Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey: Login with Image Based Password Authentication

Mr. A. A. Shinde*, Ms. S.R. Chokhandre, Mrs. R.C. Roychaudhary, Mrs. S. S. Telrandhe Mrs. C. N. Rokde
Information Technology & RTMNU
India

Abstract— An important usability goal for knowledge based authentication systems is to support users in selecting passwords of higher security. We use persuasion to influence user choice in click based graphical passwords, encouraging users to select more random and hence more difficult to guess, click points. Passwords theft can happen on daily basis, so we need to protect them. A distributed system provides user with the case of being accessible. Making user familiar with the concept of images is also important, so a user guide facility is also provided. This paper describes a general purpose mechanism for authenticating users through image selection.

Keywords— Authentication, passwords, persuasion, Click Based Authentication, Selection based Authentication

I. INTRODUCTION

Authentication of humans is based on some combination of what you are (biometric), what you have (token) and what you know (password). Text based username-password systems have been traditionally used in authenticating users before allowing them to access the services. One way to overcome this problem is to assign a random password to the user. The problem with this scheme is human difficulty in recalling a random character string. Often the user will then write it down, making it vulnerable to interception. Another major drawback with text is word of mouth transferability. A user can tell his friend the password quite easily. This paper considers the knowledge based authentication. Authentication plays an important role in protecting resources against unauthorized use. Still the most widely used authentication system is based on text passwords. Text based passwords are not secure enough for many applications that enforce security by access control mechanisms. More sophisticated authentication process is costly and may need additional equipment or hardware. Image based Authentication (IBA) is based on user's successful identification of his image key password. After the username is sent to the authentication module, it responds by displaying an image which consists of click based approach in image from the user's password set mixed with other images. The purpose of this paper is to present the authentication process which is simple enough and cost effective.

II. LITERATURE REVIEW

Some researchers have worked on image based authentication. One of the researchers in his paper proposed that there will be set of images and some of the images will be password. User is assigned a subset of images from a large set. Images from the large sets are presented to the user who then selects those that belong to his image set. [1] Another researcher proposed in his paper that the user submits user id and an image as credentials to the system. If the image matches with the one stored in the system, the user is authenticated. The system remains simple as password based one. The images are not stored in the system. Only the hash values are stored. User carries the image with him. [2] Some researchers proposed that the system will display both images and the corresponding alphanumeric characters assigned to the images together. Images are rendered unclick able. [3] The text based passwords are ubiquitous, ambiguous and error prone authentication system. To overcome this anomaly, the graphical password is considered as an alternative to traditional textual password. This paper also tells about enhanced graphical password authentication techniques like selection based authentication and click based authentication mechanisms. [4] In this paper researchers concluded that User authentication is a fundamental component in most computer security contexts. They proposed a more secure graphical password authentication system where they proposed that main reason for adaption of graphical password is that people are better at memorizing graphical passwords than text-based passwords. The system combines graphical password scheme along with a handheld device to form a novel method of multi-factor authentication. This authentication scheme ensures the protection from threats such as key loggers, hotspot, shoulder surfing etc.[5]

III. BACKGROUND

The method described in our paper authenticates a user to a device using a visual login technique called Image password. Its aim is to give users a simple and natural means of authentication through image selection.

For image authentication, there are four different authentication mechanisms.

- Selection-Image based Authentication
- Click-Image based authentication
- Segment-Image based authentication
- Split-Image based authentication

Image based authentication methods like click-based authentication and selection based authentication system displays an image or set of images to the user, who would then select one to identify them. The system uses such image based passwords and integrates image registration and notification interfaces. Image registration enables users to select the image as per their choice or convenience.

Image based authentication schemes are simple authentication techniques where images are used as passwords. The user submits User ID and an image as credentials to the system. If the image matches with the one stored in the database, the user is authenticated. Since images are easy to remember, this reduces the overhead of users to remember lengthy and complex textual passwords and of which combinations of alphabets, special symbols or digits they are.

Table I: Click Based Approach

Usability	74%
Ineffectiveness	89%
Reliability	94%

A common security goal in password-based authentication system is to maximize the password effectiveness. This impacts usability when user choice is involved, where it is possible to allow user choice while still increasing the password effectiveness.

Methods for authenticating a user for access to a restricted resource comprises of:

Login to the account for user includes following steps.

- Presenting a first image to user (images being divided into sections).
- Accepting a selection of first section selected by user.\
- Subsequently generating code from selection.
- Storing the code generated.
- Displaying second image to the user.
- Accepting the second section selected by user.
- Generating code from selection.
- Storing the said account code.

This process proceeds until the authentication process get completed.

IV. PROPOSED SYSTEM

To enrol with the image based authentication system, one has to sign up the form where in user has to fill in the required details. The users who already have been authenticated manually by the administrator can exercise the login process. This is done by feeding the unique user information and the email id's in the authentication server beforehand. Next, user initiates the process of signing up. If the user is authenticated i.e. the entered id matches one of those already fed then the corresponding email id is displayed. Username selected by the user should be distinctive and should be chosen according to the requirements of the designer. If the needed information is submitted successfully, the user proceeds to the password generation to decide on his new set of images as password. The clicking of mouse on images does not highlight the selected image. Finally after the sign up process is completed, login window will get open. After that if the login is successful the user is all set to use the system.

V. FEATURES

The system has a very user friendly graphical user interface (GUI), where main window will have an option comprising for new user and existing user login. A user has to register before he can login to the system. A user is registered by entering his personal details along with an image. Once the user selects the image it will be displayed on the window for the user to verify his image. The image is user's choice. He can bring his own image in a storage device.

User proceeds to the next stage for generating password. For generating the password, there will be a window consisting of number of images displayed on it. User will select any one of the image by its own choice for first password. For Increasing security is to enforce a minimum number of click points, but allow users to choose the length of their password, similar to minimum text password lengths. The system would continue to show next images with each click, and users would determine at which point to stop clicking and press the login button. Although most users would likely choose the minimum number of click-points, those concerned with security and confident about memorizing can select a longer password.

- As per sign-up steps, user will definitely login to the system. In the login window, users enter its existing user id and selected images for authentication.
- The home window will glow when user get entered successfully in authenticated system. There will be lots of option for user's requirements, with logout option.

VII. OBSERVATION AND FUTURE ENHANCEMENT

Use of fractal images makes this system somewhat difficult to use in the beginning. Better user interface design can influence users to select stronger passwords. Log files also show that this is true. User's success rates show much improvement over time, with corresponding decreases in authentication time as experience is gained. Future

enhancements about this proposed system is that this design can be further improves to enhance security. We can implement much better features like black list accounts approach for unauthorized accessing with the aid of database.

VIII. CONCLUSION

Image- based authentication techniques, although currently in their infancy, might have a wider applicability in future. We perceive it more user-friendly technique that helps to increase the password quality tremendously compared to a text-based approach. In this paper we have proposed simple secure authentication technique issues of how better to protect the available information. We have also identified various issues related with such a system and proposed a novel concept.

REFERENCES

[1] Richard E. Newman, Piyush Harsh and Prashant Jayaraman, "Security Analysis of and Proposal Foe Image- based authentication", Proceedings of IEEEICCST 2005, p.-141, October 2005 CISE Dept., University of Florida, Gainesville FL 32611.

[2] Srinath Akula, Veerabhadram Devisetty, "Image Based Registration and Authentication System", Department of Computer Science, St Cloud State University St. Cloud, MN 56301.

[3] Piyush Harsh, Richard Newman, "Usability and Acceptance of UF-IBA and Image Based Authentication System", Proceedings of IEEE ICCST-2007, CISE DEPT, University of Florida, Gainesville FL 32611-6120.

[4] Thirumaram M. DhavachelvanP, Maria Stepen, "Segment and Split-Image Based Authentication Techniques for mobile Devices", Dept. of Computer Science, Dept of Computer Science, Pondicherry University, Pondicherry, India. International Journal of Engineering & Technology, Volume 2, Number4, December 2009.

[5] A Aswathy Nair#1, Theresa Rani Joseph#2, Jenny Maria Johny#3, "A Proficient Multilevel Graphical Authentication System", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, No 6, June 2013.Pg 1341-1344.

