RESEARCH ARTICLE OPEN ACCESS

MINIMIZE SHOULDER SURFING ATTACK BY MEANS OF MANUSCRIPT AND COLOUR BASED GRAPHICAL CODE WORD PROPOSAL

P.Gayathri [1], Mr. A.Senthil Kumar [2]
1(Mphil (Research Scholar), Tamil University, Thanjavur, Tamilnadu, India)
2 (Assistant Professor, Department of Computer Science, Tamil University, Thanjavur, Tamilnadu, India)

Abstract:

A Textual Password Scheme and passage based shoulder surfing unwilling graphical code word system; the better Text and Colour Based Graphical Password system to decrease Shoulder Surfing Attack is projected. By means of this system user can professionally login the system. The proposed system is used to decrease the Shoulder surfing attack and it will get better the safety measures of existing Applications.

Keywords — **Graphical Password, Textual Password, Shoulder Surfing, safety measures, recognition model**

I. INTRODUCTION

The shoulder surfing is a attack which can be can be performed by unauthorized user to obtain the authorized user's password by watching over the user's shoulder when he enters his password. Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they fill out a form, enter their PIN at an automated teller machine, enter a password at a cyber cafe, public and university libraries, or airport kiosks Shoulder surfing can also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand. The conventional password schemes which was used previously are vulnerable to shoulder surfing, so to reduce the effect of Shoulder Surfing attack, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes. Since then, many graphical password schemes with different degrees of resistance to shoulder surfing have been proposed, e.g.,, and but each scheme has some advantages and Disadvantages. It seems that most users are more familiar with textual passwords than pure graphical passwords, Zhao et al. proposed a text-based shoulder surfing resistant graphical password scheme, S3APS. In S3PAS, the user has to mix his textual password on the login screen to get the session password. However, the login process of Zhao et al.'s scheme is complex and tedious. And then, several text based shoulder surfing resistant graphical password schemes have been proposed.

II. LITERATURE REVIEW

In 2002, to reduce the shoulder surfing attack, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme. But from all this schemes, the Movable Frame scheme and the Intersection scheme fail frequently in the process of Authentication. In the Triangle scheme, the user has to select and memorize several pass icons as his password. To login the system, the user has to correctly pass the predetermined number of challenges and in every challenge, the user has to find three pass-icons from a set of randomly chosen icons displayed on the login screen, and then click inside the invisible triangle created by those three pass-icons.

In 2006, to overcome the drawbacks of Sobrado and Birgets Scheme, Wiedenbeck et al propose the Convex Hull Click Scheme (CHC). It is an improved version of the Triangle scheme with great security and usability. To login the system, the user has to correctly follow several challenges and in each challenge, the user has to find any three pass-icons displayed on the login screen, and then click inside the invisible convex hull formed by all the displayed pass-icons. But this scheme Convex-Hull Click has long login time.

In 2009, to overcome the shoulder surfing attack, Gao et al propose a graphical password scheme, which uses colour login and provide resistant to the shoulder surfing attack. In this scheme, the background colour is a usable factor for reducing the login time... This Scheme has drawback like, the probability of accidental login of Colour Login is too high and the password space is too small.

In 2009, a shoulder surfing resistant graphical password scheme, TI-IBA, in which icons are presented not only spatially but also temporally. TI-IBA is less constrained by the screen size and easier for the user to find his pass-icons is proposed by Yamamoto et al. Unfortunately, TI-IBA's resistance to accidental login is not strong. In addition, it may be difficult for some users to find his pass-icons temporally displayed on the login screen. As most users are familiar with textual passwords and conventional, textual password authentication schemes have no shoulder surfing resistance.

In 2007, a text-based shoulder surfing resistant graphical password scheme, S3PAS, in which the user has to find his textual password and then follow a special rule to mix his textual password to get a session password to login the system is proposed by Zhao et al. However, the login process of Zhao et al.'s scheme is complex and tedious.

In 2011, a text-based shoulder surfing resistant graphical password scheme by using colours is proposed by Sreelatha et al. Clearly, as the user has to additionally memorize the order of several colours, the memory burden of the user is high.

In 2011, after Sreelatha, a text based shoulder surfing resistant graphical password scheme, and employed an analysis method for accidental login resistance and shoulder surfing resistance to analyse the security of their scheme is proposed by Kim et al. Unfortunately, the resistance of Kim et al.'s scheme to accidental login is not satisfactory. In 2012, a text based shoulder surfing resistant graphical password scheme, PPC is proposed by Rao et al. To login the system, the user has to mix his textual password to produce several pass-pairs, and then follow four predefined rules to get his session password on the login screen. However, the login process of PPC is too complicated and tedious.

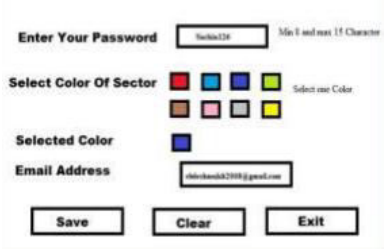
III. IMPLEMENTATION

Existing process

In current days very popular method for Authentication of User is Textual Password. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. Again this Textual Password is also vulnerable to many Attacks like Brute Force Attack, Dictionary Attack, Guessing and Shoulder Surfing. From all of this attack shoulder surfing Attack is most happening. The shoulder surfing attack in an attack that can be performed by the adversary to obtain the users password by watching over the user's shoulder as he enters his password. As we know most users are more familiar with textual passwords than pure graphical passwords, text based graphical password schemes have been proposed. But none of existing graphical password and text based graphical password schemes is both secure and efficient enough to reduce the Shoulder surfing Attack.

Proposed methodology

In this Proposed Scheme, we will describe a simple and efficient Method to avoid the shoulder surfing Attack using Texts and colour based graphical Password Scheme. The Proposed Scheme Contains alphabets i.e 64 characters (26 Capital Letter, 26 Small case letters, 0-9 i.e. 10 decimal digits, two symbols"." and"/".



This proposed system involves registration and the login phase. The System will work in two steps,

Password Registration: In the proposed scheme, user has to set textual password K of length L The minimum length of Password is 8 Characters and the maximum length of password is 15 characters i.e password length is between 8 to 15 Characters, and choose one colour as his pass colour from 8 colours assigned by the system. The remaining 7 colours not chosen by the user are his decoy colours. And, the user has to register an e-mail address for re-enabling his account when he enters a wrong password. In this scheme, registration process should carried out in an environment free of shoulder surfing. In addition, a secure channel should be established between the system and the user during the registration phase by using SSL/TLS or any other secure transmission mechanism. The system stores the user's textual password in the users entry in the password table, which should be encrypted by the system key. So in short in registration phase the user set is textual password and select 1 Colour from 8 Colours.

Login: In the login phase when an user sends an login request to the system, the system displays a circle which is composed of 8 sectors of equal Size. The colors of the arcs of each sectors is different, and every sector is identified by the color of its arc, e.g., the red sector is the sector of red arc. In this Step 64 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counter clockwise by clicking the "counter clockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel.

IV. CONCLUSIONS

In this paper, we had proposed a system which uses text and colour based graphical password which is useful to reduce shoulder surfing attack. Using this authentication method user can login the system without caring about shoulder surfing and he can enter the password without using physical keyboard. This method uses both textual password and color based graphical password and as the user are familiar with both this password scheme user can easily and efficiently login the system. In future, we can use this system in an application, which requires high security.

REFERENCES

1. *Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh," A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme," IEEE 2nd International Symposium on Next-Generation Electronics (ISNE),February 2013 , Kaohsiung, Taiwan.*
2. *L. Sobrado "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4,2002*
3. *J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005.*
4. *S. Wiedenbeck 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.*
5. *H. Gao, X. 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.*
6. *B. Hartanto and S. Welly, "The usage of graphical password as a replacement to the alphanumerical password," Informatika, vol. 7, no. 2, 2006, pp. 91-97.*
7. *S. Man, 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 .*
8. *T. Perkovic, "SSSL: shoulder surfing safe login," Proc. Of the 17th Int. Conf. on Software, Telecommunications & Computer Networks, Sept. 2009, pp. 270-275.*
9. *Z. Zheng, 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.*
10. *T. Yamamoto, and M. Nishigaki, "A shouldersurfingresistant image-based authentication system with temporal indirect image selection," Proc. of the 2009 Int. Conf. on Security and Management, July 2009, pp. 188- 194.*