Authentication System with Graphical Security and Sound Signature

Vikram Verma
Computer Science and Engineering Department, ASET,
Amity University
Noida, India

Shilpi Sharma
Assistant Professor
Computer Science and Engineering Department, ASET,
Amity University
Noida, India

ABSTRACT

This document provides guidelines for implementing an authentication system which works on graphical password and includes sound signature. Click based graphical password provides security from brute force and dictionary attacks and they are not predictive thus it’s not easy to breach them and a sound signature is integrated along with which enhances the security as this sound signature also under goes the password verification, and once the graphical password along with the sound signature is verified the user is allowed to log into the system.

Keywords

Cued click points, sound signature, authentication, encryption.

1. INTRODUCTION

Passwords are used for Authentication, Authorization and Access Control. Users mostly select passwords which are easy to predict. This is the case 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. The predictability problem can be solved by restricting user from choosing predefined passwords and assigning passwords to users, this generally leads to usability issues because users cannot easily remember such random passwords.

Many graphical password systems have been developed, study shows that, textual passwords suffer with both security and usability problems. According to a recent news article, a security team at a company used a network password cracker and within 30 seconds and they identified about 80% of the passwords. It is a well-known fact that the human brain recognizes and recalls images better than text, thus using images as password is a better approach than textual passwords.

Considerable work has been done in this area. One of the best known of these systems are Passfaces, Brostoff and Sasse conducted an empirical study of Passfaces, which shows how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall that is a user clicks on several previously chosen locations or coordinates in a single image to log in. As implemented by Passlogix Corporation, the user needs to choose several predefined regions in an image as his or her password and to log in, the user has to click on the same regions.

The problem that persists in this scheme is that the number of predefined regions is small, perhaps a few dozens in a picture thus the password may have to be about12 clicks for adequate security which is again a tedious task for the user. Another problem of this system is the need for the predefined regions to be readily identifiable. In effect, this would require artificial, cartoon-like images rather than complex, real-world scenes, thus restricts the user’s space from choosing the images for creating a secure yet easy to recognize password.

In order to overcome these problems, a new method called Cued Click Points (CCP) is a proposed as an alternative to PassPoints. In CCP, the user can click only one point or the number of points he can remember based on his memorizing capability on each of the images rather than on clicking on several points on one single image. Thus it offers cued-recall and introduces visual cues which instantly alert the valid users if they have made a mistake when entering their latest click-point and then at that point they can cancel their attempt and retry from the beginning. It also helps in making attacks on hotspot analysis more challenging.

2. OUTLINE

Data security has been a prime concern since networking. Although various algorithms and tools are available to secure data, it is however being intruded or data hacked.

Following are some approaches which were proposed earlier:

Recognition Based Techniques: Dhamija and Perrig [2] proposed a graphical authentication scheme which was based on the Hash Visualization technique [4]. In that system, the user was asked to select a certain number of images from a set of program generated images. Later, the user was prompted to identify the pre-selected images in order to get authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. The major drawback of this system was that the system needs to store a huge data in order to store images for each user. Also, selecting images for each user from the picture database is a challenging task and it needs a lot of computation time.

Passface: “Passface” is another technique which was developed by Real User Corporation [6]. The basic idea behind this is that the user will be asked to choose four images of human faces from a database of face images as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated only if he identifies the four faces correctly. This technique is based on the assumption that people can recall human faces easier than other pictures. User studies by Valentine [7,8] have shown that Passfaces are very memorable over long intervals. However the effectiveness of this method is still uncertain.

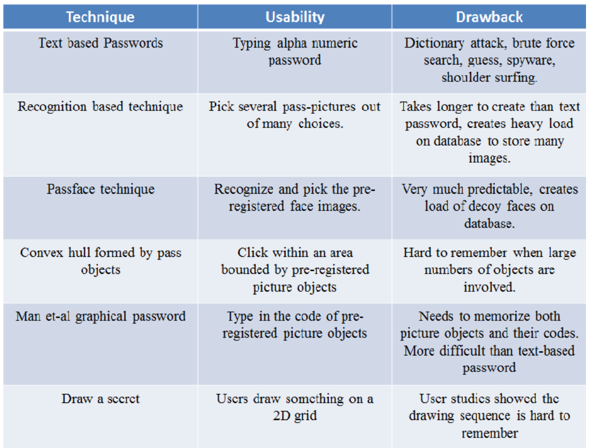
Davis, et al. [10] studied the graphical passwords created using the Passface technique and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Passface password somewhat predictable.

Convex Hull of Pass Objects: This method was given by Sobrado and Birget [11] to develop a graphical password, this technique deals with the shoulder-surfing problem. In the first scheme, the system will display a number of pass-objects which are pre-selected by the user among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. To make the password hard to guess, Sobrado and Birget suggested the use of 1000 objects, which makes the display very crowded and the objects are almost indistinguishable, and using fewer objects would lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user needs to move a frame until the pass object on the frame lines up with the other two pass-objects. It is also suggested to repeat this process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the log in process can be slow.

Et-al Graphical Password: Man, et al. [12] proposed another graphical password system. In this system, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass-objects. The benefit is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because there is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant.

Draw a Secret: Jermyn, et al. [13] proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password. A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. The drawback of this system is that, the drawing sequence is hard to remember.

Comparison of existing systems:



Technique	Usability	Drawback
Text based Passwords	Typing alpha numeric password	Dictionary attack, brute force search, guess, spyware, shoulder surfing.
Recognition based technique	Pick several pass-pictures out of many choices.	Takes longer to create than text password, creates heavy load on database to store many images.
Passface technique	Recognize and pick the pre-registered face images.	Very much predictable, creates load of decoy faces on database.
Convex hull formed by pass objects	Click within an area bounded by pre-registered picture objects	Hard to remember when large numbers of objects are involved.
Man et-al graphical password	Type in the code of pre-registered picture objects	Needs to memorize both picture objects and their codes. More difficult than text-based password
Draw a secret	Users draw something on a 2D grid	User studies showed the drawing sequence is hard to remember

3. PROPOSED SYSTEM OVERVIEW

The system proposed here is a multi-layered system to strengthen security. The system intends to create a graphical password using a single/multiple images and associate a sound file. Password is generated by assigning click points in each image and associating sound file, above that the SQL server is used to maintain users and provide another security layer. Steps for creating graphical password:

- Identifies a matrix of images to generate graphical password by choosing click points.
- Redirect the image and the password generated to the SQL server database after performing encryption on click points.
- Identify a sound signature (file), convert to byte form and perform encryption and then associate it with the graphical password in the database.

Steps for verifying password:

- The first step would ask the user to verify him-self by entering his SQL server account details.
- Once he gets verified from SQL server, he is taken to sound signature verification screen, where he needs to provide the right sound file to the system, which is then verified by the system by performing encryption and then comparing the encrypted form with the database.
- Once the sound file is verified he is taken to graphical password screen where he gets images in the same sequence as he gave the system during password creation, here as the sound file is verified the user gets some clue area where his click points are present, the user then needs to click on the exact correct click points on the image in the right sequence, these click points are verified by the system image by image by performing encryption on click coordinates and then comparing the encrypted form with the database

4. OBJECTIVE OF THE PAPER

The objectives and purpose for this paper is to analyse the existing password systems and suggest a new graphical password system which would enhance the security and also help in smoothening the system working. This not only focuses on security maintenance of the data but also keeps in mind about the resources which are being used thus focus is on complete optimization of graphical password system, along with enhancing the security by addition of sound signature into the graphical password system.

5. MODULES OF PROPOSED SYSTEM

User maintenance:

This module allows the registration of the users. The users are created with security accounts in the SQL Server database. Each user is associated with password. Only users having these accounts can access the application to perform any specific task.

Graphical password generator:

The module allows the user to generate password from images. The user has to specify the required image and click on the image to generate strokes. Each stroke provides a pair of co-ordinates x, y location from the image. The co-ordinates in the pattern clicked and the number of strokes along with the image is redirected to the database after performing encryption. The source image can be deleted as the application does not have a direct dependency on the physical file as the image and click information has been directed to SQL database.

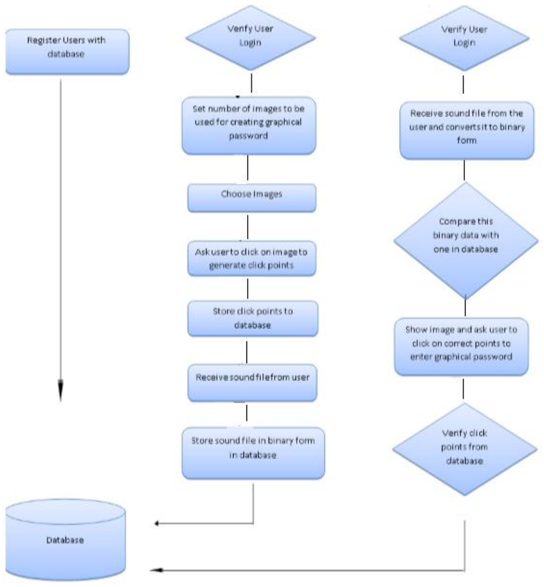
Associate sound signature:

The module allows the user to choose an audio file at runtime or use his voice for creating sound file. This audio is converted to binary format and this binary file is then encrypted and associated with the graphical password and dumped into the SQL database. It strengthens the security of the protected data.

Verification:

This module asks user to provide SQL password and then asks user to provide audio file and then performs binary conversion and encryption of sound file then verifies it with the stored sound file's encrypted form and then shows images to the user for reading graphical password from the user, as the user is verified partially with the help of sound file, he is provided with approximate areas which helps user to recognize his click points, it then perform encryption on click points and then compares them with the stored password.

6. ARCHITECTURE OF PROPOSED SYSTEM


Register Users with database
Verify User Login
Set number of images to be used for creating graphical password
Choose Images
Ask user to click on image to generate click points
Store click points to database
Receive sound file from user
Store sound file in binary form in database
Verify User Login
Receive sound file from the user and converts it to binary form
Compare this binary data with one in database
Show image and ask user to click on correct points to enter graphical password
Verify click points from database
Database

System includes a SQL server for storing user information and graphical password associated with sound signature, GUI is provided with the help of windows forms, which provide an interface to users to interact with the system for creating graphical password by choosing images and then providing click points and then for providing sound file to the system for associating sound signature. The click points undergo MD5 encryption and then the associated sound file is converted to binary form and then MD5 encryption is performed on binary data and stored in database.

During verification user first needs to verify his login to SQL server, he gets access to the system and then he provides the sound file which is then verified by converting and comparing in encrypted form, then the user is taken to graphical password screen where user click on click points and system verifies this graphical password.

7. CONCLUSION & FUTURE SCOPE

The use of graphical images and sound signatures strengthens the security system by almost removing the chances of getting breached. This application can be used for providing security to any application by placing this application over any application which is needed to be secured and whose security system is to be enhanced. The application here can be used by any organization or industry that needs to handle confidential data. The application ensures that only a legitimate user who can provide the right SQL user password, graphical password and there sequence and along with the right sound file for verification will be able to access the application protected by this security system.

This system can further be enhanced by providing a more user friendly and easy access for legitimate users by providing them with the facility to use sound signature first and on its authentication system generates the approximate graphical password which must be further corrected by the legitimate user. Thus helps legitimate users in recollecting graphical password and stops any kind of false trails of illegitimate users.

8. REFERENCES

[1] Integration of Sound Signature in Graphical Password Authentication System International Journal of Computer Applications (0975 – 8887) Volume 12– No.9, January 2011

[2] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[3] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes.13th USENIX Security Symposium, 2004.

[4] A.Perrig and D.Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[5] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[6] RealUser, "www.realuser.com," last accessed in June 2005.

[7] T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[8] T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.

[9] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

[10] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[11] L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[12] S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[13] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.