Industrial Science
Vol.1,Issue.6/Aug. 2014 **ISSN** : 2347-5420

Research Papers

ANDROID MOBILE APPLICATION USING NEWLY INVENTED GRAPHICAL PASSWORD TECHNIQUE

Rashmi Wable[1] and Suhas Raut[2]

[1]NK Orchid College of Engineering & Technology, Solapur.
[2]NK Orchid College of Engineering & Technology, Solapur.

Abstract

Graphical authentication technology till now is made for Desktop applications here in this paper have taken effort to make it for the android application. The two techniques cued click point and persuasive click point having their own advantages and disadvantages so have tried to make the third technique which will help to overcome from these disadvantages.

Here is taken an effort to increase its complexity and to increase its security. Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures. This paper consist review of making the third combining technique of these two techniques together. This will surely make the system more safe and secure.

KEY WORDS:

Android mobile system, Graphical password.

INTRODUCTION

Graphical passwords basically use images or representation of images as passwords. Till now this system is made for mainly for desktop mobile applications but this review is done for android mobile device. Nowadays it is become necessary to make such an application for android device and the combination of multiple images provide the security for the mobile. The number theme made in this system will help user to make security more tight and also this will increase its complexity. Our focus is also on to increase the speed of operation. At the same time, we will take effort to make passwords assigned by the scheme are difficult to hack & also will be difficult to remember. Specifically, if people have a bias toward specific types of images, such as photos of faces, they choose it as authentication tokens, and then an attacker may use this bias to improve his chances of guessing the right authentication tokens.

RELATED WORK

The text passwords are unfortunately broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks. To mitigate the problems with traditional methods, advanced methods have been proposed using graphical as passwords [7]. The technique Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique [3]. In their system the user is asked to select a certain number of images from a set of random pictures generated by a program later the user will be required to identify the pre selected images in order to be authenticated. In the CCP technique the same technique provided with the queue. But it was time consuming task to select

the images from the random images In persuasive cued click point technique it consist of problem of shuffling and finding of view port. All the time resetting the scheme and finding a view port was also time consuming task. This drawback of the system is get covered in our innovative graphical password system that the user select the image user wanted from the number of images and then as per clicks number theme will get defined to user. So this will save the time as well as it is easy for user to recognize n guess the theme if user follows the particular sequence But as per security point of view it is the strong system but finding click points sequence and also remembering that specific tolerance region 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.

III. PROPOSED SYSTEM

The existing graphical password system where a password consists of an ordered sequence of five click-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. 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 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. As with CCP, a password consists of five click points, one on each of five images.

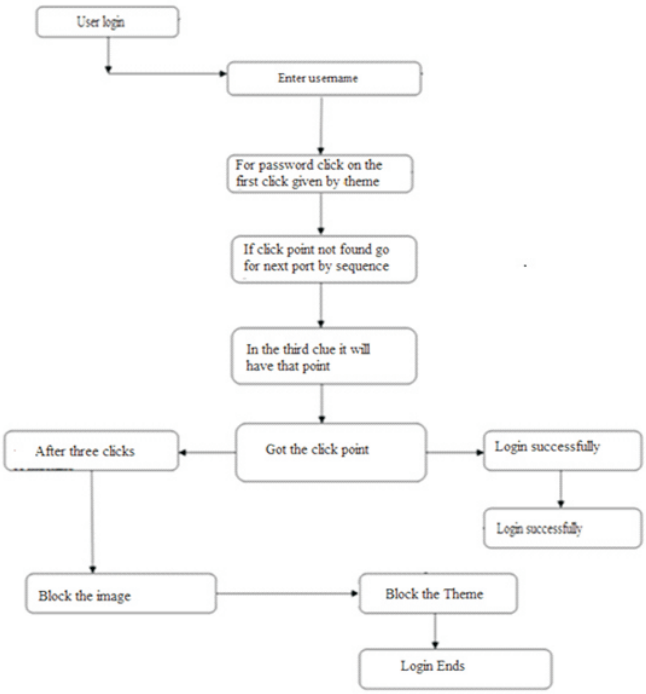

Figure 1: System workflow

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 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 points theme will be accepted otherwise after three clicks that user will get 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 block.

VI. EXPECTED PERFORMANCE IMPROVEMENT

In the above proposed system mentioned scheme theme click point is combination of sequencing and shuffling together so security maintained for the graphical password scheme will be more and also the number of more images will increase the complexity of the graphical password. The technique will surely help to provide the more security.

V.CONCLUSION

The purpose of proposed system will help to make a system secure and safe. The 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. Output of the system will be combination of sequencing and shuffling together. We expect more secured system upon implementation of our password strategy.

VI. 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.I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.
6.S. Man, D. Hong, and M. sLas Vegas, NV, 2003.
7.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.
8.L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
9.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.
10.Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto , "An association-based graphical password design

resistant to shoulder surfing attack", International Conference on Multimedia and Expo (ICME), IEEE.2005.
11.Real User Corporation www.realuser.com
12.K. Dinesh Kumar Automated attacks on pass point style graphical password
13.Robert Biddle, Sonia Chiasson, P.C. van Oorschot Graphical Passwords: Learning from First Twelve years