Graphical Password Authentication System with Supportive Echo

Gopika Mane[1], Sayali Gadhave[2], Neha Mali[3], Monali Jadhav[4], Suvarna Choudhari[5]
Department of Computer Engineering,
Marathwada MitraMandal's Institute of Technology,
Lohgaon, Pune-47.

***Abstract*— In Computer Industry, Security is maintained through passwords. A Password is secret word or phrase that gives a user access to a particular program or system. This paper presents Graphical Password system with supportive echo. In proposed work a click-based graphical password scheme called Cued Click Point (CCP) is presented. In this system a password consist of series of some images in which user can select one click-point per image. Supportive Echo is provided for recalling click point on the image.**

I. INTRODUCTION

Passwords are mandatory for Authentication and Authorization. Authentication means the process used to ensure that user is who they say they are. Authorization is process used to ensure that only authenticated user has right to access and modify data.

On the whole user select text-based password which is easy to remember and easy for attacker to guess. Text based password suffers with both usability and security problems. According to recent reports article, a security team at a company ran a network password cracker and within 30 seconds they identified about 80% of the password. To offer more security we use graphical password [1] using Cued Click Point(CCP).In CCP, we select only one point per image as a password. We also provide echo for recalling intention.

A. Graphical Password Technique:

There are two main techniques for graphical password

1. Recognition-based:–A user is presented with set of images and passes the authentication by recognizing and identifying the images. User selected during registration stage.
2. Recall-based:-A user is asked to reproduce somethingthat user created or selected during the registrationstage.

B. Graphical Password for better security:

A Graphical Password is Authentication System that works by having the user selects from images in specific order presented in Graphical User Interface (GUI).Graphical Passwords are easier than text-based password for human being to remember. Instead of entering a password consisting of number of letters and digits the user can selects area of picture called "click point"[1] which are easier for user to remember and due to the somewhat random selection method, more tricky for someone else to guess. Graphical Passwords may offer better security than text-based password. Dictionary search can allow hacker to gain entry into system into seconds, but if series of images are selected hacker must try each possible grouping at random. Suppose there are 100 images on each of the 8 pages in an 8 image password there is 1008 possible combination that could form Graphical Password.If system has built in delay of only 0.1sec following the selection of each image until the presentation of the next image. It would take millions of years to break into system by hitting it with random image sequences.

II. LITERATURE STUDY

A. Hotspot Problem:

Hotspot[2] means region of image that users are most likely to select. In this only one image and particular area on that image is select as password so that password can easily guess because password search space is restricted

B. GPI:

After hotspot problem the evaluation of new graphical password scheme i.e. GPI (Graphical Password Icon) which have a potential to overcome hotspot problem while keeping the system usable. These schemes are icon as the clicking points on the graphical password interface and provide. A password space equivalent to earlier system. In GPI to mitigate the hotspot problems user may click on subset of displayed icon as their password instead of selecting exact location on background image.

C. Pass point:

Previously Graphical Passwords were generated using pass point[2] technique in which numbers on clicks on one image is set to as password but disadvantage of using this system is that remembering more than one click on one image is difficult to user.

D. Robust Discretization:

Robust Discretization[4] technique of Discretization of click points so that approximately correct entries are received For selecting fairly accurate position of click point.In this method image is divided into grid square of size 6r*6r ,but in this system grid size is greater so password search space is low for attacker.let r=2 then grid square size becomes 12*12.

III. PROPOSED WORK

A. *Cued Click Point:*

In CCP[3], passwords consist of one click point per image for sequence of image. The next image displayed is totally based on previous click point. so user accept immediate implicit feedback whether they are follow correct path or not. When logging using CCP offers both improve usability and security. As shown in following figure 1, user clicks one point on each image. It offers cued recall and introduced visual cues that instantly alert valid users if they have made mistake when entering their latest click points means if click point is incorrect then next image will be open which not a valid image, so only authenticated user knows that previous click point is wrong. In this case user immediately cancels their login attempt and tries from beginning. In addition we can assign unique name for each click point and we are converting this name into sound signature by using SAPI technique which is helpful for login.

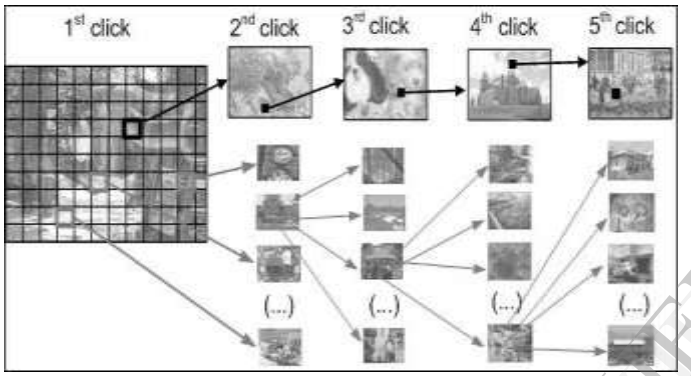

Figure 1. Cued Click Point

B. *Centered Discretization:*

Centered Discretization[4] is algorithm used to find approximate position of click points. It offers usability and security improvements. It offers Centered tolerance, which increase security because the size of grid square can be reduced (to 2r*2r instead of 6r*6r) thereby increasing password search space. If r=2 where r is tolerance level then size of grid can become 4*4.

Let us assume that 1-D Password Consist of single click point x, then,Image is divided into grid square according to tolerance level r given by user with size of grid square is 2r*2r.To store this password x we must discretize the point by calculating its offset d where offset must inside $0 < d < 2r$,also find corresponding segment identifier i where $i > -1$.Offset d is stored obvious and i is stored in protected form in hash value h(i,d).Segment identifier i is calculated using $i= (x-r)/2$ and d is calculated using $d=(x-r) \bmod 2r$.To verify re-entered click point say x',to be acceptable the system calculates $i'=(x'-d)/2r$.If x' is within tolerance r of x, then $i' = i$ and hence if h(i',d) equals the stored value of h(i,d) and system accepts the entry.

IV. SYSTEM ARCHITECTURE

1. Registration (user information)
2. Select images and click point
3. Final Registration (step 1+step 2)
4. Login
5. Detect Mouse Position

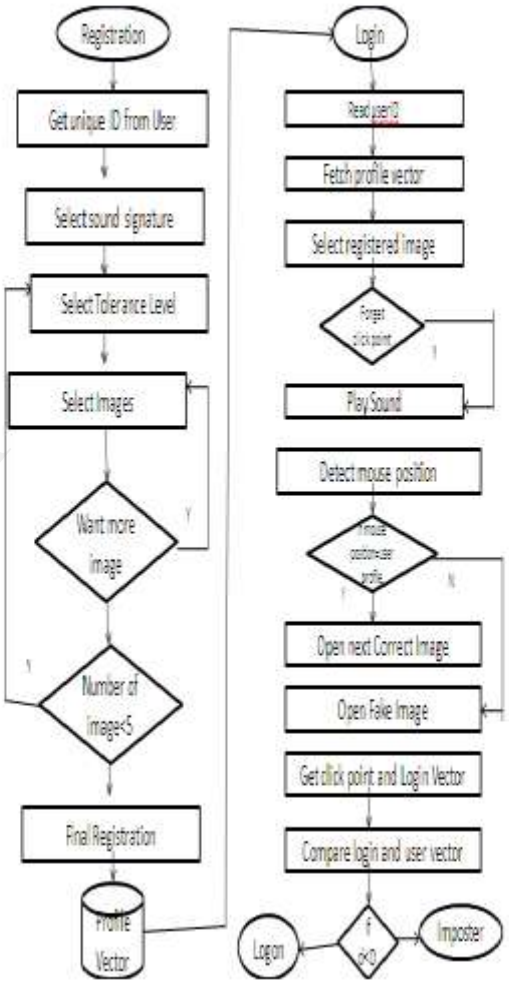

Figure 2.Graphical Password System Architecture

MICROSOFT SAPI

The Speech Application Programming Interface is an API developed by Microsoft to allow the use of speech recognition and speech synthesis within windows application. We are using SAPI technique to convert click point name to sound for more remembrance purpose. In general the Speech API is freely-redistributable component which can be shipped with any windows application that wishes to use speech technology.

6. CONCLUSION

The major advantage of CCP is its large password space over alphanumeric passwords. there is a growing interest for graphical passwords since they are better than text based password. We have proposed an approach which user sound signature to recall graphical password click points.

7. REFERENCES

[1]. Gaurav Agarwal, Saurabh Singh, "Integration Of Sound Signature In Graphical Password Authentication System," Volume 8. INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS,2011.

[2]. Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, Hakan Gurbaslar, Burak Erdeniz, "Towards Usable Solutions To Graphical Password Hotspot Problem", IEEE INTERNATIONAL COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE,2009.

[3]. P.C. Van Oorschot, Sonia Chiasson And Robert Biddle, "Graphical Password Authentication Using Cued Click Points", SCHOOL OF COMPUTER SCIENCE, CARLETON UNIVERSITY, OTTAWA, CANADA, 2011.

[4]. S. Chiasson, "Centered Discretization With Application To Graphical Password," CARLETONUNIVERSITY OTTAWA, 2008.

[5]. Stobert, A. Forget, S. Chiasson, P. Van Oorschot, And R. Biddle, "Exploring Usability Effects Of Increasing Security In Click-Based Graphical Passwords," IN ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE (ACSAC),2010.