ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (67-72), Month: October 2014 – March 2015, Available at: www.paperpublications.org

Graphical Password Authentication Using Modified Persuasive Cued Click-Point

[1]Mohite Sandhya, [2]Kare Rohini, [3]Bhongale Pooja, [4]Bhosale Priyanka,
[5] Prof. Parchure S.V.

[1]Department of Computer Engineering, SBPCOE, Indapur (Pune), India
[2]Professor, Department of Computer Engineering, SBPCOE, Indapur (Pune), India

Abstract: **There are many authentication systems which are used for computer based authentication purpose. Generally user have put username and password in alphanumeric form. But alphanumeric password which is easy for remember can be guess by any hacker/attacker. But strong password given by user which is hard to remember sometime. This paper introduces modified persuasive cued click point authentication system. In persuasive cued click point authentication system, due to viewport chances of hotspot creation is increased. Due to elimination of viewport, hotspot creation is reduced in the modified PCCP, which gives more security to system.**

Keywords: **Cued Click Points, Graphical Password, Modified PCCP, Server side images, and security.**

I. INTRODUCTION

For authentication purpose we generally use text passwords but text password can be easily hacked by hacker. If we give strong password is sometime hard to remember. If we want to avoid this, the system assigned password is very hard to remember to user. So the graphical password authentication gives images and its click-points for strong authentication. This gives strong security to our system. This paper gives information about modified PCCP authentication technique. In PCCP technique viewport is used and users have to enter click-point in viewport which is given by system at the time of login.

II. LITERATURE SURVEY

For security purpose user generally prefer text password which is combination of characters, numbers, etc. If any user gives text password which is easy to remember but there is great chances of breaking password for attackers but human brain can easily understand and remember pictures than text. Graphical password authentication provide click points for every image. So, it is difficult for attacker to guess password that is image and its correct click- points on them. Authentication methods can be divided into following:

1. Token Based Authentication
2. Biometric Based Authentication
3. Knowledge Based Authentication

1. Token Based Authentication

In this technique cards are generally used for authentication purpose. Smart cards, ATM cards, credit cards, key cards, etc. are used.

2. Biometric Based Authentication

In Biometric authentication technique for security purpose fingerprints, facial expressions are used as password. Sometimes voice is also used for security purpose. This provide strong security to system but it requires highly expensive devices.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (67-72), Month: October 2014 – March 2015, Available at: www.paperpublications.org

3. Knowledge Based Authentication

Concept of authentication using graphical/picture password proposed by the Greg Blonder in 1995[2]. Knowledge based authentication have three types given below:

I. Recognition Based Technique

II. Recall Based Technique

III. Cued Recall Based Technique

I. Recognition Based Technique

In this technique user have to select set of images at the time of registration. Same set of images should be selected by user at the time of login [3].

Fig.1 Recognition based technique

II. Recall Based Technique

In this technique user have to draw any shape like circle, square, etc. and at the time of registration user have to draw pattern and at login time same pattern drawn by user[3]. For pattern drawing 2D grid is used.

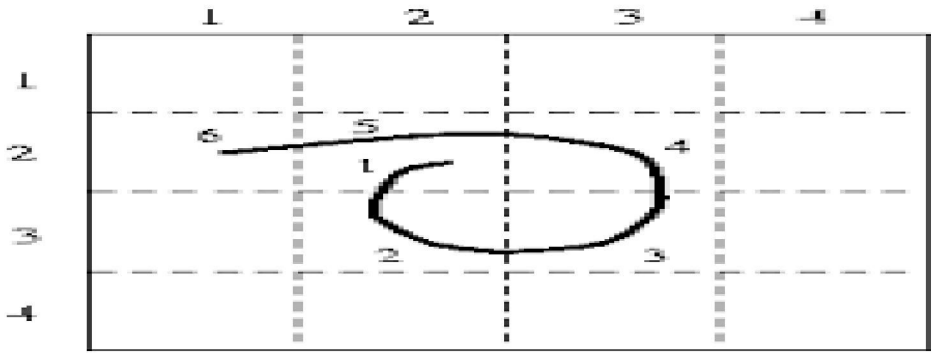

Fig.2 Recall based technique

III. Cued Recall Based Technique

Cued Recall based technique further divided into three parts:

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (67-72), Month: October 2014 – March 2015, Available at: www.paperpublications.org

A] Pass Point

B] Cued Click Point

C] Persuasive Cued Click point

D] Modified Persuasive Cued Click Point

A] Pass Point-

In Pass Point Technique user has to select sequence of click points on a single image, Discretization square is used for authentication. In pass point method as we are using only one mage and click point should be selected on a single image so the tolerance area generated will be maximum[1], so attacker can attack/hack the system by choosing click points on image randomly.

Fig.3 Pass Point technique

B] Cued click Point-

By selecting all click point on single image introduces hotspots creation. In CCP user have to select different five images instead of selecting click point on same image. For every image user have to select only one click point[4]. When user click on a correct position on image, then next image will displayed. In CCP address of next image is stored in previous click point. If click point is wrong then wrong image will be displayed. Users have to select sequence of click-point on correct images.

C] Persuasive Cued Click Point-

Fogg invented the Persuasive technique of authentication [5]. In PCCP, when user select image then automatically block will be selected called viewport. Viewport can be selected by system and user have to select position of click point within viewport. Viewport can be moved anywhere on image by shuffle button. At the time of password creation shuffle button will be displayed [6].

III. PROPOSED SYSTEM

In modified PCCP we have to remove concept of viewport .In PCCP viewport can be displayed on image and user have to click in the viewport. So, due to automatic display of viewport on image in PCCP, any attacker can get idea and by randomly selecting position of click-point attacker can attack the system easily. But in modified PCCP viewport is removed, so system cannot display viewport and hacker cannot get idea about where to click on image exactly and due to elimination of viewport hotspot creation is minimize and so the chances of hacking is minimized. In modified PCCP, we can choose any number of images at the time of registration, so for storing images more memory is not required. In modified PCCP, user have to select his/her choice of images and for these selected images system provide server side images which gives strong authentication to system. Set of images will assigned to user on the basis of username calculation and finally for complete password user side images and server side images are combined.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (67-72), Month: October 2014 – March 2015, Available at: www.paperpublications.org

IV. ALGORITHM

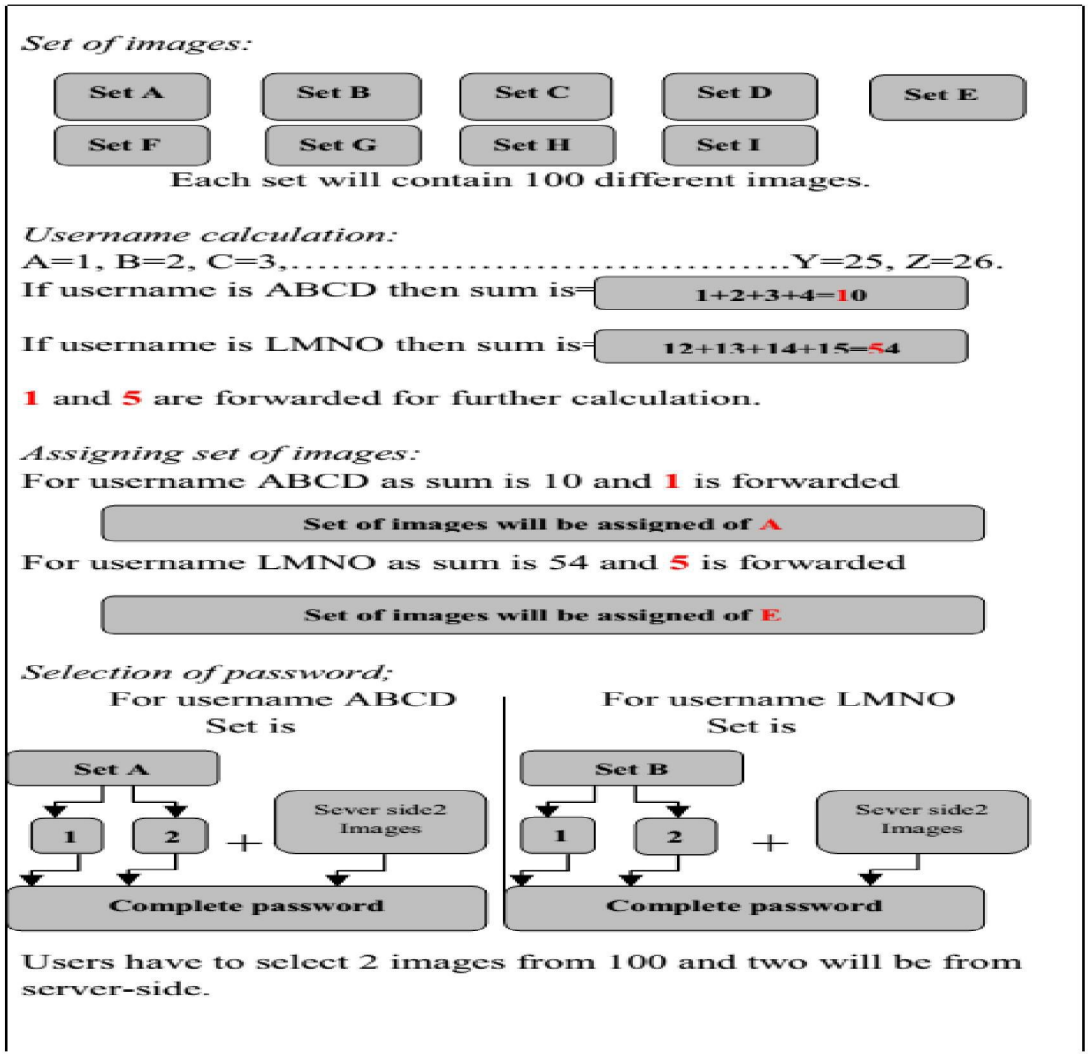

Fig.4 Flow of system

Modified PCCP provides better security due to server side images provided by system. steps of password generation-

Step I: User has to provide it's username to system for system authentication.

Step II: From fig.4, suppose ABCD username is provided then according to position of alphabet, username calculation is done successfully. If sum of ABCD is 10, then system consider left side first digit.

Step III: Now 1 is forwarded and set of images from set A is assigned to given username.

Step IV: User should have to select two images from set A and separate click point for every image. For this set of image server side images selected by system.

Step V: Finally set of image selected by user and server side set of image gives complete password.

V. MATHEMATICAL MODEL

1] Representation in the set format-

Let S be set represents various parameters such as input(I), output(O),function(F) and failure case(FC).

S= {(I), (O), (F), (FC)}

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (67-72), Month: October 2014 – March 2015, Available at: www.paperpublications.org

Input (I)-

I is the subset of set S which represent input given by the user.

Input contains set of images within that images click-points are passed as input.

I = {Username, image 1, image 2,……image n}

Output (O) -

O is the subset of set S which represent authentication is successfully.

If set of click-points of images are correct then it display login successfully.

O = {authentication successful, login successful}

Function (F)-

Set the click point of images.

F= {Function}

Failure Case (FC)-

If sequence of click points of images is not correct.

2] Calculation for username -

Let L be the set of all capital letters A to Z.

L = {A, B ,C……..Z}

P is set of position on letter in L as,

P = {1, 2, 3 …… 26}

<L× *P*=def {< l, p >: l ϵ L ,p ϵ P }>

u is username such that

{u : u is a word which can be described as English words build up of combination of letters in set L}

Let u has length 'len'

Then sum of position values is done with function f(x) as

$$f(x) = \sum_{n=1}^{len}(Pn)$$

Such that 'n' is the index representing the letter in L and Pn is associative position in P.

Sum=f(x) will do the calculation from username.

D1 represent the first digit of sum and always will be from 1 to 9.

3] Assigning set of image-

I = {I1, I2 …….I9} set of images such that each Ii is fixed set of images as given below

Ii ={i1, i2,……..in}where i1 is one image from set Ii.

4] Selection of password-

i1 and i2 will be two images selected from given set Ii

i3 and i4 are two images from server side image set Is

Above 4 images from a password Pw for user Ui

Pair (Pw, Ui) will be stored for each user.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 1, Issue 2, pp: (67-72), Month: October 2014 – March 2015, Available at: www.paperpublications.org

VI. CONCLUSION

Security is most important factor for any system authentication. Firstly pass point method is proposed but due to all click point on the same image minimize the security of system. In CCP technique more images with separate click point on it is used. But problem of hotspot creation is not solved. So to eliminate that PCCP mechanism is developed which does not provide security due to viewport on image. Modified PCCP is the improvement of PCCP technique, which eliminate the displaying of viewport on image at the time of login and for attacker it is difficult to guess correct click point on image. So modified PCCP gives better security than PCCP.

REFERENCES

[1] S. Chiasson, R. Biddle, and P. van Oorschot, "A second look at the usability of click-based graphical password, "in ACM Symposium on Usable Privacy and Security (SOUPS),July 2007

[2] P. P. Ray, "Ray's scheme: Graphical password based hybrid authentication system for smart hand held device," Journal of Information Engineering and Application, vol. 2, no. 2, 2012.

[3] X. Suo, Y. Z. G. and S. Owen, "Graphical passwords: A survey."

[4] A Aswathy Nair, Theresa Rani Joseph, Jenny Maria Johny, "A Proficient Multilevel Graphical Authentication System," International Journal of Science, Engineering and Technology Research (IJSETR), Volume 2, No 6, June 2013.

[5] B. Fogg,Persuasive Technologies: Using Computers to Change What We Think and Do.Morgan Kaufmann Publishers, 2003.

[6] Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme P. R. Devale Shrikala M. Deshmukh, Anil B. Pawar.