Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Two Level Authentication System Based on Pair Based Authentication and Image Selection

Madhuri Achmani[1], Radhika Dehaley[2], Anuja Gaonkar[3], Anindita Khade[4]
[1,2,3]UG Student of Department of Computer Engineering, S.I.E.S. Graduate School of Technology
[4]Assistant Professor of Department of Computer Engineering, S.I.E.S. Graduate School of Technology

Abstract--This paper presents a two level authentication using pair based authentication and image selection. The most common method for authentication is textual passwords. Though textual passwords are easy to remember, they are vulnerable to eaves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords have been introduced as an alternative to textual passwords. But same as textual passwords, shoulder surfing attacks make most of the graphical schemes vulnerable. To address this problem, textual passwords can be combined with graphical schemes in what gives a two level security. This paper presents an integrated evaluation of the pair based passwords and graphical password scheme, including usability and security evaluations and implementation considerations.
Keywords--Authentication, Two level security, Session password, Intersection, Graphical password.

I. INTRODUCTION

A number of problems are associated with knowledge based authentication, typically text based passwords. To make a textual password secure, random and lengthy passwords are used. But such passwords are difficult to remember and recollect. Owing to this, users tend to pick short passwords or the ones that are easy to remember. Unfortunately, these passwords can be guessed or cracked easily [1]. Biometrics was proposed as an alternative technique. But it has its own disadvantages. Biometrics such as finger prints, iris scan or facial recognition have been introduced but they are not yet widely adopted. A major drawback of these systems is that not only these systems are very expensive, but also the identification process can be slow [3]. Though graphical passwords provide a better security, most of them are prone to shoulder surfing.

People select predictable passwords, while setting textual and/or graphical passwords. Users tend to select passwords that are memorable in some way, which unfortunately often means that the passwords tend to follow predictable patterns that are easy for the attackers to exploit. Though the problem of predictable passwords can be solved by disallowing the choice of the users and assigning them the passwords directly, usability issues occur in such cases because the users cannot remember and recollect the randomly generated passwords.

A password authentication system should encourage string passwords while maintaining memorability. Our proposed system encourages user to select a normal password, yet maintaining the security of the application [2]. To achieve this, we have proposed a system that gives two levels in which the user is authenticated. If the user fails the authentication test, he/she will not be allowed to go to the second level. This paper presents a detailed description of the flow of the proposed system as well as the working of the same.

II. BACKGROUND

Text passwords are the most popularly used user authentication method, but are vulnerable to security and usability problems. One major problem with the textual passwords is the vulnerability to dictionary attack, shoulder surfing and guessing attacks. As discussed earlier, alternative techniques such as biometric and tokens have their own drawbacks [1], [2], [3].

The concept of session passwords and graphical passwords came into use so that the drawbacks of textual passwords can be overcome. Session passwords are one time passwords and change with every login, thereby making the system more secure. Also graphical passwords provide a good level of security as they are based on "Recognition and Recall" techniques.

This paper provides details about a system that increases the level of security by using a user authentication scheme that integrates the session password and the graphical password schemes. Owing to this, the system will be provided with a two level security, first that uses session passwords and the second that uses graphical passwords. The advantage of this type of authentication system is that if the user is not validated in the first phase of authentication, he/she cannot go for the second phase. Therefore, the system validates the user more effectively and efficiently.

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III. RELATED WORK

Dhamija and Perrig[4] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre selected images for authentication from a set of images as shown in Fig. 1. A drawback of this system is the vulnerability to shoulder surfing.

Fig. 1: Random images used by Dhamija and Perrig

Passface [5] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user as shown in Fig. 2. In this technique, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. The procedure is repeated four times since there are four images to be selected.

Fig. 2: Example of Pass faces

Jermyn[6] proposed a new technique called "Draw- a-Secret" (DAS) as shown in Fig. 3 where the user is required to re-draw the pre-defined picture on a 2D grid. The user is authenticated if the drawing touches the same grid in the same sequence.This technique of authentication is vulnerable to shoulder surfing.

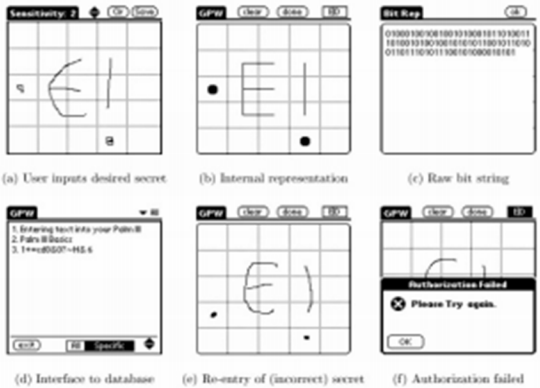

Fig. 3: DAS technique by Jermyn

Syukri [7] came up with a technique where authentication is done by drawing user signature using a mouse as shown in Fig. 4. This

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

technique included two stages, registration and verification. At the time of registration stage the user draws his signature with a mouse and the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature. A disadvantage of this technique is the forgery of signatures. Also, drawing with mouse is not familiar to many people and it is difficult to draw the signature in the same perimeters at the time of registration.

Fig. 4: Signature technique by Syukri

Blonder [8] designed a graphical password scheme where the user must click on the approximate areas of pre-defined locations. Passlogix [9] extended Boulder's scheme by allowing the user to click on various items in correct sequence to prove their authenticity.

Haichang [10] proposed a new shoulder-surfing resistant scheme as shown in Fig. 5 where the user is required to draw a curve across their password images orderly rather than clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user.

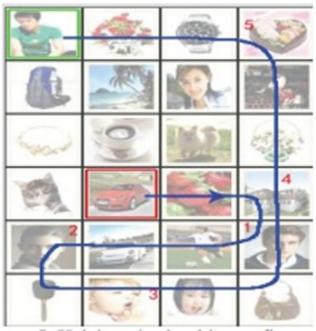

Fig. 5: Haichang's Shoulder surfing Resistant technique

Wiedenback [11] describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks as shown in Fig. 6. A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess large number of objects can be used but it will make the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large.

Fig. 6: Example of a Convex Hull

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Jansen [12,13] proposed a graphical password scheme for mobile devices. During password creation, a user selects a theme consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence of the chosen images will create a numerical password. As the number of images is limited to 30, the password space of this scheme is not large.

Weinshall and Kirkpatrick [14] proposed several authentication schemes such as picture recognition, object recognition and pseudo word recognition and conducted user studies on these. The results declared that pictures are most effective than the other two proposed schemes. Goldberg [15] designed a technique known as "passdoodle". This is a graphical password authentication scheme using handwritten design or text usually drawn with a stylus onto a touch sensitive screen. To overcome the shoulder-surfing problem, many techniques are proposed. Zhao and Li [16] proposed a shoulder-surfing resistant scheme "S3PAS". The main idea of the scheme is that in the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region. The system integrates both graphical and textual password scheme and has high level security.

IV. PROPOSED SYSTEM

A. Grid-Based Authentication Scheme

Text based passwords are widely used as a method of authentication. But because of their vulnerability to various attacks, new methods of authentication are being encouraged. The proposed system makes the use of text based passwords in the first level of authentication in a way which is based on recalling ability of the human mind.

The first layer of authentication is pair based authentication scheme where modules are divided into three parts those are user registration process, system login process and session password selection [17]. At the time of registration user submits his username and password. The length of the password should be 8 and it can be called as secret pass which is a session password. The session password should contain 4 characters. During the login phase, when the user enters his username an interface comprised of a grid will displayed. The size of grid is 6 x 6 and it consists of digits and alphabets. These are randomly generated and the grid interface changes every time. User has to consider his secret pass in terms of pairs based on some rules. For the first letter in the pair the row has to be considered and for the second letter column is considered. The intersection letter is the first character of the 4 characters of the session password. If the two letters are in the same row and column then special character or one of the two letters is to be entered as the character of the session password. This is repeated for all pairs of secret pass. If the password is correct, the user is allowed to enter in to the second layer of authentication.

Fig. 7: Login Interface

Fig. 8: Intersection letter for pair AN

B. Image Selection Authentication Scheme

Graphical password scheme is an authentication system that works by having the user select images from a set of images, that is presented in a graphical user interface. This is a technique that been evolving in recent years as a better and safer way of authentication.

During registration, the user selects three images from the displayed set of images in the form of 3*3 grid view. These selected images are recorded and the user is supposed to remember the images selected during the registration process. During login process, the user selects the same images selected by him during registration. If the user selects the correct images the user will be proceeded for the pair based session password. If the user fails to select the correct images chosen by him during the registration process the user will be deauthenticated and will have to login again with correct image selection process to proceed for pair based pair password entry.

Fig. 9: Grid Interface for Registration and Login Phase

V. CONCLUSION

The system was tested for various users and has been verified for the authentication schemes. It has been observed that though the proposed system provides a better security, the time required for the login process is a more than a normal login procedure. But for a safer security mechanism, this is a small compromise.

VI. ACKNOWLEDGMENT

We thank Prof. Mrs. Anindita Khade for her support and for providing the necessary guidance concerning the implementation of our project. We would also like to thank the Department of Computer Engineering, SIES Graduate School of Technology and our Principal Dr. Alka Mahajan for their support and facilities provided to us for the same.

REFERENCES

[1] L. Jones, A. Anton, and J. Earp, “Towards Understanding User Perceptions of Authentication Technologies,” Proc. ACM Workshop Privacy in Electronic Soc., 2007.
[2] L. O’Gorman, “Comparing Passwords, Tokens, and Biometrics for User Authentication,” Proc. IEEE, vol. 91, no. 12, pp. 2019-2020,Dec. 2003.
[3] A. Jain, A. Ross, and S. Pankanti, “Biometrics: A Tool for Information Security,” IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.
[4] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.
[5] Real User Corporation: Passfaces. www.passfaces.com
[6] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.
[7] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): SpringerVerlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[8] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[9] Passlogix, site http://www.passlogix.com.
[10] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing
[11] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102-127.
[12] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.
[13] W. Jansen, "Authenticating Users on Handheld Devices “in Proceedings of Canadian Information Technology Security Symposium, 2003.
[14] 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.

[15] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.
[16] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.
[17] N. S. Joshi,"Session Passwords Using Grids and Colors for Web Applications and PDA" in International Journal of Emerging Technology and Advanced Engineering