Image and Sound Based Authentication of User

Badgude Puja, Ghorpade Hemlata, Ghadge Yogita, More Supriya

Abstract - An image and sound based authentication of a user,it means we will authenticate the users of a system by a password that they entered through a sequence of images. And also having some special sound effects associated with a password.

In the previous days, Pass Point was the technique,used to give image based password.But it requires five clicks on one image.This will take more memory to store the clicks and become easy for attacker to guess.

To overcome that drawback CCP technique was developed which takes a sequence of five images and one click on each image. In addition, a user has to select sound signature with respective each click on image to easily recall the password.

After addition a persuasive feature to CCP, we will get PCCP,which was used to address an issue of hotspots.While creating an image based password a complete image is dimmed except viewport area.A user has to click within this viewport.This viewport area can be repositioned randomly by using shuffle button.

In the proposed work, we aimed to build more interactive, user-friendly and secure email system by creating strong and difficult password to guess by attacker.

Keywords: CCP and PCCP technique, system architecture, working of proposed system.

I. INTRODUCTION

Most of the time the users refer the password for their convenience. As the users set the password which are easier to remember them. But such passwords may lead to insecure passwords, they can be easily guessed by an attacker.

To overcome such disadvantage we have developed graphical password system which can be operate with a sound signature. Psychologist said that a human brain is very strong & sharp to remember visual things very fast. Our proposed work is exactly used to capture the human brain's ability.

II.EXISTING SYSTEM

In the existing system, previously a technique is used to enter click points on image which is called as PassPoint (PP) technique. Pass Point technique allows a user to enter maximum twelve click points on each image [3]. But more click points on an image consumes more memory. The huge disadvantage of this technique is a careful observation of an attacker that is shoulder surfing attack cannot be overcome and user cannot easily recall more click points.

To overcome these drawbacks,a technique called Cued Click Point(CCP) is used. It allows user to enter one click point on each image and like this it allows sequence of five images to set as a password [3]. A CCP technique is used only at the login time. While login into system if a user clicks on wrong click point it leads a user to incorrect path.

Manuscript Received on March, 2014.

Badgude Puja, Student of COMP/IT (Dept.) S.P.C.O.E.,Otur, India.

Ghorpade Hemlata, Student of COMP/IT (Dept.) S.P.C.O.E.,Otur, India.

Ghadge Yogita, Student of COMP/IT (Dept.) S.P.C.O.E.,Otur, India.

More Supriya, Student of COMP/IT (Dept.) S.P.C.O.E.,Otur, India.

It means if an attacker tries to login into an email account of a user and if he misplaced a one click point then the sequence of images set as a password are changed and on the place of correct sequence images random images will be displayed. This change in sequence is recognized only by authorized user not by an attacker and finally system gives a result as failed login attempt.

Before a user has to make a registration for his/her email account. For registration purpose a technology named as Persuasive Cued Click Point(PCCP) is used. In PCCP [3] a user is allowed to choose a set of images(that is 5) to set as a password for an email account. While creating an image based password except a viewport area complete image is dimmed[3].The images that a user chose for password may be downloaded from web, may be from system itself and one image space is reserved for user that means a user can give any image by his own(for example-a paint image, his own photo image). A system provides memory space for total 50 images and all these images are stored in one directory out of that 49 images are from system and one image block is reserved for user itself.

In PCCP technique a user make a click point on one image that allows him/her to navigate on next image. A click point which provides a link to next image is called as a hotspot and the area which covers that hotspot is called as a viewport area. If a user wishes to change viewport location then he/she can does this by clicking on shuffle button [3]. A shuffle button randomly reposition a viewport area on an image [2].

III.PROPOSED SYSTEM

Before this no system has been developed which uses graphical password with integrated sound signature for authentication purpose. Sound signature is used to recall the objects in the image. A proposed work includes two vectors for creating user's profile vector; those are Master vector[1].

Master vector- (User ID, Sound frequency, Tolerance area _value).

Detailed vector-(Images, Click points).

Master vector - (Harsh,4738,70)

Detailed vector-

Images	Click points
I1	(120,122)
I2	(137,148)
I3	(450,350)
I4	(200,450)
I5	(375,300)

Master vector &detailed vector is required at the time of registration [1].

IV.SYSTEM ARCHITECTURE

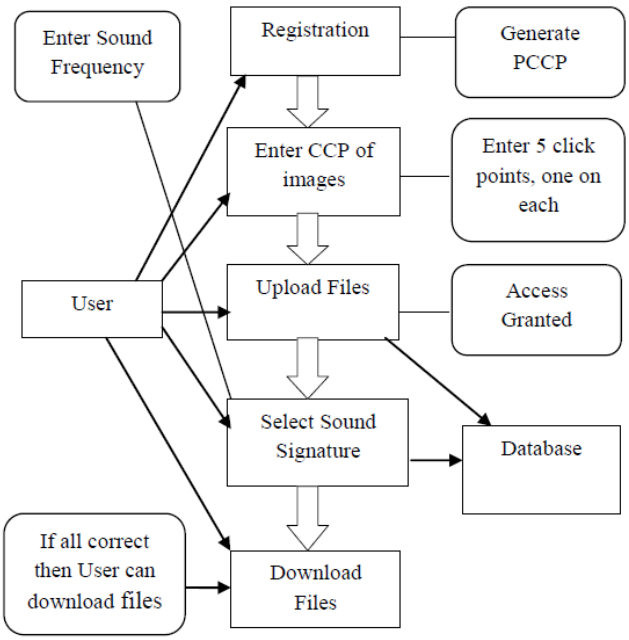

Fig: System Architecture

The system architecture tells us that the user requires to do his/her registration for creating an email account in a system. He can do his registration in a formal manner as he does for email accounts like Gmail. A user can set a text password also. But for more security we also provide large password i.e. in the form of sequence of images.

A user chooses some set of images from a system and also he has to select viewport on each image as a link for moving forward on next image through PCCP technique [3].

User has to select minimum 5 images for password and one click on each image. After selecting the images user has to select a particular sound frequency that he wants to be played at the time of login [1]. And all this information (i.e. user id, sound signature frequency, tolerance area value of image & information about images along with their click points as a password) is stored in the database which will create a particular profile vector for a particular user [1].

At the time of login when user enters his user id & clicks on each image, is compared in the database & if each click is correct then correct sound file will be played otherwise for wrong click a random sound is played. If a legitimate user click on a wrong point/out of viewport area, random sound will played that will be recognized by legitimate user but if the unauthorized user tries to hack a password, he will not recognize that the password is correct or not until he clicks on last image. If a user goes through a correct path for logging into an email system, he/she can successfully logins into the system.

V.MATHEMATICAL MODEL

To achieve security & usability mechanism our system uses center discretization. Center tolerance are used to reduce the size of grid square (that means 2r * 2r instead of 6r * 6r) & also increased password search space [4].

For single click point , we calculate a offset d of discretized point (0<=d< 2r) & it's corresponding segment identifier i (i>= -1) which is stored in protected form as it hash value *h(i,d).*The segment identifier is calculated by *i=[(x-r)/2r],* that's means identifying segment that consist of real number that is *x* [4].

The distance between origin & left boundary of segment 0 determined by calculating the offset d= [(x-r) mod 2r][4].

At the time of verifying re-entered click point x' is acceptable. Then calculate which segment consist of x' using same offset as origin point based on x' which is pre-determined System computes i'=[(x-d)/2r] [4].

If x' is within the tolerance r of x, then it gives the entry after verifying i'= i & h(i',d) which is equals to stored value h(i ,d).

If x' is outside the tolerance r of x, then it reject the entry after verifying i'!= i & h(i',d) which is not equals to stored value h(i ,d).

Example:

Consider $x= 23 \& r =5$, then we compute ,

$i = [(x-r)/2r] = [(23-5)/10] = 1$,

$d = [(x -r) \bmod 2r] = [(23-5) \bmod 10] = 8$, Offset

$d= 8$ is stored along with protected

$h(i, d) = h(1,8)$.

If a user enters $x' = 24$ during login, then system calculates

$i' = [(x' - d)/2r] = [(24-8)/10] = 1$

It then compares $h(i', d)$ and $h(i ,d)$& if match found then accepted [4].

When password consists of more than one click point, all segment indices and their offsets are concatenated and hashed together as one.

VI.CONCLUSION

In this paper, we have passed a sound file with a graphical password that will be played at login time. We have used two cued recall techniques in that one is CCP and the other is PCCP. A CCP technique makes user easily recall the click points and requires less time and also produce an accurate result. Playing a sound file at the login time makes a system more interactive. A sound file simply plays a role of hint. But this hint will not make an email account of a user insecure. A user can play any sound it can be a name of an object on which user clicks or any other object name to secure the email account from social engineering attacks.

REFERENCES

1. S.Singh, G.Agrawal "Integration of sound signature in graphical password authentication system" Invertis University Bareilly,India, January 2011.
2. S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, "Persuasive cued click-points: Design, implementation and evaluation of a knowledge-based authentication mechanism," School of Computer Science, Carleton University ,Tech. Rep. TR-11-03, February 2011.
3. Chippy.T, R.Nagendran "Defence Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points" International Journal of Communications and Engineering Volume-3, 01 March 2012.
4. S.Chiasson,JaykumarSrinivasan, Robert Bibble, P.C. van Oorschot "Centered Discretization with Application to Graphical Passwords" Ottawa,Canada Carleton University.