IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 3, March 2017

Authentication using Graphical Password with Association of Sound Signature

C. Rajalakshmi[1], C. Rohini[2], S. Sowndharya[3], A. Christy Jebamalar[4]

UG Students, Information Technology, Sri Krishna College of Technology, Coimbatore, India [1,2,3]

Assistant Professor, Information Technology, Sri Krishna College of Technology, Coimbatore, India[4]

Abstract: A graphical password system with a supportive sound signature to enhance the remembrance of the password and to enhance the security level in authentication system is discussed. In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is implemented. 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 which is correlated to each click point this sound signature will be used to help the user in recalling the click point on an image. Systems shared very good Performance in terms of speed, accuracy, and enhance the security. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was very easy and sound signature helps considerably in recalling the click points.CCP offers both improved usability and security.

Keywords: Sound signature, Authentication, Cued click point.

I. INTRODUCTION

Passwords are used for –

(a) Authentication (the process or action of verifying the identity of a user)
(b) Authorization (Permission to access a resource)and
(c) Access Control (selective **restriction** of access to a place or other resource).

Mostly user prefers password that can be easily predicted. This happens with both text and graphical based passwords. Users look after to choose significant password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for hackers to guess. While this predictability issue can be solved by disallowing user choice and allocating passwords to users, this usually leads to usability problems since users cannot easily remember such random passwords. Many number of graphical password systems have been developed, Study shows that text-based passwords agonize with both security and usability issues[1][8]. According to a recent news article, a company's security team ran a network password cracker and within 30 seconds and they identified about 75% of the passwords [2]. It is well known that the human brain is better at recognizing and recalling images than text[3][7], humancharacteristic is exploited using graphical passwords.

II. PREVIOUS WORK

Substantiate work has been done in this area.The best known of these systems are Passfaces [4][7]. Brostoff and Sasse (2000) carried out an empirical study of Passfaces, which illustrates well how a graphical password recognition system typically operates. Passfaces are graphical passwords that use faces as a unique verification technology for secure logon.Blonder-style passwords are based on cued recall. A user selectson several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation (Boroditsky, 2002), the user prefers to choose several predefined regions in an image as his or her password.

In order to log in,the user has to click on the same regions. The problem with this scheme is that the number of predefined regions is little, in case a few dozens in an image. The password may have to be up to 12 clicks for sufficient protection, again rigour for the user. Another problem of this system is the requirement for the predefined regions to be instantly identifiable. In consectary, this needs artificial, cartoon-like images rather than intricate, real-world scenes[5][6]. Cued Click Points (CCP) is an alternative which is proposed to PassPoints. In CCP, users click one point on each of 3 images rather than on five or more points on one image. It offers cued-recall and presents visual cues that readily alert precise users if they have make an error when entering their proximity click-point (at which point they can cancel their effort and retry from starting). It also makes attacks based on hotspot analysis more difficult.

As shown in Figure 1, each click results in showing a next-image, in result leading users down a "path" as they click on their alignment of points. An incorrect click leads down a wrong way, with a descriptive sign of authentication defeat only after the last click. Users are allowed to choose their images only to the area that their click-point dictates the next image. If they distaste the resulting images, they could create a new password involving alternate click-points in order to get different images.

DOI10.17148/IJARCCE.2017.6394

III. PROPOSED WORK

In the proposed work we have integrated sound signature in order to assist in recalling the password. No system has been developed so far which employs sound signature in graphical password authentication. Study says that sound signature or tone can be employed to recall stuffs like images, text etc[6]. In daily life we see discrete examples of recalling a substance by the sound related to that substance[6]. Our opinion is inspired by this novel human skill.

A. ProfileVectors-

The proposed system creates user profile vectors such as
1.Master vector -
(User ID, Sound Signature frequency, Tolerance)
2.Detailed Vector - (Image, Click Points)

B. Registration Process-

Enter the User ID and choose one sound frequency which the user want to be played at login time, a tolerance value is also chosen, which will decide that the user is legitimate or an imposter. To fabricate detailed vector user has to choose alignment of images and clicks on each image at click points of the users selection. Profile vector is materialized.

Table 1. Attempts by authorized participants

No.	Login ID	Login Trails	Times Accepted	Times Rejected
1	U1	3	3	0
2	U2	3	2	1
3	U3	3	3	0
4	U4	3	3	0
5	U5	3	3	0
6	U6	3	1	2
7	U7	3	3	0
8	U8	3	3	0
9	U9	3	3	0
10	U10	3	2	1
11	U11	3	3	0
12	U12	3	3	0
13	U14	3	3	0
14	U14	3	3	0
15	U15	3	3	0
16	U16	3	3	0
17	U17	3	3	0
18	U18	3	3	0
19	U19	3	3	0
20	U20	3	3	0

C. System Tolerance

After fabrication of the login vector, system evaluates the Euclidian distance between login vector and profile vectors which is stored. Euclidian distance between login vector **p** and profile vector **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 evaluated for each and every image if this distance comes out less than the tolerance value D. The value of D is resolved as stated by the application. In our system this value is elected by the user.

Table 2. Attempts by Pretender

No.	Login ID	Login Trails	Times Accepted	Times Rejected
1	U1	3	0	3
2	U2	3	0	3
3	U3	3	0	3
4	U4	3	1	2
5	U5	3	0	3
6	U6	3	0	3
7	U7	3	0	3
8	U8	3	0	3
9	U9	3	0	3
10	U10	3	0	3
11	U11	3	1	2
12	U12	3	0	3
13	U14	3	0	3
14	U14	3	0	3
15	U15	3	0	3
16	U16	3	0	3
17	U17	3	0	3
18	U18	3	0	3
19	U19	3	0	3
20	U20	3	0	3

IV. EXPERIMENTATION RESULT

Data which is brought together from 20 participants. Each participant was requested to register himself/herself and then each user was called for login trail 5 times as legitimate user and 5 times as imposter unusually. Users were final year engineering students of age group 18-28 Y. Table 1 restrains the detail of the data produced by legitimate users and Table 2 shows the data produced by imposters. According to the data produced FRR is 4.0 and FAR is 2.0 which are better for Graphical password certification system.

V. CONCLUSION AND FUTURE WORK

We have suggested an innovative method which employs sound signature in order to recall graphical password click points. No formerly developed system used this method. This system is very useful when the user or participant is logging after a very long time.

In fortune systems various other patterns might be used for remembering purpose such as tap of odor, study shows that these patterns are very helpful in remembering the associated objects such as text or image.

DOI10.17148/IJARCCE.2017.6394

REFERENCES

[1] Birget, J.C., D. Hong, and N. Memon. Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.

[2] Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.

[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.

[4] Cranor, L.F., S. Garfinkel.Securityand Usability. O'Reilly Media, 2005.

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

[6] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163,1967.

[7] 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.

[8] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp.1399-1402.

DOI10.17148/IJARCCE.2017.6394