INTEGRATION OF SOUND SIGNATURE IN GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Shital Kharche , *Department Of Computer Science and Engineering , G.C.O.E, Amravati* ,
shitalkharche@outlook.com

Pushpanjali Chauragade , *Department Of Computer Science and Engineering , G.C.O.E, Amravati*

***Abstract*—**In proposed work a click-based graphical password scheme called Cued Click Points (CCP) will be implemented. Here a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. 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. This Systems will give very good Performance in terms of speed, accuracy, and ease of use. Here we will use preferred CCP to Pass Points, considering that selecting and remembering only one point per image is easier and sound signature helps considerably in recalling the click points.

Keywords: Sound signature, Authentication, ccp

1. INTRODUCTION

Passwords are used for –

(a) Authentication (Establishes that the user is who they say they are).

(b) Authorization (The process used to decide if the authenticated person is allowed to access specific information or functions) and

(c) Access Control (Restriction of access-includes authentication & authorization).

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 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. It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic. The Cued Click Points (CCP) scheme is a proposed alternative to PassPoints. In CCP, users click on

one point on each of 5 images rather than on 5 points on one image. It offers cued-recall and introduces visual cuest hat instantly alert valid users if they have made a mistake when

entering their latest click-point.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.

2. LITERATURE SURVEY

Sr. no.	Technique	Usability	Drawback
1	Text based Passwords	Typing alpha numeric password	Dictionary attack, brute force search, guess, spyware, shoulder surfing.
2	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.
3	Passface technique	Recognize and pick the pre-registered face images.	Very much predictable, creates load of decoy faces on database.
4	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.
5	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
6	Draw a secret	Users draw something on a 2D grid	User studies showed the drawing sequence is hard to remember

Table 1: Literature survey

3. DESIGN

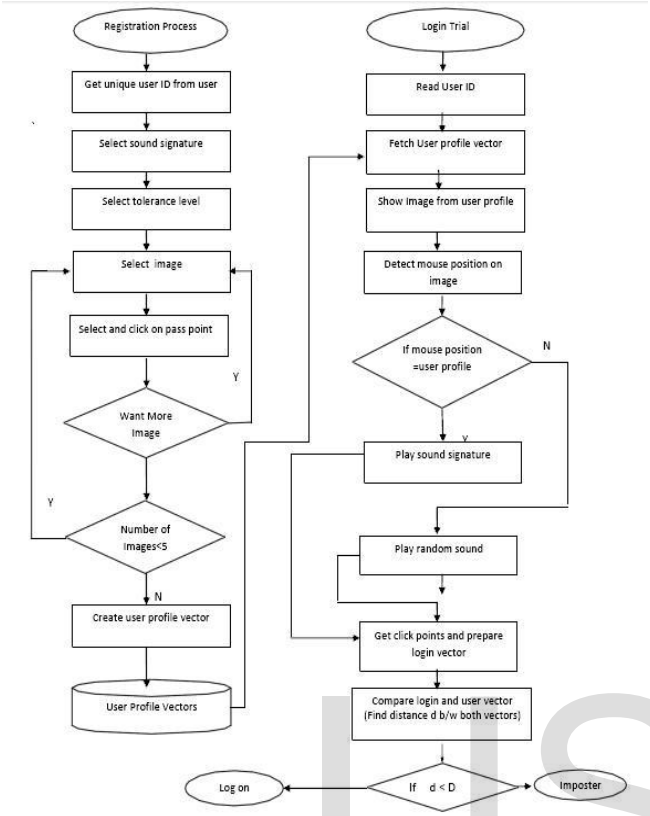

Figure 1. System Flow Chart

2.1 Create User profile Vector (master)

While registration of user information, the user id, sound frequency or time and tolerance are getting for creating master vector.

2.2 Create Detailed Vector

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. Detailed Vector - (Image, Click Points).

2.3 Compare User Profile/login Vector

Enters User ID and select one sound frequency or time 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. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image and sound signature helps considerably for login.

4. PROCEDURE

4.1 Login Registration

In this step, the users are registered with the SQL Server database. The proposed system creates user profile using registration form to fill the detail about the user. A user has to select one or more (not more than five) target images from the given collection presented by the system. Enter the lock code which is only four digit number to open the system.

4.2 Graph password Generator

In this step, a collection of 5 target images is presented on the user profile during registration. The user can browse from one set to other using the "browse image" button on the screen.A user can choose each image from a different set. Browse and choose the click point on the first image to store as a password. Again browse and choose the click point on the second target image, this process continue upto 5 target images. *The fiveselected images (target images) with click point (cued-click point) make up a password.*

4.3 Associate Sound Signature

This module allows the end user to choose an audio file at runtime. The file is converted to binary form and then it is associated with the graphical password.

4.4 Data Protection and Non-protection

This module allows the user to specify text content or file at runtime for whom data protection is to be provided and also specifies the container image to perform steganography.

5. RESULT

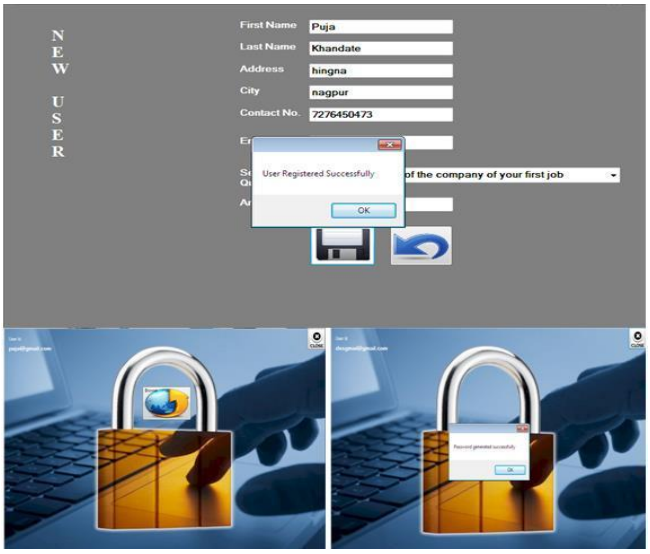

Fig 2. Graph password Generator

6. SYSTEM TOLERANCE

After creation of the login vector, system calculates the Euclidian distance between login vector and profile vectors stored. Euclidian distance between two vectors p and q is given by-

$$\mathrm{d}(\mathbf{p},\mathbf{q}) = \sqrt{(p_1-q_1)^2+(p_2-q_2)^2+\cdots+(p_n-q_n)^2} = \sqrt{\sum_{i=1}^{n}(p_i-q_i)^2}.$$

Above distance is calculated for each image if this distance comes out less than a tolerance value D. The value of D is decided according to the application. In our system this value is selected by the user.

7. CONCLUSION

We have proposed a novel approach which uses sound signature to recall graphical password click points. 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.

8. ACKNOWLEDGEMENT

this paper has benefited from conversations with many different people – far more than can be acknowledged completely here. still we would like to particularly thank, hod of computer science and engineering, mrs. pushpanjali chauragade madam, for her guidance and support.

REFERENCES

1] A. M. Andrew. Another efficient algorithm for convex hulls in two dimensions. *Information Processing Letters*, 9(5):216– 219, 1979.
2] Proceedings of the 8th USENIX Security Symposium Washington, D.C., USA, August 23–26, 1999.
3] Pinks, B. and T. Sander. Securing Passwords against Dictionary Attacks. ACM, CCS, 200.
4] Wiedenbeck, S., J.C. Birget, A. Brodskiy, and N. Memon. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS, 2005.
5] Van Oorschot, P.C., S. Stubblebine. On Countering Online Dictionary Attacks with Login Histories and Humans-in-the-Loop. ACM Trans.Information and System Security 9(3), 235-258, 2006.
6] Thorpe, J. and P.C. van Oorschot. Human Seeded Attacks and Exploiting Hots-Spots in Graphical Passwords. 16th USENIX Security Symposium, 2007.
7] K. Golofit. Click passwords under investigation. In 12t h European Symposium On Research In Computer Security (ESORICS), Springer LNCS 4734, September 2007.
8] 15. Dunphy, P., J. Nicholson, and P. Olivier, *SecuringPassfaces for Description. 2008.*
9] Y. Xiang et al. (Eds.): ICA3PP 2011 Workshops, Part II, LNCS 7017, pp. 153–164, 2011.Springer- Verlag Berlin Heidelberg 2011, Engineering and Technology
10] In© World Academy of Science International Journal of Computer, Information, Systems and Control Engineering Vol:8 No:2, 2014