"IMPLEMENTATION OF SOUND SIGNATURE IN GRAPHICAL PASSWORD AUTHENTICATION SYSTEM"

[1]NAFEES FATEMA
Department of Information Technology, HVPM College of Engineering & Technology Amravati, India
nafeesfatema95@gmail.com
[2]BHAKTI KADU
Department of Information Technology, HVPM College of Engineering & Technology Amravati, India
kadubhakti95@gmail.com
[3]PROF. S. G. ANANTWAR
Department of Information Technology, HVPM College of Engineering & Technology Amravati, India

ABSTRACT: *In this project, a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image. System showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.*

Keywords Authentication, 3-level passwords, textual passwords, graphical passwords, PassPoints, Cued Click Point, Sound Signature, Tolerance Level

1. INTRODUCTION

Our system is a multifactor authentication scheme. It combine the benefits of existing authentication schemes to form the 3-levels of secure password. The 3-level of password is constructed using the exciting features of the current authentication systems such as textual passwords and graphical passwords.

In our system there are three levels of security. Consider an example of our house, whenever we are going to attend any function we are always providing security to first our safe then our rooms and then main entrance of our house. Indirectly we are increasing the levels of security for our house. In the same way we have implemented the three security levels.

The three levels are as follows,

A. Textual Passwords:

Textual passwords are the passwords normally every websites have, those passwords are vulnerable and can be easily hacked by dictionary attacks.

B. Graphical passwords:

Basically two types of techniques are present to implement graphical password [2].

Pass Point Technique : In this technique only one image was used to implement the system and user has to select multiple points in that single image .System was more secured but it was quite complex for user to remember number of pixels in one image only[3].

Figure 1: Pass Points

Cued Click Point Technique: In CCP, users click one point on each of images rather than multiple points on one image .System developer will select the number of images to be used. 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, as we discuss later. As shown in Figure 1, 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.

Figure 2: Cued click points

A. Sound Signature

Sound signature is integrated to help with the password. No system has been devolved so far which uses sound signature. Study says that sound signature or tone can be used to add facts like images; text etc .Our idea is inspired by this novel human ability. Research says that human can remember images as well as sound tone easily; by applying this method we design our project so it will provide more security. Observed that all

student who were registered entered their graphical password and video sound clip and it will be more secured from their point of view it is very good for Graphical and sound clip password authentication system.

2. LITERATURE REVIEW

Considerable work has been done in this area, the best known of these systems are Pass faces. Brostoff and Sasse (2000) carried out an empirical study of Pass faces, which illustrates 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 (Boroditsky, 2002), the user chooses several predefined regions in an image as his or her password. To login the user has to click on the same regions.

In effect, this requires artificial, cartoon-like images rather than complex, real-world scenes. 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. As shown in Figure 2, 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. If they dislike the resulting images, they could create a new password involving different click-points to get different images.

3. ANALYSIS OF PROBLEM

The 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 [1].

So we have implemented our authentication system with the CCP and Sound Signature.

4. IMPLEMENTATION

In the proposed methodology we have integrated sound signature to help in recalling the password. 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 we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which he want 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 sequence of images and clicks on each image at click points of his choice. Profile vector is created.

A. 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: (Rajeev, 9675, 34) Detailed Vector

Image Click points

I 1 (564,674)
I 2 (345,967)
I 3 (154,756)
I 4 (756,984)
I 5 (486,684)

We have calculated the sound signature using the package of windows media player library .user has to cross all the layers otherwise user will be considered as an imposter.

B. Architecture of the developed system

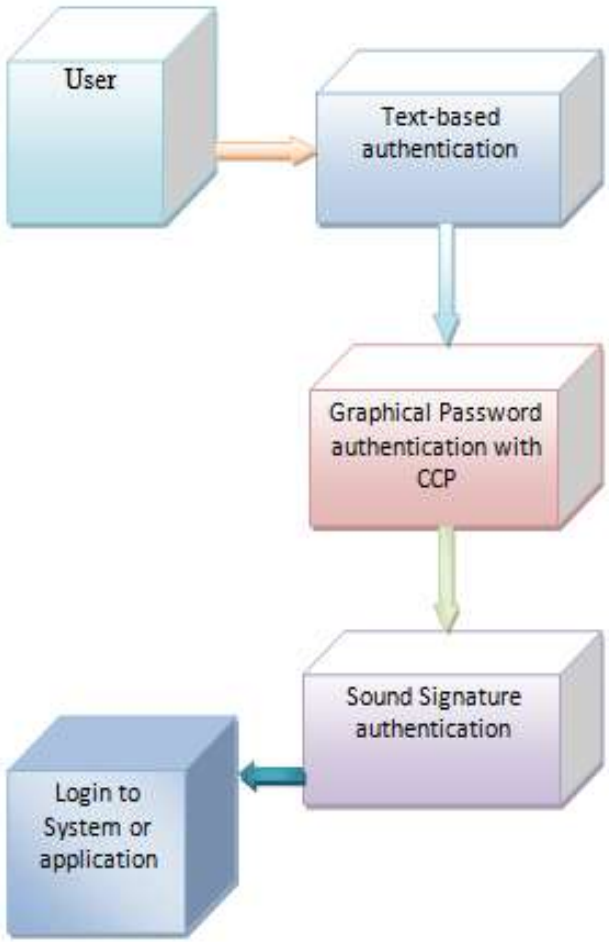
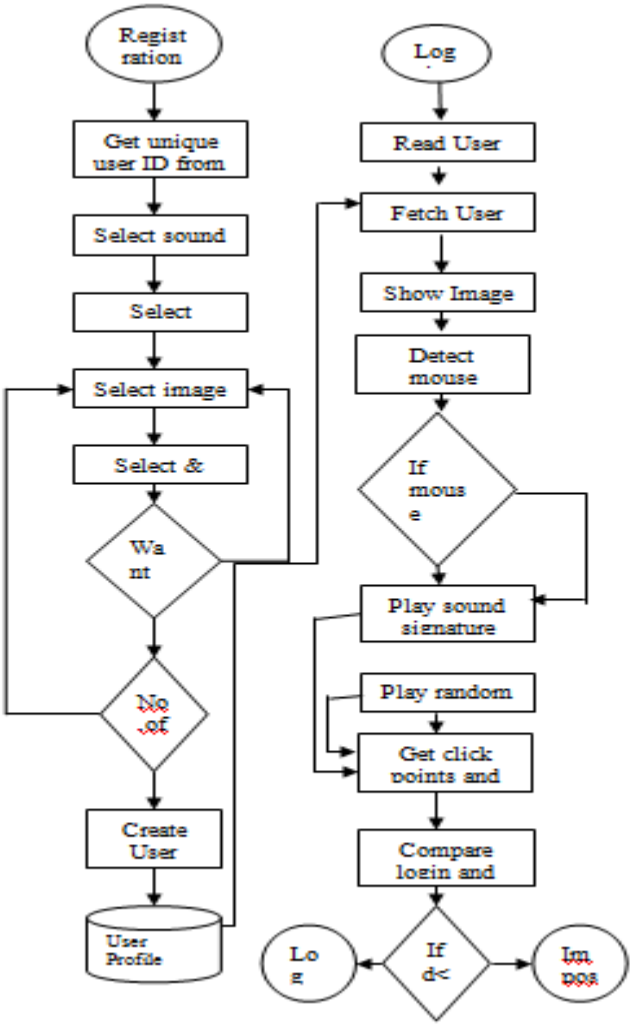


Figure 3: Architecture of the developed System

C. System flow chart



D. Working Process

User has to sign up for creating account
In figure 4 the user bhakti is sign up for the account.
During signup user will have to entre his information like user id, user password, mobile number, and the most important is sound signature.

Figure 4: Registration Process

We have implemented this using windows media player. At the time of Sign in user will have to enter user id and the password.

After successful registration user has to select a sequence of images as password with the corresponding sound signature

Figure 5: Login process

Fig.5 shows us that user selected 3 images for the password .After selecting sequence of images user will have to select pixels and a corresponding sound signature on images as password. The selected point is shown in the figure 5.After login account will be shown to user.

5. CONCLUSION

In today's life security is one of the most important parameter to the organization. In the current state there are many authentication schemes. Some of the schemes are based on the physical and behavioral properties of the user, and some other authentication schemes are based on the knowledge of the user such as textual and graphical passwords. Also, there are other authentication schemes that are based on tokens such as smart cards i.e., based on what you have. Among the various authentication schemes, the most commonly used schemes are textual password and token-based schemes, or the combination of both .These passwords can be easily cracked .Thus, by considering all the issues and problems related to the security we have designed the discussed system.

6. REFERENCES

[1] Lalu Varghese1, Nadiya Mathew2, Sumy Saju3, Vishnu K Prasad4, 3-Level Password Authentication System, Department of Information Technology, Amal Jyothi College of Engineering, Kanjirappally, Kerala, India.

[2] Sonia Chiasson1, 2, P.C. van Oorschot1, and Robert Biddle2, GraphicalPasswordAuthentication
Using Cued Click Points, School of Computer Science, Carleton University, Ottawa, Canada2 HumanOrientedTechnologyLab, CarletonUniversity, Ottawa, Canada (chiasson, paulv)@scs.carleton.ca, Robert biddle@carleton.ca

[3] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007