequence of five clicks-points on a pixel-based image .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. CCP is developed as an alternative click based graphical password scheme where users select one point per image for five images [Sonia Chiasson et al]. 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.

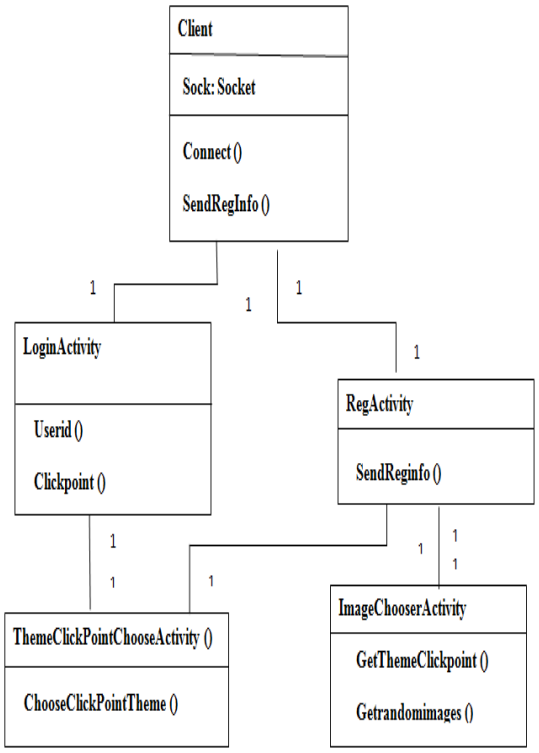

Figure 2: Client Class Diagram

The existing 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 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. To address the issue of hotspots, PCCP was proposed [6]. As with CCP, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned. 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. In the proposed system the existing result present is the graphical passwords according to the sequencing. The second system they have is the shuffling of graphical passwords. But shuffling is more problematic because the entire time user has to search for the new click point. To overcome from this problem of shuffling the new system of click points has been introduced that is mentioned in the diagram .In the setup phase of the system first user will login according to theme and he will do clicks according to it. And in this way security will be generated to the system that the user only knows that theme. So any other third party will not be able to hack that system and also there is no need to search the view port all the time. According to theme if user clicks that point theme will be accepted otherwise after three clicks that user will get a blocked means user will not be able to login by having wrong clicks on split images and this is the setup phase of the system. This graphical password have created for android mobile and have provided selection of number of images as per user's requirement and number of splits gives for images will be define by user on the server. Then on client side user will select the clicks as per defined on the server side if clicks are right then it will show login successfully otherwise if clicks are wrong then it will show wrong images and login cannot be successful that is it get blocked.

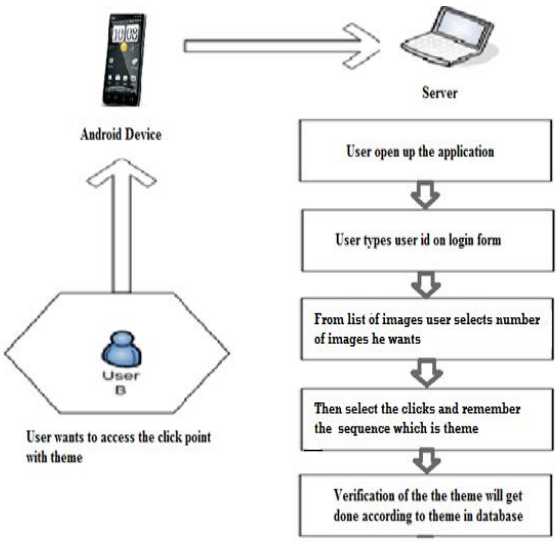

Figure 3 : Software Block Diagram

3.1 The Experimental setup of the system

In the experimental phase of the system first check the clicks given by the user are correct or not according the clicks mentioned on the server by user and while giving clicks on server side the user will remember the sequence of clicks given by user that is theme. The first step on server side for user is to register user on admin after registering that user will login then on first window user has to give number of image and number of splits user want to give for the image then, user will confirm this first and then next window will get open. In the next window user will select the images as per user given the number in the previous window and then user will click on confirm button. Now the images with splits are shown to the user click on images as on 1st image user can give 5 clicks on it and numbering of splits shown to user after user select the clicks now user has to note down it and this will be the theme for the user which is stored in the database. For example if user has selected two images and then defined clicks on the server then the theme sequence stored like 1.2,2.2,1.3,2.4#1.2,2.2,1.3,2.4 in this way this click based sequence means theme will get stored into the database.

4.RESULTS

The result of the system consists of the following screen-shots. In the first login first user has to establish the connection with server by giving servers IP address and then will click on green check box if server IP address is correct it will show the message connection establish with the server. Now the system is ready to access the right click points from the server.

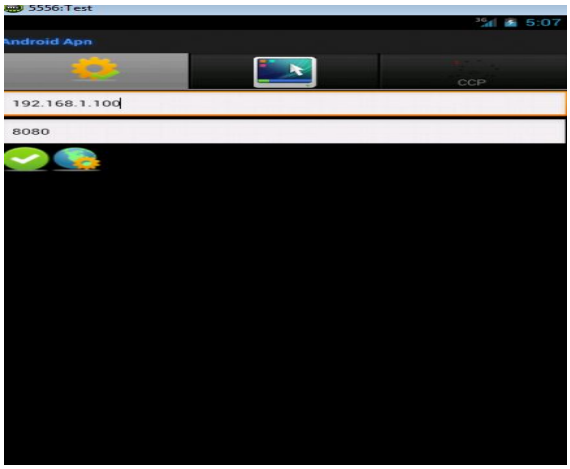

Figure 4: IP Input

The next screenshot shows login id given by user after clicking on login button then the window of first image comes with splits on mobile screen i.e. figure 6 now user has to click points per defined by theme. Then click on image 2 and then login completes.

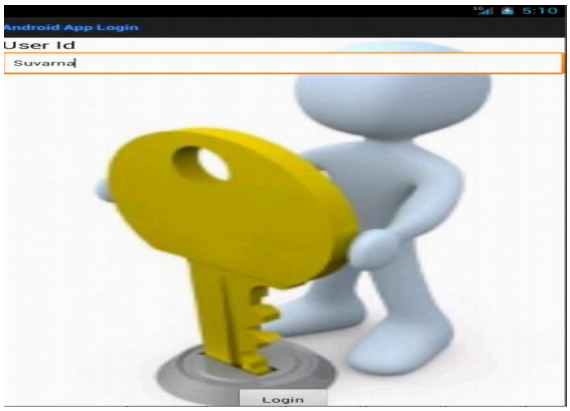

Figure 5: Login screen

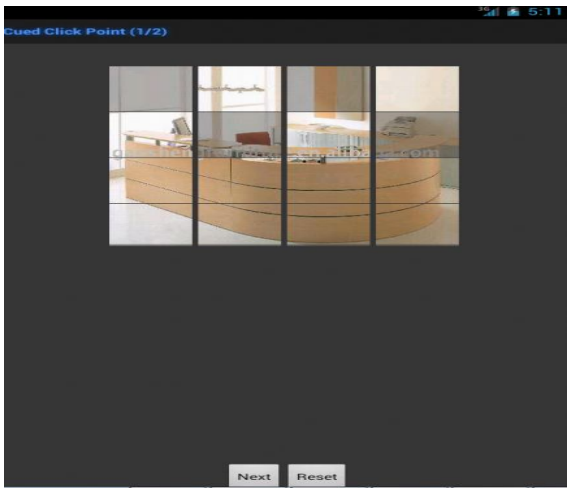

Figure 6: First image clicks

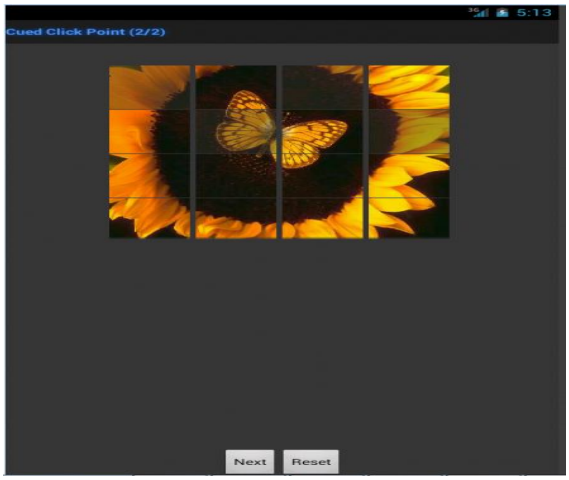

Figure 7: Second image clicks

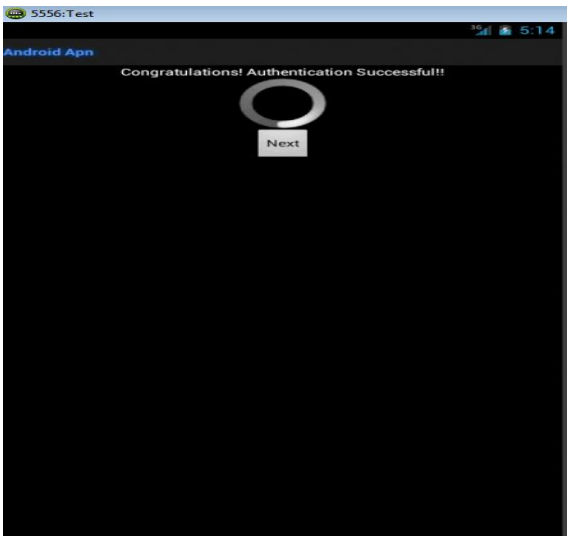

Figure 8: Login successfully

5.EVALUATION

Table 1. Evaluation of Result

User	# Image no	# Split no	# Matrix divide	Maximum selections allowed per image	Selections given by user
User 1	1	4	4x4= 16 splits per image	5	5 clicks
User 2	2	3	3x3=9 splits per image	5+5=10 selections allowed for 2 images	1st image=5 2nd image=5 = 10 clicks

For CCP password methodology only sequencing is provided with the help of cue and also it is the combination of multiple images which are used as click points. The Theme click point password provides the user to click their click points with the split images and click points allowed for it maximum up to 5 click points. So in the evaluation phase the following steps include

Select Number of images = 2
Select Number of Splits = 4

Now to assign splits for per images have to multiply
Number of image splits = 4x4=16

So the now images get divided into 4x4 matrix and we have got 16 splits now the next step user has to follow is selection of click points on each image 5 clicks selection is allowed so 5+5=10 total 10 clicks selection allowed now it's up to user how many clicks user want to select. Multiple numbers of images we have given to increase the complexity of the system.

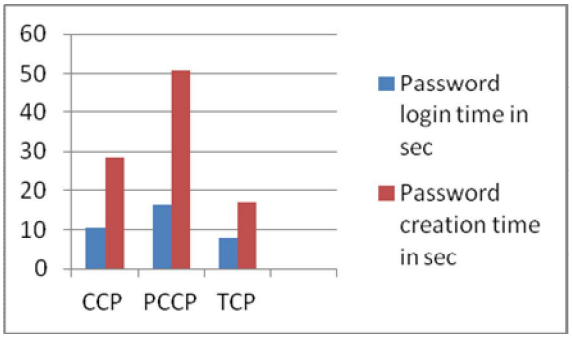

Figure 9: Password creation and login time in seconds

The two techniques Cued Click Point and shuffling of click points having some drawbacks so the third methodology suggested in this paper will help the user to provide more security for the android mobile device and also overcome disadvantages with the help of this technique which were present in the previous techniques [5]. The number theme provided in the sequence which is numbering theme will avoid the problem of shuffling as in the technique of shuffling user has to select all the time the view port until user find correct view port and this was the time consuming task [7]. The comparison of graphs shows TCP technique saves a lot of time because of numbering sequence proper sequencing theme has been provided and also the problem of shuffling is get overcome with this technique and combination of both the techniques will get provided in this technique and surely this will save the time of user also.

6. CONCLUSION

The output of proposed system will help to make a system secure and safe. Also as per evaluation TCP completes the process of password creation in 18 seconds and this shows it is faster than CCP and PCCP technique. The number theme will make easier to remember click and this will surely helpful for user. Combination of the theme of click point's passwords will help the system to prevent from the hacker. This new Click point password makes the system more secure. The output system is combination of sequencing and shuffling together.

REFERENCES

[1] A.Adams and M.A.Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46 1999
[2] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwes Instruction and Computing Symposium, 2004.
[3] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
[4] Jansen, W., Gavrila, S., Korolev, V., Ayers, R., Swanstrom, R., "Picture Password: A Visual Login Technique for Mobile Devices"
[5] Suresh Pagidala, C. Shoba Bindu Improved Persuasive Cued Click Points for Knowledge-Based Authentication
[6] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing Shoulder-surfing by using Gaze based Password Entry", Symposium on Usable Privacy and Security (SOUPS), July 18-20, 2007, Pittsburgh, PA, USA.
[7] Alain Forget Sonia Chiasson Robert Biddle P.C. van Oorschot "Influencing Users towards Better Passwords Persuasive Cued Click-Points"
[8] Real User Corporation www.realuser.com