IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-02, Issue-12 E-ISSN: 2347-2693

Graphical Password Authentication Using Cued Click Points

[1]Greeshma P.Y, [2]Jerry Joe, [3]Jisna V.A, [4]Krishnapriya M.A, [5*]Saranya T.G

[1, 2,3,4,5*]*Department of Information Technology*
Jyothi Engineering College, Cheruthuruthy, Thrissur, Kerala, India

www.ijcaonline.org

Received: Nov /22 /2014 Revised: Nov/30/2014 Accepted: Dec/12/2014 Published: Dec/31/ 2014

***Abstract*—** Cued Click points (CCP) is a click-based graphical password scheme, a cued-recall graphical password technique. Users Click on one point per image for a sequence of images. Performance was very good in terms of speed, accuracy, and number of errors. Users preferred CCP to Pass point, saying that selecting and remembering only one point per image was easier, and that seeing each image triggered their memory of where the corresponding point was located, CCP also provides greater security than Pass Points because the number of images increases the workload of attackers.

Keywords— *Cued Click Points, Graphical Password, Performance, Passpoint, Security, Attackers*

I. INTRODUCTION

Today computers have become a major part of everyone's life. Use of computers is not only restricted for corporate use but also for personal use and inter communication purpose [1]. Passwords are used for (a) Authentication (Establishes that the user is who they say they are). (b) Authorization (The process used to decide if the authenticated person is allowed to access specific information or functions) and(c) Access Control (Restriction of access-includes authentication & authorization).Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess.While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Number of graphical password systems has been developed;
Study shows that text-based passwords suffer with both security and usability problems.

According to a recent news article, a security team at a company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords[2]. It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic. The password is a very common and widely authentication method still used up to now but because of the huge advance in the uses of computer in many applications as data transfer, sharing data, login to emails or internet, some drawbacks of normal password appear like stolen the password, forgetting the password, week password, etc so a big necessity to have a strong authentication way is needed to secure all our applications as possible, so researches come out with advanced password called graphical password where they tried to improve the password techniques and avoid the weakness of normal password. Alphanumeric passwords were first introduced in the late 1960s.Today, many networks, computer systems and Internet-based environments used this technique to authenticate their users. The vulnerabilities of this technique have been well known generally. Dictionary attack is the commonly method used by hackers to break or crack the alphanumeric password, such attack is very efficient mechanism because its only need a little time to discover the users passwords.

Another major drawback of this method is the difficulty of remembering the passwords.Graphical password techniques have been proposed as an alternative to alphanumeric based techniques. It has been designed to overcome the known weakness of traditional alphanumeric password. It also designed to make the passwords more memorable, easier for people to use and therefore more secure. Based on the two assumptions; first, humans can remember pictures better than alphanumeric characters and second, a picture worth a thousand passwords; some psychological studies and company software seem to agree with these assumptions. As known generally, the main drawbacks for the current graphical password schemes are the shoulder surfing problem and usability problem. Even though graphical passwords are difficult to guess and break, Nevertheless, the issue of how to design the authentication systems which have both the security and usability elements is yet another example of what making the challenge of Human Computer Interaction (HCI) and security communities.

II.OVERVIEW

Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, users click one point on each of

Corresponding Author: *Saranya T.G*

images rather than on five points on one image. A password consists of one click-point per image for a sequence of images. Our project is mainly divided into two process. They are registration process and login process. In registration process the user has got the opportunity to choose a unique username.

Then user selects the number of images he/she wanted. At each image user selects a particular point users has to select at least five images as their password. Users has got the privilege to select more than five images too. Then the system while create a user profile vector which is a combination of the username and the click points on each image. This user profile vector is stored in the database.Next we have the login process. The user will sent the login information which contain the username. Then the system will show the set of images to the user. Then the user will select the click points in each image. The system will detect the mouse position on the image . The next step is to create profile vector. This is then compared with the profile vectors in the database. If it matches then the login is granted. If it does not matches the login is discarded .Here we can upload and download files.[3]Hotspots that is areas of the image that users are more likely to select are a concern in click-based passwords ,so CCP uses a large set of images that will be difficult for attackers to obtain. For our system, hotspot analysis requires proportionally more effort by attackers, as each image must be collected and analyzed individually.

CCP appears to allow greater security than Pass Points ,because the workload for attackers of CCP can be arbitrarily increased by augmenting the number of images in the system. As with most graphical passwords, CCP is not intended for environments where shoulder-surfing is a serious threat.

III.EXISTING SYSTEM

The existing system for authentication are character password, passpoints, passfaces and biometric authenticationn.The commonly used authentication technique is character password.In this sequence of characters is used as password.The password should be created by the user.The main problem with this is lack of security.The character password is very easy to break.So inorder to make a strong character password we have to add symbols,numbers, and other special characters.Length of character is also a great concern.The another type of authentication is graphical password aauthentication which uses images instead of characters.There are several type of graphical password authentication schemas.Passpoint is such a scheme in which user have to click on several points within a image during login process.In passfaces,we have to click on faces of people within a image.If all the clicks are right then we can login successfully.The another category of authentication is biometric authentication which uses iris,fingerprint for login.

IV.PROPOSED SYSTEM

The proposed system is “Graphical password authentication using cued click points” which is a combination of passfaces and passpoints.In this system during registration process user has to select the number of images the user needs and a particular points in each images.This is then stored in the database.When a user want to login he has to click on this points on these images.

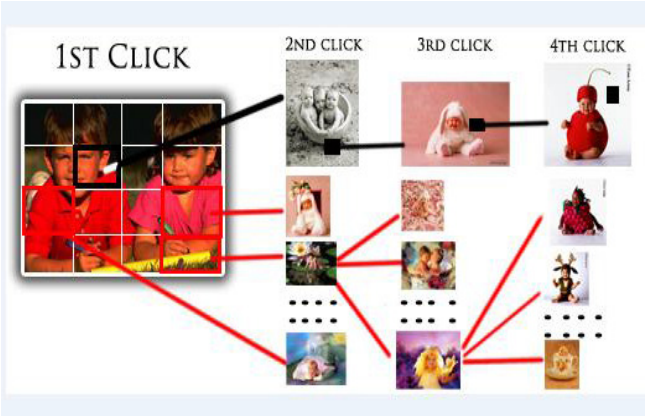

Fig1:Cued click points

As shown in the above fig,when a user click on a particular point on the image which he has choosen during registration process,the next image will be displayed and like we have to click on points on images which we have selected for authentication process.This technique provides more security and it is hard for the hackers to attack.Because when an hacker click on wrong point on the image a different image will be displayed to him.Therefore he has to click on those wrong images and atlast only he can understand that it was wrong.

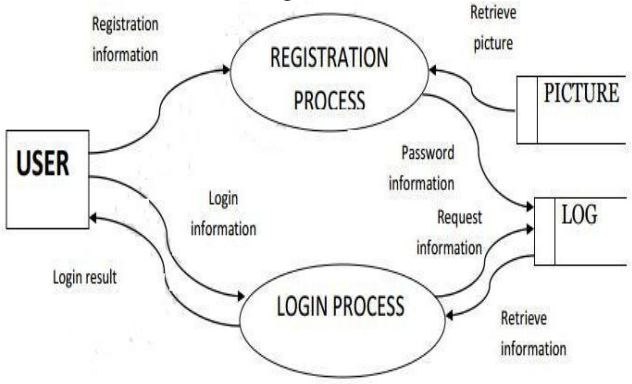

Fig 2:Dataflow diagram

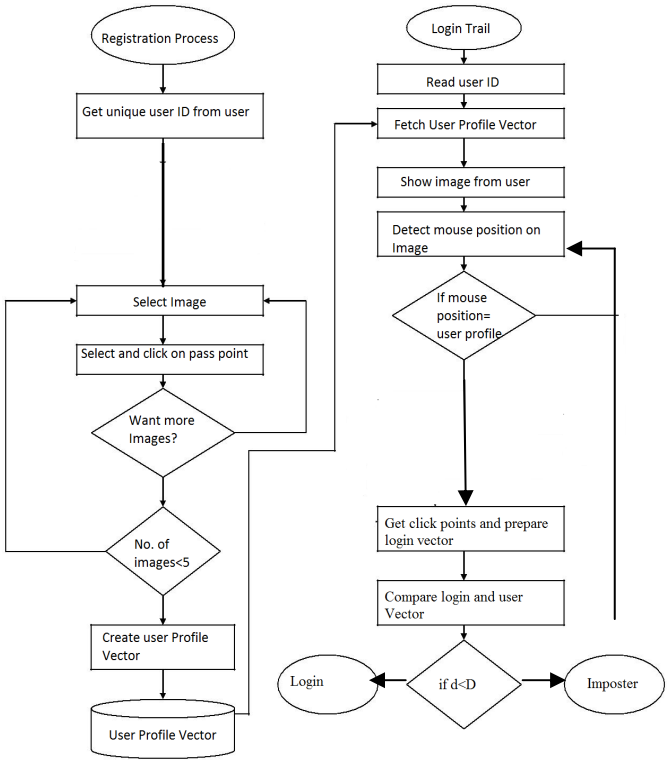

Fig:Working of CCP

V.HARDWARE AND SOFTWARE REQUIREMENTS

Processor	**Intel core 2 Duo**
Harddisk	80 GB
RAM	512 MB
Monitor	LCD Color
Operating system	Windows XP
Language	ASP.NET with c#
Database	Sql server 2005
Execution tool	Microsoft visual studio

Table1:Hardware and Software requirements

VI.CONCLUSION AND FUTURE WORK

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 Pass Points 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 offers a more secure alternative to Pass Points. 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.

ACKNOWLEDGMENT

We take this opportunity to express our gratitude and thank to our Head of our Department Ms. Divya M Menon who have helped us a lot in the successful completion of initial phase of our project. We extend our gratitude and sincere thanks our project coordinator Ms. Sabna AB who has always given her valuable time for us and also for her moral support. We remember the invaluable support offered by Mr Bineesh M, our project guide and for his good suggestions and constant encouragement.

REFERENCES

[1] Sonia Chiasson , P.C van Oorshcot, and Robert " Graphical Password Authentication Using Cued Click Points " © Springer-Verlag Heidelberg 2007,ESORICS 2007, LNCS 4734

[2] Tzong-Sun Wu · Ming-Lun Lee · Han-Yu Lin Chao-Yuan Wang "Shoulder-surfing-proof graphical password authentication scheme"© Springer-Verlag Berlin Heidelberg 2013

[3] John Charles Gyorffy , Andrew F. Tappenden ,James Miller "Token-based graphical password authentication "Published online: 2 October 2011 © Springer-Verlag 2011

