International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Integration of Sound Signature in a Graphical Password Authentication System

Syed Misbahuddin
(M.Tech) (CNIS) computer networks and information technology, Department of IT at Sreenidhi Institute of Science and Technology(SNIST), Hyderabad India.

Guide
Mr. Md Jaffar Sadiq
Associate Professor, Department of IT at Sreenidhi Institute of Science and Technology (SNIST), Hyderabad, India.

Abstract:
Here, 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 click point this sound signature will be used to help the user to login. 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.

Introduction

The image-handling component enables users to choose images or to introduce their own; the images are stored together with a collection of images provided by the system. For this password system to work well, it is important that the images be fairly intricate, with hundreds of interesting details that could be chosen as click regions (e.g., topographic maps, architectural images, cityscapes, certain landscapes, and renaissance paintings)[5]. The password selection component allows the user to select a new password. Assuming the user has already logged in (by using either a graphical or a conventional password), the user enters the “password” command. The system then prompts the user for a user name and current password. If the system accepts the current password, it lets the user specify a new image (or keep the current image), and set the safety parameter r for robust discrimination (or keep a default value).

The graphical password schemes we considered in this study have the property that the space of passwords can be exhaustively searched in short order if an offline search is possible [2]. So, any use of these schemes requires that guesses be mediated and confirmed by a trusted online system. In such scenarios, we believe that our study is the first to quantify factors relevant to the security of user-chosen graphical passwords. In particular, our study advises against the use of a Pass faces TM-like system that permits user choice of the password, without some means to mitigate the dramatic effects of attraction and race that our study quantifies [6]. As already demonstrated, for certain populations of users, no imposed limit on the number of incorrect password guesses would suffice to render the system adequately secure since, e.g., 10% of the passwords of males could have been guessed by merely two guesses [16].

A “zero-knowledge” approach of never showing a picture group twice gives immunity from eavesdropping, but separate tests showed that when groups were reused, the subjects’ accuracy improved [11]. They did not confuse the destructors with the

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

images on which they had been trained, and thus could use our methods for longer times without the need for retraining.

A sound signature recognitions password system is introduced, as from the existing relationship system, we incorporated sound signature by clicking the image a beep sound is introduced, the same sound is produced in all the images, if we proceed the same click point in all the images with similar sound then the authentication proceeded to the login page, there we can read out the important messages [8].
The click-point fails in any relating images and sound or if we failed to click exactly, then it will not transmit to the login session. The mail advantage of this proposed system is to enhance authentication process in a high reliable one for the end users.

Passwords are used for

- Authentication (Establishes that the user is who they say they are).
- Authorization (The process used to decide if the authenticated person is allowed to access specific information or functions) and
- 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 [1][8].

Existing System:

In the existing system, Brostoff and sasse carried out an empirical study of passfaces, which illustrates well how a graphical password recognition system 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, the user chooses several predefined regions in an image as his or her password. To log in the user has to click on the same regions in effect, 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. 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.

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

Disadvantages of Existing System:

The problem with this existing 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 the existing system is the need for the predefined regions to be readily identifiable.

Proposed System:

In the proposed work 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.

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 (Smith, 2689, 50)
Detailed Vector

Image	Click points
I_1	(123,678)
I_2	(176,134)
I_3	(450,297)
I_4	(761,164)

Advantages of Proposed System:

- The proposed sound signature will be used to help the user to login.
- The proposed System also has a 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

MODULES:

- Create User profile Vector (master)
- Create Detailed Vector
- Compare User Profile/login Vector
- Upload/Download Module

MODULES DESCRIPTION:

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.

Master vector –
(User ID, Sound Signature frequency, Tolerance)

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)

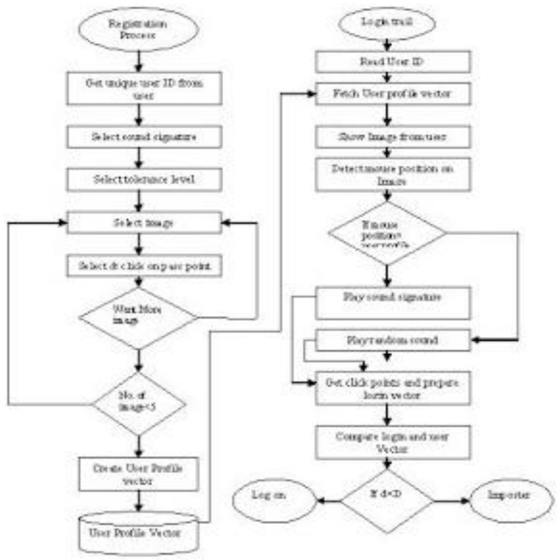
Compare User Profile/login Vector:

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.

Upload/Download Module:

Admin, defence, navy and air force are going to upload secret file between them. They can share the uploaded files. User (defence, airforce and navy) uses sound signature for download files. System showed very good Performance in terms of speed, accuracy, and ease of use.

System Flow Chart:



Conclusion & Future Enhancement

An OTP (one time password), has been added to login which needs username and the graphical password. At the time of login whenever we type the username then the OTP will be sent to the respective registered email, the graphical password will be asked only when the user enters the correct OTP.

And another feature is added to capture the IP address and send it to the registered email if there are any illegal login attempts of 3 from any of the computer.

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. Security and 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.

[9] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy and N. Memon, "PassPoints: Design and longitudinal valuation of a graphical password system", International Journal of Human-Computer Studies, vol. 63, (2005), pp. 102-127.

[10] D. Weinshall, "Cognitive Authentication Schemes Safe against Spyware", (Short Paper), IEEE Symposium on Security and Privacy, (2006).

[11] G. E. Blonder, "Graphical Passwords", United States Patent 5,559,961, (1996).

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

[13] J. C. Birget, D. Hong and N. Memon, "Graphical Passwords Based on Robust Discretization", IEEE Trans. Info., Forensics and Security, vol. 1, no. 3, (2006) September.

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

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

[15] L. F. Cranor and S. Garfinkel, “Security and Usability”, O’Reilly Media, (2005).

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

Mr. Md. JaffarSadiq is working as an Associate Professor , Department of IT at Sreenidhi Institute of Science and Technology (SNIST), Hyderabad, India. He has received M.Tech.(CSE) from JNTUH, Hyderabad. He has 10 years experience in teaching. His main research interests are Image Processing,web Technologies.

Syed Misbah uddin student of M.tech (CNIS) computer networks and information technology, Department of IT at Sreenidhi Institute of Science and Technology(SNIST), Hyderabad India.