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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

A Simple Text Based Graphical Password Scheme to Overcome Shoulder Surfing Attacks

Monali Bendale[1], Neeta Singh[2], Sujata Baid[3] , Aman Maurya[4]

BE (comp), Department of Computer Engineering, SSBT's COET Bambhori, Jalgaon (M.S.), India[1,2,3]

Assistant Professor, Department of Computer Engineering, SSBT's COET Bambhori, Jalgaon (M.S.), India

Abstract: As conventional password schemes are harmful to shoulder surfing, most of the shoulder surfing resistant graphical password schemes have been proposed. But most of the users are more familiar with textual passwords rather than graphical passwords, however text-based graphical password schemes have been proposed. In existence there are no text-based shoulder surfing resistant graphical password schemes which are both secure and efficient enough. So, in this paper, we propose an enhanced text-based shoulder surfing resistant graphical password scheme by using pointers. The user can easily and efficiently login system in the proposed scheme. Later, we analyze the security and usability of the proposed scheme, and shows the resistance of the introduced scheme to accidental login and shoulder surfing.

Keywords: Shoulder Surfing Attacks, accidental login, usability, resistance, pointers.

I. INTRODUCTION

The Shoulder Surfing Attack is an attack which can be done by just observing over someone's shoulder to guess when user enters his/her password. As conventional password schemes are harmful to shoulder surfing three shoulder surfing resistant graphical password schemes are proposed by Sobrado and Birget [1]. With them, many graphical password schemes have been proposed with different degrees of resistance to shoulder surfing, e.g., [2][3][4][6][9][7][8][5], and each has its drawbacks and benefits.

Most of the users are known with textual passwords than graphical passwords, a text-based shoulder surfing resistant graphical password scheme with S3APS have been proposed by Zhao et al. [10]. In S3PAS, the user has to mix His/her textual password on the login screen to gain the session password. But, this login process of Zhao et al.'s scheme is complicated and tedious. And then, most of the text based shoulder surfing resistant graphical password schemes have been proposed, e.g., [11][13][14][12][15]. It is very dangerous that, none of existing text-based shoulder surfing resistant password schemes is both efficient and more secure. We will propose an enhanced text-based shoulder surfing resistant graphical password scheme by using pointers in this paper. This proposed scheme is very simple and easy to learn by the users who are mostly familiar with textual passwords. The user can easily and simply login into the system without using any on-screen keyboard or normal keyboard.

The rest of this paper is organized as follows. In Sec. II, we will describe related works. Proposed scheme will describe in Sec. III. Next, we will analyse the result of the proposed scheme in Sec. IV. , Then conclusions are made in Sec. V

RELATED WORK

In reference [14] Z. Imran and R. Nizami proposed "ADVANCED LOGIN SCHEME" in which they used a "MATRIX". The elements of the matrix will be a RANDOMLY generated set of alphabets, numerals and symbols "without" REPITITION.

In reference [16] Dhamija and Perrig proposed a graphical authentication scheme in which the user identifies the pre-defined images to prove the authentication of the user. In this scheme, during registration the user selects a set of images from a predefined set of images. Later on at the login time the user has to select the images that he had selected during the registration time to prove his authentication.

But this system is vulnerable to shoulder-surfing.

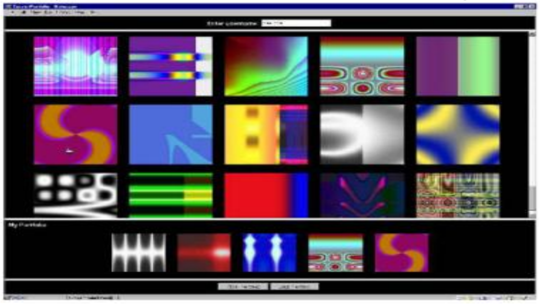


Fig 1.Graphical Authentication Scheme 1

In reference [17] Passface scheme is a grid of nine faces and the user to select on image from the grid. The user chooses four images of human as their password and has to select their pass image from the other eight images. Since there are four users who select images as it is done four times. But this scheme was very easy to attacks by guessing or trying for number of time.

DOI 10.17148/IJARCCE.2015.4387

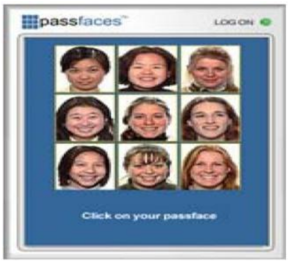
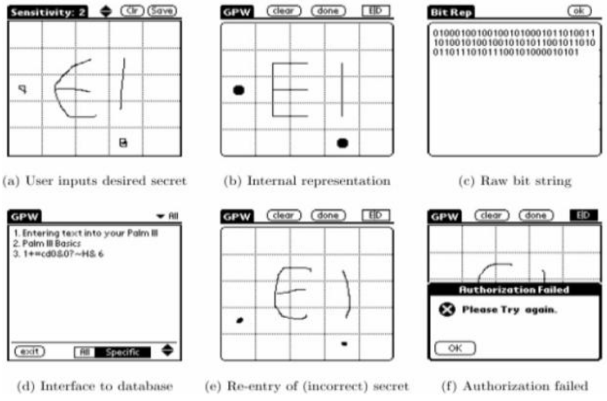


Fig 2.Passfaces

Further studies were made on authentication schemes and a new scheme was proposed known as "Draw-a-Secret"(DAS) by Jermyn, et al. .The user has to draw a picture on the grid at the time of registration. The user has to draw the same picture on a 2D grid at the time of login. If the drawing of picture touches the same grid in the same sequence the users gets authenticated. But this scheme was prone to shoulder surfing attacks.

In reference Draw –A-Secret Similar to this a same scheme was introduced by Syukri [18].This authentication scheme was based on the principle that the user has to draw his signature by using mouse. This scheme had two stages of implementation viz. the registration phase and the verification phase. At the time of registration the user draws a signature that is extracted by the system. At the time of registration the signature is taken as an input and normalization is done and then the parameters are extracted and checking is done and the user is authenticated if the parameters get matched. But drawing with mouse is not so easy and actual parameters cannot be matched with the signature that was drawn at the registration time. This scheme is prone to forgery of signature.



01000100100100101000101101001 1
10100101001001010101100101101 0
0110111010111001010000101 01

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&07~H& 6

Authorization Failed
Please Try again.

(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Fig3. DAS Scheme

PR0POSED SYSTEM

In this part, we will discuss the proposed scheme which is simple text based efficient graphical password scheme using pointers. In which we have considered 64 characters of which 24 Upper cases and 24 Lower cases which also includes all special symbols and alphanumeric characters. It consist of two phases

1. Registration Phase

2. Login Phase

So now we will discuss the phases independently.

1. Registration Phase:-

When the user register for the first time he/she has to enter his/her password K of length L characters and select one pointer which will be a default pointer out of given 8 pointers. the user has to register an e-mail address for re-enabling his disabled account. The Registration phase should not be working in a Shoulder Surfing environment. In addition, a secure channel should be established between the system and the user during the registration phase by using SSL/TLS [16][17] or any other secure transmission mechanism. The user's textual password gain by the system from the users entry in password table should be encrypted by the system key.

2.Login Phase:-

When the user request for the login system it displays the circle consist of 8 sectors filled with different colours as shown in snapshot given below fig 4.

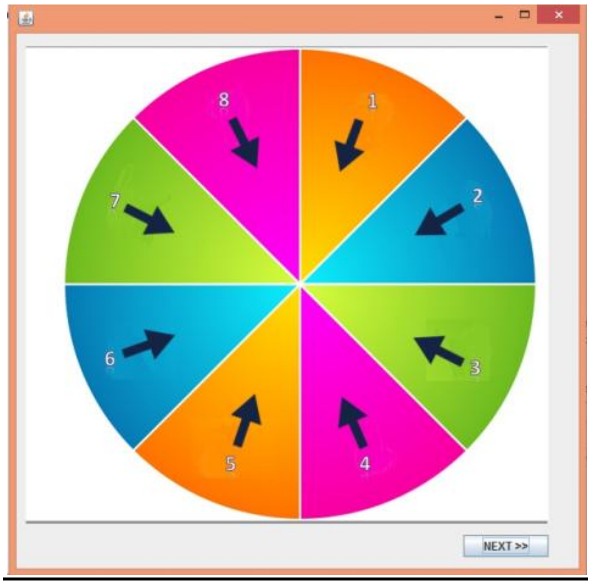


Fig4 .Login Phase

Each sector is identified by the pointers with unique number assigned to each. All the displayed characters can be simultaneously rotated

into either the sectors clockwise by clicking the "clockwise" button once or the adjacent sector anticlockwise by clicking the "anticlockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel. To login the system the user have to go through the following algorithm known as text based graphical password MANS algorithm.

Step 1: The user request to login into the system.

Step 2: The system shows a circle composed of 8 equally sized sectors,

and places 64 characters in which the 8 sectors randomly so that each sector contains some characters. All the characters are in three typefaces in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the Special symbols are in regular typeface, and the 10 alphanumeric characters are in italic typeface. It also

DOI 10.17148/IJARCCE.2015.4387

displays, the button for rotating clockwise, the button for rotating anticlockwise, the "Confirm" button, and the "Login" button are also displayed on the login screen.
All the shown characters can be simultaneously rotated into either the sectors clockwise by clicking the "clockwise" button once or the adjacent sector anticlockwise by clicking the "anticlockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel.
Let i = 1.The user has to select the rotating sector containing the i-th character of his password K, denoted by K_i, into his pointer , and then Click on the "Confirm" button. Let i = i + 1.

Step 4: If i < L, the system randomly shows all 64 characters, and then GOTO Step 3. Otherwise, the user has to click the "Login" button to complete the login process. If the account is unsuccessfully authenticated for three consecutive times, this account will be disabled and the system will send to the user's registered e-mail address an e-mail containing the secret link that can be used by the own user to re-enable his disabled account. The login process of the proposed scheme can be illustrated by an example shown below in Fig. 4. The user has to rotate the sector containing K_i into his pointer. As conventional password schemes are harmful to shoulder surfing, most of the shoulder surfing resistant graphical password schemes have been proposed. But most the users are more familiar with textual passwords rather than graphical passwords, however text-based graphical password schemes have been proposed. In existence there is no text-based shoulder surfing resistant graphical password scheme which is both secure and efficient enough. So, in this paper, we propose an enhanced text-based shoulder surfing resistant graphical password scheme by using pointers. The user can easily and efficiently login system in the proposed scheme. Later, we analyse the security and usability of the proposed scheme, and shows the resistance of the introduced scheme to accidental login and shoulder surfing.

RESULT

As you can see in the given result, first a dialog box will appear in which there are options for new user registration and direct login. Selecting new user will open the registration box in which new user will fill all the new login details and the login button will direct an existing user to the login page. When new user will fill all the detail after completing all the required information user will click on the submit button which will show a notification box of new user registered. After registration user will open the login page. Login page will have a wheel rotating in clockwise and anticlockwise. User will select a region(pointer) as he wants. After selecting the region the wheel will start rotating in clockwise and anticlockwise and wheel contains all the alphanumerical symbols. User will click on the submit button as its desired symbol come under the region. This step will continue until user enters his/her complete password. After completion of the password user will click on login button. Clicking on login button after selecting password will display a dialog box in which a message will display as user authentication successful. User will get three chances to enter his /her correct password, if he/she fails to enter the correct password his/her username will be blocked and an email will be sent to his/hers email id.

CONCLUSION

This paper concludes a simple text-based shoulder surfing resistant graphical password, in which the user can efficiently and easily complete the login process without worrying about shoulder surfing attacks. The method of the suggested scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and simply login into the system without using any on-screen keyboard or normal keyboard.. Finally, we have analyzed the resistances of the proposed scheme to shoulder surfing and accidental login.

REFERENCES

[1] L. Sobrado and J. C. Birget, "Graphical passwords," The Rutgers Scholar, an Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[2] L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005. (http://clam.rutgers.edu/~birget/grPssw/srgp.pdf)
[3] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant Graphical password scheme," Proc. of Working Conf. on Advanced Visual Interfaces, May. 2006, pp. 177-184.
[4] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, "Design and analysis of a graphical password scheme," Proc. of 4th Int. Conf. on Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.
[5] B. Hartanto, B. Santoso, and S. Welly, "The usage of graphical password as a replacement to the alphanumerical password," Informatika, vol. 7, no. 2, 2006, pp. 91-97.
[6] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," Proc. of the 2003 Int. Conf. on Security and Management, June 2003, pp. 105-111 .
[7] T. Perkovic, M. Cagalj, and N. Rakic, "SSSL: shoulder surfing safe login," Proc. of the 17th Int. Conf. on Software, Telecommunications & Computer Networks, Sept. 2009, pp. 270-275.
[8] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme,"Proc. of the First Int. Workshop. on Education Technology and Computer Science, Mar. 2009, pp. 90-95.
[9] T. Yamamoto, Y. Kojima, and M. Nishigaki, "A shouldersurfing-resistant image-based authentication system with temporal indirect image selection," Proc. of the 2009 Int. Conf. on Security and Management, July 2009, pp. 188-194.
[10] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication Scheme," Proc. of 21st Int. Conf. on Advanced Information Networking and Applications Workshops, vol. 2, May 2007, pp. 467-472.
[11] B. R. Cheng, W. C. Ku, and W. P. Chen, "An efficient login-recording attack resistant graphical password scheme—Sector Login," Proc. of 2010 Conf. on Innovative Applications of Information Security Technology, Dec. 2010, pp. 204-210.
[12] M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar. "Authentication schemes for session passwords using color and images," International Journal of Network Security & Its Applications, vol. 3, no. 3, May 2011.
[13] S. H. Kim, J. W. Kim, S. Y. Kim, and H.G. Cho. "A new shoulder-surfing resistant password for mobile environments," Proc. of 5th Int. Conf. on Ubiquitous Information Management and Communication, Feb. 2011.
[14] Z. Imran and R. Nizami, "Advance secure login,"International Journal of Scientific and Research Publications, vol. 1, Dec. 2011.
[15] M. K. Rao and S. Yalamanchili. "Novel shoulder-surfing resistant authentication schemes using text-graphical passwords," International Journal of Information & Network Security,vol. 1, no. 3, pp. 163-170, Aug. 2012 .
[16] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9thUSENIX Security Symposium, 2000.
[17] Real User Corporation: Passfaces. www.passfaces.com
[18] 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): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

DOI 10.17148/IJARCCE.2015.4387