Achieving Shoulder Surfing Resistant Authentication Using Graphical Password

Pramoth G
Department of Information Technology,
SRM University, Kattankulathur, Chennai, India

Mukesh Krishnan M. B
Department of Information Technology,
SRM University, Kattankulathur, Chennai, India

***Abstract* — The usual text password methods are exposed to shoulder surfing, so many shoulder surfing resistant graphical password methods have been deployed. However, most of the users are feeling more comfort with textual passwords over pure graphical passwords. Unfortunately, all the existing text-based shoulder surfing resistant graphical password schemes are not secure and efficient enough. So in this paper, we propose an improved graphical password scheme for shoulder surfing resistant authentication by using colors in various sectors. In the scheme which we proposed, the user can able to login to an application in very simple and effective manner. Here we analyze the security and usability of the proposed graphical scheme, and prove the resistance of the scheme to accidental login and shoulder surfing.**

General Terms--Pass character, Color sector, Shoulder surfing, Graphical password.

I. INTRODUCTION

An attack that can be performed by a person by watching over the user's shoulder when he enters his password, for acquiring the user's credentials, is commonly known as shoulder surfing attack. More than that, the text password which is usually given as input can be saved by the browser. But in this graphical password method, the passwords are not entered directly, so it would be difficult for anyone to find the user's login credentials. As existing text password schemes are exposed to shoulder surfing, the three shoulder surfing resistant graphical password method was proposed [8]. After that, numerous graphical password methods with various aspects of resistance to shoulder surfing have been proposed [1][2][3][4][5][6]. In S3PAS, to get the session password, the user has to mix his textual password on the login screen. But, this login process is difficult and tedious. Since none of the proposed graphical password schemes are efficient and secure enough, by this paper, we propose an improved text based graphical password scheme for shoulder surfing resistant by using colors. The proposed scheme's working functionality is simple to understand for users, who are familiar with textual passwords. The user can efficiently login to the system without using physical keyboard or on-screen keyboard. The rest of this paper is organized as follows. In section II, we discuss and review the related works. In section III, we discuss the loopholes in existing schemes. In section IV, we will describe the proposed method. In Section V, possible future works will be discussed, before conclusion in section VI.

II RELATED WORKS

The three shoulder surfing resistant graphical password scheme (S3PAS) [1], was proposed in 2002. Then the Triangle Scheme was introduced after the Movable Frame scheme and the Intersection scheme. In the Triangle scheme, the user has to choose and remember several pass characters as his password. In 2006, convex hull click scheme [3] was introduced. To login the application or system, the user has to match the pass correctly in the prearranged number of challenges. In every challenge, the user has to find three pass characters among a set of randomly preferred characters or icons displayed on the login screen, and then the user should click inside the invisible triangle generated by those three pass characters. In 2009, a shoulder surfing resistant graphical password scheme called TI-IBA [7] was proposed. In which icons are presented spatially but temporally. TI-IBA is less controlled by the screen size and simple for the user to find his pass characters. Unfortunately, the resistance to accidental login is not strong in TI-IBA. It is difficult for some users to find their pass characters which are temporally displayed on the login screen. Then another shoulder surfing resistant graphical password scheme was proposed in the same year which is Color Login [4]. The background color is a usable factor for reducing the login time in that scheme. However, the probability of accidental login of Color Login method is too high and the password space is small. In 2007 S3PAS[8] scheme was introduced, in which the user has to find his textual password and then has to follow a special rule for mixing his textual password to obtain a session password to login the application or system. But the login process of S3PAS scheme is complex and tedious. In 2011, yet another text-based shoulder surfing resistant graphical password scheme by using colors [10] was proposed. Here, the user has to memorize the order of several colors, the user's memory burden is high in this scheme. In the same year another text based shoulder surfing resistant graphical password scheme [11] was proposed and employed an testing method for shoulder surfing resistance and accidental login resistance to analyze the security of their scheme. Unfortunately, the resistance of that scheme to accidental login is not satisfactory. In 2012, scheme called PPC [13] was introduced. In this scheme, to login the system, the user has to mix his textual password to generate numerous pass-pairs, and then follow four predefined rules to get their session password on the login screen. But PPC also came out as difficult unfortunately.

III.VULNERABILITIES IN EXISTING SCHEMES

In computer security and cryptanalysis, password cracking is the process in which the passwords are recovered from data that have been transmitted or stored by a computer system. A common approach (brute-force attack) is to try repeated guessing for the password. The purpose of cracking the password is to help a user to recover a forgotten password (though installing a new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a particular system, or as a defensive measure by Administrator of a system to check the passwords which are easily crackable. On a file-by-file basis, cracking the password is utilized to gain access to digital evidence, for which a admin has permissible access but the particular file's access is restricted. In Dictionary attack, the search space can be built in a variety of ways. Most attackers will grab list of words for a variety of topics and languages. Other things tossed in a targeted list of word would include usernames which are relevant to the site being attacked (if known).

Algorithm	Time needed to try entire dictionary
LANMAN	965 seconds (about 16 min)
NTLM	4,541 seconds (about 1.25 hrs)
crypt()	8,783 seconds (under 2.5 hrs)
FreeBSD MD5	1,225,791 seconds (under 15 days)

Hash guessing, here some limited password cracking tools can both crack and extract password hashes, but most password crackers should have the LM password hash before begins the process of cracking. (Some tools can work on NT hashes.)

IV.THE PROPOSED SCHEME

In this section, we describe a efficient shoulder surfing resistant graphical password method based on texts and colors. This scheme includes total of 64 pass characters comprises of 26 small letters(a-z), 26 capital letters(A-Z), 10 numbers(0-9) and any two special characters (here we use . and ,). The proposed scheme have two phases, first one is the registration phase and the second is login phase.

A. *Registration phase*

The user should set his textual password P of length LN (8≤LN≤15) characters, and choose one among eight colors(assigned by system) as his pass color. Then, the user have to register an e-mail address for acquiring his disabled account. The registration phase should be done in an environment free of shoulder surfing. Along with that, a secure channel must be enabled between the user and the system during the registration phase. This can be done by using SSL/TLS [14][15] or any other secure transmission mechanism. The system stores the textual password of the user in the password table of user's entry, which should be encrypted by the system key.

B. *Login phase*

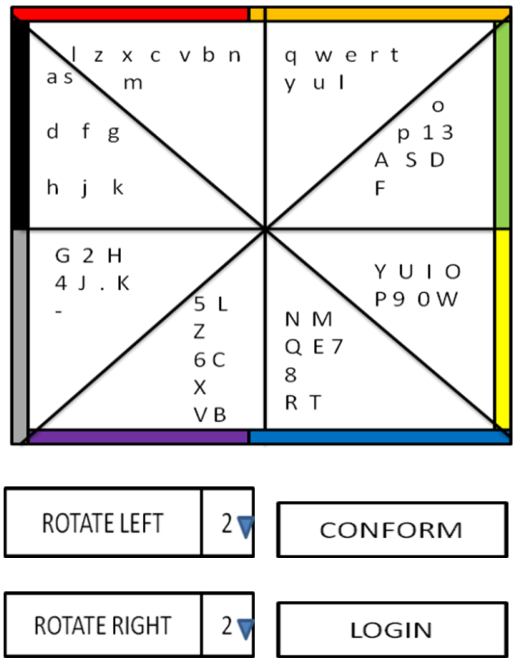

Fig.1 Login Screen

To login the system, the user should complete the following steps:

Step 1: The user should send request to login the system.

Step 2: The system displays a Square composed of 8 equally sized sectors, and provides 64 pass characters among the 8 sectors randomly. So that, each sector consists of 8 characters. The color of each sector's arcs differs from each other. And each sector can be identified by the color of its arc, e.g., the blue sector is the one which are colored blue on its arc. The 64 characters are in two typefaces in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the two symbols "." and "/" along with 10 numbers are in regular typeface. The button for rotating anti-clockwise, the button for rotating clockwise, the "Conform" button, the dropdown list for choosing values and the "Login" button are also displayed on the login screen. All the displayed pass characters can be simultaneously rotated into either the next sector clockwise by clicking the "ROTATE RIGHT" button once or the next sector counterclockwise by clicking the "ROTATE LEFT" button once. Then the dropdown box which have values up to 7 is provided for revolving the pass characters of particular sector to another by skipping the in-between sectors. For example, if the user chose "ROTATE LEFT" button and chose number "3" from dropdown list, then the pass characters will rotate three times anti-clockwise(i.e from blue to black in the fig. which is given below). Let i = 1.

Step 3: The user should rotate the sector containing the i-th pass-character of his password P, denoted by Pi, into his pass-color sector, and then clicks the "Conform" button. Let i = i + 1.

Step 4: If i < LN, the system permutes all the displayed pass characters randomly, and then GOTOs Step 3. Otherwise, the user should click the "Login" button to finish the login process.

If the account is not authenticated successfully for three consecutive times, it will be disabled. Then the system will send an e-mail containing the secret link that can be used by the legitimate user to re-enable his disabled account, to the user's registered e-mail address.

V.POSSIBLE FUTURE WORK

In future, the geo captcha technique may be merged with authentication. By that the user should choose some three location from a map while registering. During the login phase, the user should point three locations i.e drawing a triangle from the map(provided by the system). Along with that one time password can also be generated and the user will receive that in their mail, to login.

VI.CONCLUSION

In this paper, we have proposed a simple shoulder surfing resistant graphical password which is text-based, in which the user can simply and efficiently complete the login process without bothering about shoulder surfing attacks. The operation of the proposed method is simple and easy to understand for users those who are familiar with textual passwords. The user can efficiently login the system without any physical keyboard or on-screen keyboard. Finally, we have analyzed the resistance of the proposed scheme to accidental login and shoulder surfing.

ACKNOWLEDGMENT

I am grateful to the principal and management of SRM University for extending all the facilities and constant encouragement for carrying out this work. Also heartily thank Dr. Mukesh Krishnan M.B for giving me an opportunity to complete this research. You have been a tremendous mentor for me. I would like to thank you for encouraging my research. Your advice on both research as well as on my career have been priceless.

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.

[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. 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.

[8] 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.

[9] B. R. Cheng, W. C. Ku, and W. P. Chen, "An efficient login-recording attack resistant graphical password scheme — SectorLogin," Proc. of 2010 Conf. on Innovative Applications of Information Security Technology, Dec. 2010, pp. 204-210.

[10] 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.

[11] 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.

[12] Z. Imran and R. Nizami, "Advance secure login," International Journal of Scientific and Research Publications, vol. 1, Dec. 2011.

[13] 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 .

[14] Network Working Group of the IETF, "The Secure Sockets Layer (SSL) Protocol Version 3.0," RFC 6101, 2011.

[15] Network Working Group of the IETF, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, 2008.