Implementation of Integrating Sound Signature with Graphical Password System

Prof. Nitin Ujgare  
NDMVP’s KBT College of Engg  
Nashik, (India)

Abhilasha Deshpande  
NDMVP’s KBT College of Engg  
Nashik, (India)

Sujata Bagade  
NDMVP’s KBT College of Engg  
Nashik, (India)

ABSTRACT
Graphical password with supportive sound signature technology is to increase memorization of password.

In this paper we are going to propose a system to recall the password that consists of sequence of some images in which user can select one-click point per image in addition user is asked to select sound signature to each click-point. In graphical password click result in showing next image in effect leading users down a path as they click on their sequence of points. Wrong click leads to wrong image. This system will be helpful to recall the password when user is logging into account after a long time and provides more security.

Keywords: Sound signature, Authentication, CCP.

1. INTRODUCTION

Various graphical password schemes have been proposed as alternatives to text-based passwords. Psychology research has proved that the human brain is better at recognizing and recalling images compare to text. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While the predictability problem can be solved by prohibiting user choice and assigning passwords to users using some standards, this usually leads to usability issues since users cannot easily remember such random passwords.

Number of graphical password systems has been developed. Study shows that text-based passwords suffer with both security and usability problems. Integration of sound signature in graphical password authentication system is designing and developing new model of graphical password which works on click based graphic method, in this method random images are used where user need to select one click per image after selecting image user is requested to select sound signature corresponding to each click point.

2. RELATED WORK DONE

The Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of user’s ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. The existing system is Pass Points proposed passwords which could be composed of several points anywhere on an image [3].

Graphical Password:
Access to computer systems is most often based on the use of alphanumeric passwords. However, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. The password problem arises largely from limitations of human’s long-term memory (LTM) [2].

3D Password:
In the beginning of 3D password user will be authenticate with simple textual password. After successful authentication user moves in 3D virtual environment. Thereafter a computer with keyboard will be seen on screen. On that screen user have to enter password (textual), which is stored in a simple text file in the form of encrypted co-ordinates (x1, y1, z1). After successfully completion of this authentication, Then user automatically enter into an art gallery, where he/she has to select multiple point in that gallery or can do some action in that environment. It seems obvious that some areas of an image are more attractive to users as click-points. If this phenomenon is too strong, the likelihood that attackers can guess a Password significantly increases. They can select a set of likely hotspots through image processing tools or by observing a small set of users on the target image and then building an attack dictionary based on those points.
2.1 Technology Used

2.1.1 NetBeans:

The NetBeans Platform allows applications to be developed from a set of modular software components called modules. A module is a Java archive file that contains Java classes written to interact with the NetBeans open APIs and a manifest file that identifies it as a module. Reason for Using Java is to explore systems running different operating system. In order to do so, there should be some way to connect to bridge those operating systems so that all the differences between them are solved and the functionalities are achieved.

2.1.2 SAPI:

The Speech Application Programming Interface (SAPI) allows speech recognition and speech analysis within windows applications. We will use SAPI basically to integrate sound with graphical password. This software converts our text into speech or sound.

2.1.3 Serialization:

In context of data storage Serialization is a process of translating data structures or object state into a format that can be stored and reconstructed later in the same or another computer environment. Java provides this mechanism, called object serialization where an object can be represented as a sequence of bytes that includes the object’s data as well as information about the object’s type and the types of data stored in the object. Thus serialization will act as a database of our system.

3. IMPLEMENTATIONS DETAILS

We have proposed system and implementing an application for the security and recovery of the graphical password. Till now the systems are developed for the security of the password but by this application we are trying to provide the security as well as recovery also. This application will use sound signature to help the user to recover the password. In addition we are going to use centered Discretization Algorithm [2].

Hence to store the password, we need to discrete the point by calculating its offset d and its corresponding segment identifier i. Offset d will get stored in clear while i store in protected form. Hence when the re-entry of the password will occur the system should aware of the tolerance segment identifier i which is the acceptable inaccuracy calculated by

\[ i = \left[ \frac{x-r}{2r} \right] \quad \ldots \ldots \ldots \ (i) \]

At the time of sign-up user has to select a sequence of points on images with required tolerance and the corresponding sound signature and at the time of login if user clicks on pixel that lies within a tolerance area his/her login will be successful. Otherwise any random images will be shown to the user.

To store the images and account details (eg. User_id ,email_id). We have used a mechanism called object serialization which will act as a database of our system. We have also used serialization instead of any other database system as it is less complex as well as it requires less time than any others. The main goal of our system is to integrate the sound with graphical password for this purpose Speech Application Programming Language (SAPI) software is being used. This is basically a text to speech converter.

Thus whatever textual signature you will give will be converted into sound signature. You may assign a sound of your own choice to your graphical password. User can select sound to each image or selected set of images depending on your wish. In case if user forgot the password and clicked on any wrong pixel then as a result user’s selected sound signature at the time of registration will be play. This will definitely help the user to recover the password. This system will work...
same as that of real world accounts, you can send mail, receive mail, send image files, etc [3].

4. RESULT

User has to sign up for creating account.

Fig 4.1: Signup for mail

In fig. 4.1 the user sujata is sign up for the account. During signup user will have to enter his information like user id, user password, mobile number, and the most important is sound signature. We have implemented this using Net beans and serialization. At the time of Sign in user will have to enter user id and the password.

Fig 4.2: Selecting Sequence of images as a password

After successful registration user has to select a sequence of images as password with the corresponding sound signature. Fig. 4.2 shows us that user selected 4 images for the password.

Fig 4.3: Selecting pixel on an images

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 fig 4.3.

Fig 4.4: User Account

After login account will be shown to user. User can send file, message or any picture. It will work as real world email account.

Fig 4.5 Forgot password

If the legitimate user forgot the password, and unable to recall it by the sound signature, then it can be
recover by answering the selected secret question which is shown in the image 4.5. The answer for the first pet is dog. Here user can add his own question also.

After answering the secret question the system will generate the one time password number and send it to user. This OTP will be used to reset the password.

5. CONCLUSION

This application will help the user to increase the security of user account as well as help to recover the password user can access their email account. This web application not only makes the email access more complete but also could be a harbinger to the new world of Assistive Web Technologies for mentally retarded persons.

This method of recalling the password is best but not silver bullet as it won’t be applicable to all types of users.

5.1 Future Scope

We can integrate graphics password system with other patterns like touch of smells. Study shows that these patterns are very useful in recalling the associated objects like images or text. This system will help the user to recall the password as well as it becomes difficult for hacker to hack the user account.

6. REFERENCES

[1] Integration of Sound Signature in Graphical Password Authentication System by Saurabh Singh and Gaurav Agarwal (Invertis University, Bareilly, India).

[2] Centered Discretization with Application to Graphical Passwords (by Sonia Chiasson Carleton University Ottawa, Canada Jayakumar Srinivasan Toronto Canada Robert Biddle Carleton University Ottawa, Canada P.C. van Oorschot Carleton University Ottawa, Canada)

[3] Integration of Sound Signature in 3D Password Authentication System (by Mr. Jaywant N. Khedkar1, Ms. Pragati P. Katalkar2, Ms. Shalini V. Pathak3, Mrs. Rohini V. Agawane)

[4] Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Alain Forget, Robert Biddle, Member, IEEE, and P. C. van Oorschot, Member, IEEE

[5] Integration of Sound Signature and Graphical Password Authentication System Suyog S. Nischal1, Sachin Gaikwad2, Kunal Singh3 Prof. A. Devare4
