Password Scheme Using Graphical Cued Click Points and Sound Signatures

Jeyaprakash P¹, Chandraprabha K²

PG Student¹, Assistant Professor²
Department of Master of Computer Applications
Alagappa Chettiar College of Engineering and Technology, Karaikudi, Tamilnadu, India.

Abstract: *An empirical study of passfaces, which illustrates how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall and user clicks on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation, the user chooses several predefined regions in an image as their password. Proposed system uses cued click points (ccp wherin users click one point on each of 5 images rather than on five points on one image as in existing system and also a sound signature to help in recalling the password is integrated. It is called cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point. No system has been devolved so far which uses sound signature in graphical password authentication. Problem with this scheme is that the number of predefined regions is small, perhaps a few dozens in a picture. The password may have to be up to 12 clicks for adequate security, again tedious for the user. Another problem of this system is the need for the predefined regions to be readily identifiable.*

***Key Words*:** Password Authentication, Cued click points, sound signatures, Graphical password scheme.

1.INTRODUCTION

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. second, a picture worth a thousand passwords; some psychological studies and company software seem to agree with these assumptions.

2.EXISTING SYSTEM

In the existing system**,** Brostoff and sasse carried out an empirical study of passfaces, which illustrates well how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented

by Passlogix Corporation, the user chooses several predefined regions in an image as Their password. To log in the user has to click on the same regions in effect, cued click points (ccp) is a proposed alternative to pass points.

In ccp, users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in Effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image.

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 have been developed, Study shows that text-based passwords suffers with both security and usability problems.

2.1 DISADVANTAGES

1) Users click one point on each of 5 images rather than on five points on one image.
2) Usually leads to usability issues since users cannot easily remember such random passwords.

3.PROPOSED SYSTEM

In the proposed work, a sound signature to help in recalling the password is integrated. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life various examples of recalling an object by the sound related to that object enters User ID and select one sound

frequency which the User wants to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select of images and clicks on each image at click points of their choice. Profile vector is created.

3.1 ADVANTAGES

1. No system has been devolved so far which uses sound signature in graphical password authentication.
2. To create detailed vector user has to select sequence of images and clicks on each image at click points of their choice.

4. PROBLEM DEFINITION

In the existing system**,** Brostoff and sasse carried out an empirical study of passfaces, which illustrates how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation, the user chooses several predefined regions in an image as their password. To log in the user has to click on the same regions in effect, cued click points (ccp) is a proposed alternative to pass points.

1) Users click one point on each of 5 images rather than on five points on one image.
2) Usually leads to usability issues since users cannot easily remember such random passwords.

5.OVERVIEW

In the proposed work, a sound signature to help in recalling the password is integrated. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which the user wants to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter.

1) No system has been devolved so far which uses sound signature in graphical password authentication.
2) To create detailed vector user has to select sequence of images and clicks on each image at click points of their choice.

6. LIST OF MODULES

6.1 Create User Profile Vector (Master Vector)

While registration of user information, the user id, sound frequency or time and tolerance are getting for creating master vector. Users have to Feed their Unique Master Vector Information to Register into the Web Application. Those Information are to be Viewed by the Admin only. This Vector is the Master vector for the Registration.

Profile Vectors-

The proposed system creates user profile as follows- Master vector - (User ID, Sound Signature frequency, Tolerance)

Detailed Vector - (Image, Click Points)

As an example of vectors -

Master vector (Smith, 2689, 50)

Image	Click points
I 1	(123,678)
I 2	(176,134)
I 3	(450,297)
I 4	(761,164)

MASTER VECTOR

User ID (Login Name)

Login Name / User ID is the Data that is used for Logon to the User Profile. Login Name is Checked with the Existing Users Database and the Logon Lock images are Shown for further Logon Steps.

Email ID

The Email ID is the Data that is Used when the Logon Using the Email ID and send the Request to the Admin to Get the Locked Account Unlocked User Forgets the Click Point or the User Get Locked out of the Account.

Sound Signature frequency

Sound Signature is also the Lock for the User Account, which is a Video File that Plays During the Logon time. The User Have to Stop the Video during the Specific Predefined Period of time.

Tolerance

The tolerance value is the data that is used in the Lock images and Videos to Make the Clicks not to get too Difficult to Logon.

6.2 Create Detailed Vector (Login Vector)

To create detailed vector user has to select sequence of images and clicks on each image at click points of their choice. Then Detailed vector is created. Users have to Feed their Unique Login Vector Information (Image Locks) to Register into the Web Application. Those Information are to be used for Login Purpose.

This Vector is the Detailed vector for the Registration. The Lock images are selected During the Registration of the User. Those images are showed during the Logon time. The User Have to Click on the Same Click Points where they Clicked during the Registration. The Lock Images Are Shuffled and Viewed on the Logon Page. The order of the Image Changes Every time of Logon. The Click Points are the Key Points that are made by the User Mouse Clicks on the Lock Images During the Registration time.

Those Click Points Are Stored in the Database for future use (Login). At the time of Logon, the User is asked to Click on the image and on the same Click point where the user Clicked during the Registration (Stored on the Database).

DETAILED VECTOR

Image

The Lock images are selected During the Registration of the User. Those images are showed during the Logon time. The User Have to Click on the Same Click Points where they Clicked during the Registration. The Lock Images Are Shuffled and Viewed on the Logon Page. The order of the Image Changes Every time of Logon.

Click Points

The Click Points are the Key Points that are made by the User Mouse Clicks on the Lock Images During the Registration time. Those Click Points Are Stored in the Database for future use (Login). At the time of Logon, the User is asked to Click on the image and on the same Click point where the user Clicked during the Registration (Stored on the Database).

6.3 Compare User Profile/Login Vector

Enters User ID and select one sound frequency or time which the User wants to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image and sound signature helps considerably for login.

The Login Vector is the Only way to Logon to their Profile. At the time of Logon, the System Checks the Click Points (both the Click Points stored on the Database & the Current Click Points). If the Current Click Points (during Logon) Matches the Click Points Stored on the Database, the System Allows Logon the User to the Profile.

Sound Signature is the Video file that Plays during the time of Logon. The user has to Stop the video at a particular time when the user Stops during the time of Registration. When User stops the Video, the System checks the Time period with the Stored Predefined Time Period in the Database. If the Time Periods Matches the System Allows the user to Logon to the Profile. Otherwise the user is Blocked out of the Account.

LOGIN VECTOR

Image Click Points

At the time of Logon, the System Checks the Click Points (both the Click Points stored on the Database & the Current Click Points). If the Current Click Points (during Logon) Matches the Click Points Stored on the Database, the System Allows Logon the User to the Profile.

Sound Signature

Sound Signature is the Video file that Plays during the time of Logon. The user has to Stop the video at a particular time when the user Stops during the time of Registration. When User stops the Video, the System checks the Time period with the Stored Predefined Time Period in the Database. If the Time Periods Matches the System Allows the user to Logon to the Profile. Otherwise the user is Blocked out of the Account.

6.4. Upload/Download Module

Admin, defence, navy and air force are going to upload secret file between them. They can share the uploaded files. User (defence, air force and navy) uses sound signature for download files. Uploaded Files can be Removed by the Admin in case of Mistake Sending of Files. User Can Download the Files intended to them Unlimited Number of

times. System showed very good Performance in terms of speed, accuracy, and ease of use.

The Admin Uploads the Files (Secret Data) to the Users (defense, air force and navy) from the Admins Page and the User Downloads those files that uploaded by the Admin from the User's Profile Page. The Admin Can Delete or Remove the Uploaded File without the Knowledge of the user. But the user can't Delete the File Uploaded by the Admin. User's Access is to Download the File only not to Modify the files. Uploaded Files can be Removed by the Admin in case of Mistake Sending of Files. User Can Download the Files intended to them Unlimited Number of times. System showed very good Performance in terms of speed, accuracy, and ease of use.

The User Can View the Files Uploaded by the Admin without Downloading it. User can View Image Files, Play Video Files, View Document Files before downloading the Files. It Helps the Users to Check the files before downloading it. It Reduces the False Downloading Rate.

7. CONCLUSION

The proposed system convey that special feature of this software is the geniality and it can be worded on the personal computer, since the web page gives a variety option and the message gives clear understanding of the next page it is easy to follow and use. A novel approach which uses sound signature to recall graphical password click points is proposed. No previously developed system used this approach. This system is helpful when user is logging after a long time. In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text.

REFERENCES

[1] Veena Rathnavel, "**GRAPHICAL PASSWORD AS AN OTP**", International Journal of Engineering & Computer Science ISSN:2319-7242, Mumbai, Volume 6 Issue Page No 20090-20095, 1 January 2014.

[2] Marry Harin Fernandez, Sangeetha, ShanmugaPriya, "**GRAPHICAL PASSWORDS EFFECTS FOR TOLLERANCE PASSWORD IMAGE CHOICE & OTP LOGIN SECURITY**", SSRG International Journal of Computer science & Engineering, Chennai, Special Issue, March 2014.