International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

A Novel Customized Persuasive Cued Click-Point Password Authentication

N. Akhila[1], A. Sri Sudha[2]
[1]*Asst. Prof, Dept. of CSE, Aditya Engineering College, Surampalem*
[2]*Assistant Marketing Manager, Reportstack, Pune*

Abstract: ***Most of the authentication methods use alphanumeric characters and passwords. This type of method has several drawbacks as textual passwords are easy to guess and the password that is hard to guess will be difficult to remember. To avoid this Customized Persuasive Cued Click Point (CPCCP) based image authentication method is introduced where user selects two images which are scrambled from sixty five set of images to prevent unauthorized access from an intruder.***
Keywords: Graphical passwords, Password guessing attacks, CPCCP

I. INTRODUCTION

Authentication is the process which verifies the identity of a User who wishes to access a particular system or resource and most of the textual passwords are vulnerable to attacks. The passwords should be very much complex to prevent the attacks like brute force. But if the password is hard it becomes difficult to remember passwords over time. In order to remember password easily, a graphical password authentication is used where passwords are easy to remember and hard to guess by hacker [2]. This paper brings forward the concept of customized persuasive cued click point authentication with the technique of scrambling images by generating session password from user id.

II. RELATED WORK

Graphical password systems belong to the category of information related legalizations Such as

A. Cued Click-Based Graphical Passwords

In CCP, Rather than clicking five different points on a single image, Cued Click Point introduces single click over each five different images. The user needs to choose few regions to record their highly secured password. The major problem encountered regarding the concept of graphical password is Mouse logger.

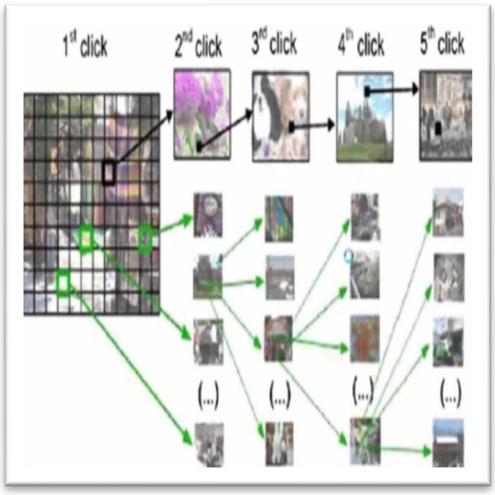

Fig 1:-Cued Click Point

B. Persuasive Cued Click-Points

When users generate a password in PCCP, the images will be little bit shaded except for the randomly chosen small block from the set of images given which is nothing but viewport as shown in Figure 2. Users need to pick out a click point from that small block. Users can make use of shuffle button to rearrange the viewport, if they are incapable to select a point from given viewport [3]. The

view port guides users to select more random passwords that are less likely to include hotspots. PCCP is very much time consuming process since the user who already destined for particular click-point may have the option to shuffle again till that viewport get relocated. The images will be shown normally with no concept of either shading or viewport thereby the users can select any point over the existing images during password entry.

Fig 2: Persuasive Cued Click point

By mistake if the user viewing the next image has selected the wrong position, then the attackers can easily guess the hotspot.

C. Modified PCCP

In the modified version of PCCP, set of images will get displayed to the individual depending upon their name calculation. Then the user side and server-side images will be integrated to have complete password. These types of passwords are easy to guess as they are on 9 sets which contain 10 images in each set. So, intruder can easily obtain password using brute force attack

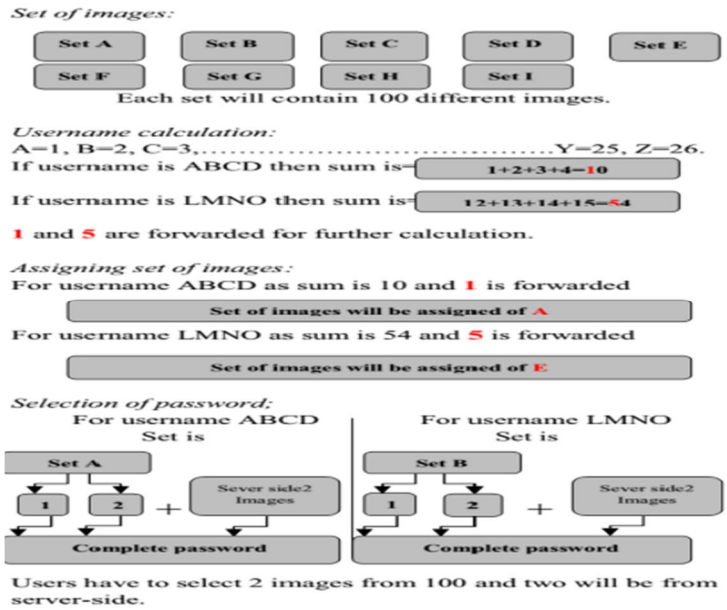

Fig 3: Flow of System

III. PROPOSED SYSTEM

In MCCP User has to give username to system for system validation. Suppose if the username is RINKY provided then according to the position of alphabet, username calculation is done successfully. If the sum of RINKY is 77, then system consider left side first digit. Now 7 is forwarded and set of images from set G is assigned to given username as shown in figure 3. The User should have to

select two images from set G and separate click point for every image and a set of image server side images selected by the system. Finally set of image selected by user and server side set of an image gives complete password. The main drawback of MCCP is even though username calculations is done one of the 9 sets (A-I) are used [1]. Summation of alphabets numbers doesn't resist to brute force attack as sets are chosen using first digit of user calculation so there are only 9 possibilities. It becomes easy for the hacker to choose two of the images from nine sets without username calculations. To avoid this drawback a Customized Persuasive Cued Click Point based image authentication method is introduced which contain 65 sets based on username calculation first two digits are forwarded and puzzles of two images from 65 set is chosen and before selecting two images from sets two images should be scrambled by user and server side set gives complete password. As the image is scrambled it becomes hard for the attackers to guess password from CPCCP.CPCCP authentication method is as follows

A. Let L be the set of 65 characters used for user id={A,B,C…Z,a,b,c.....z,0,1,2,3....9,@,_,.}
P is set of position on characters in L as,
P = {1, 2, 3 …….. 65}

B. Then sum of character position values is done with function f(x) as $f(x) = \sum_{n=1}^{len} p_n$

Such that n is the index representing the character in L and P_n is associative position in P.
Sum=f(x) will do the calculation from username.

if f(x)>=65 then $f(x)= \sum_{n=1}^{len} p_n \% 65$

C. Allotting Set of Image

I = {I_1, I_2, I_3 …….I_{65}} set of images such that each Ii is fixed set of images as given below
Ic= {i_1, i_2…i_{10}} where i_1 is one image from set I_i.

D. Selection of Password

I_1 and I_2 will be two scrambled images selected from given set I_c
I_3 and i_4 are two images from server side image set I_s
Above 4 images will act as password, Pw for user (Ui) Pair (Pw, Ui) will be stored for each user.

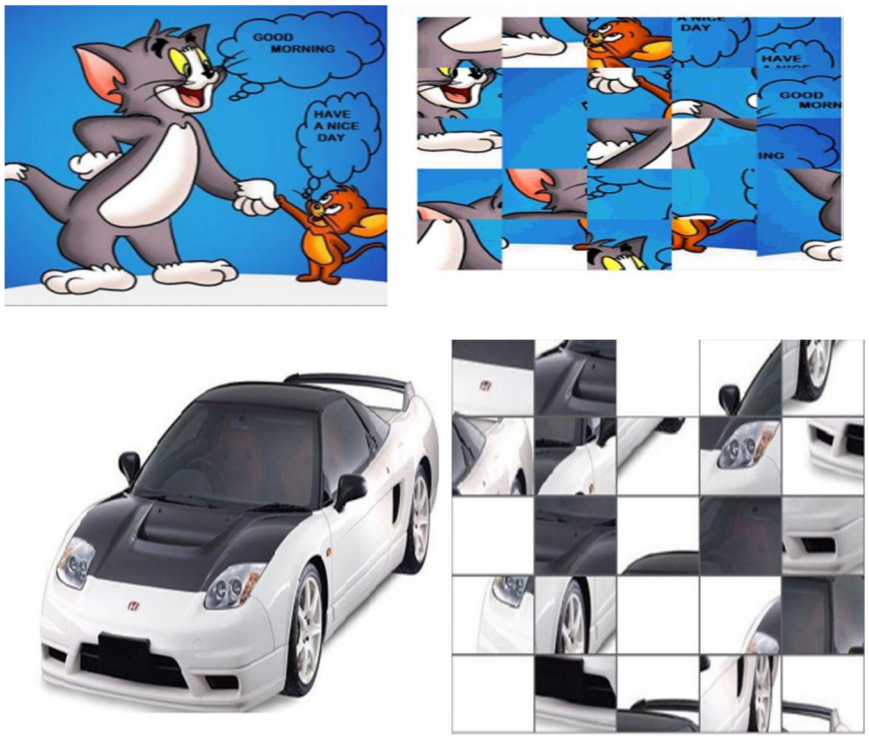

Fig 4: Two scrambled images from a set

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

IV. CONCLUSION

The suggested graphical lock scheme mainly decreases the risk of identifying the Individual passwords from several attacks, thereby providing the high security. This procedure gives so much of pressure for the attackers in acquiring text password and then image sets from the user calculations. So images as a secret word is the enhanced alternate for securing the assets and there also the better algorithm that are required for making access more secured.

REFERENCES

[1] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text" Journal of Computers, vol.5, no.5 May 2010.
[2] P. P. Ray, "Rays scheme: Graphical password based hybrid authentication system for smart hand held device," Journal of Information Engineering and Application, vol. 2, no. 2, 2012.
[3] M Sreelatha, M Shashi, M Anirudh, MD SultanAhamed,V Manoj Kumar Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security & Its Applications (IJNSA), Vol.3,No.3, May201
[4] Sonkar S.K., Paikrao R.L., Awadesh Kumar "Graphical Password Authentication Scheme Based On Color ImageGallery" (IJEIT) Volume 2, Issue 4, October 2012-13.