www.redpel.com
+917620593389

A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme

Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao
Department of Computer Science, National Taichung University of Education, Taiwan
* Email: wcku@mail.ntcu.edu.tw

Abstract

Since conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. However, as most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password schemes have been proposed. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Next, we analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login.

I. Introduction

The shoulder surfing attack in an attack that can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he enters his password. As conventional password schemes are vulnerable to shoulder surfing, Sobrado and Birget [1] 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., [2][3][4][5][6][7][8][9], and each has its pros and cons.

Seeing that most users are more familiar with textual passwords than pure graphical passwords, Zhao et al. [10] 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, e.g., [11][12][13][14][15]. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, we will propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard. The rest of this paper is organized as follows. In Sec. II, we will review related works. In Sec. III, we will describe the proposed scheme. Next, we will analyze the security and usability of the proposed scheme in Sec. IV. Finally, conclusions are made in Sec. V.

This work was supported in part by the National Science Council, Taiwan, under Grant NSC-101-2221-E-142-007.

II. Related Works

In 2002, Sobrado and Birget [1] proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme. However, both the Movable Frame scheme and the Intersection scheme have high failure rate. In the Triangle scheme, the user has to choose and memorize several pass-icons as his password. To login the system, the user has to correctly pass the predetermined number of challenges. In each challenge, the user has to find three pass-icons among 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, Wiedenbeck et al. [3] proposed the Convex Hull Click Scheme (CHC) as an improved version of the Triangle scheme with superior security and usability. To login the system, the user has to correctly respond several challenges. 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. However, the login time of Convex-Hull Click scheme may be too long. In 2009, Gao et al. [4] proposed a shoulder surfing resistant graphical password scheme, ColorLogin, in which the background color is a usable factor for reducing the login time. However, the probability of accidental login of ColorLogin is too high and the password space is too small. In 2009, Yamamoto et al. [9] proposed 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. Unfortunately, TI-IBA's resistance to accidental login is not strong. And, 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, Zhao et al. [10], in 2007, proposed a text-based shoulder surfing resistant graphical password scheme, S3PAS, in which the user has to find his textual password and then follow

www.redpel.com
+917620593389

a special rule to mix his textual password to get a session password to login the system. However, the login process of Zhao et al.'s scheme is complex and tedious. In 2011, Sreelatha et al. [12] also proposed a text-based shoulder surfing resistant graphical password scheme by using colors. Clearly, as the user has to additionally memorize the order of several colors, the memory burden of the user is high. In the same year, Kim et al. [13] proposed a text-based shoulder surfing resistant graphical password scheme, and employed an analysis method for accidental login resistance and shoulder surfing resistance to analyze the security of their scheme. Unfortunately, the resistance of Kim et al.'s scheme to accidental login is not satisfactory. In 2012, Rao et al. [15] proposed a text-based shoulder surfing resistant graphical password scheme, PPC. 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. THE PROPOSED SCHEME

In this section, we will describe a simple and efficient shoulder surfing resistant graphical password scheme based on texts and colors. The alphabet used in the propose scheme contains 64 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols "." and "/". The proposed scheme involves two phases, the registration phase and the login phase, which can be described as in the following.

A. Registration phase

The user has to set his textual password K of length L ($8 \le L \le 15$) characters, and choose one color as his pass-color from 8 colors assigned by the system. The remaining 7 colors not chosen by the user are his decoy-colors. And, the user has to register an e-mail address for re-enabling his disabled account. The registration phase should proceed 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 [16][17] or any other secure transmission mechanism. The system stores the user's textual password in the user's entry in the password table, which should be encrypted by the system key.

B. Login phase

The user requests to login the system, and the system displays a circle composed of 8 equally sized sectors. The colors of the arcs of the 8 sectors are different, and each sector is identified by the color of its arc, e.g., the red sector is the sector of red arc. Initially, 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 counterclockwise by clicking the "counterclockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel. The login screen of the proposed scheme can be illustrated by an example shown in Fig. 1. To login the system, the user has to finish the following steps:

Step 1: The user requests to login the system.

Step 2: The system displays a circle composed of 8 equally sized sectors, and places 64 characters among the 8 sectors averagely and randomly so that each sector contains 8 characters. The 64 characters are in three typefaces in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the two symbols "." and "/" are in regular typeface, and the 10 decimal digits are in italic typeface. In addition, the button for rotating clockwise, the button for rotating counterclockwise, the "Confirm" button, and the "Login" button are also displayed on the login screen. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counterclockwise by clicking the "counterclockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel. Let i = 1. The rotation operation can be illustrated by an example shown in Fig. 2.

Step 3: The user has to rotate the sector containing the i-th pass-character of his password K, denoted by K_i, into his pass-color sector, and then clicks the "Confirm" button. Let i = i + 1.

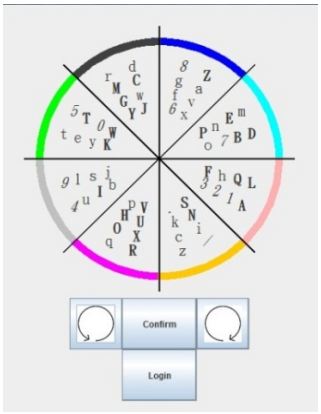

Fig. 1: An example of the login screen.

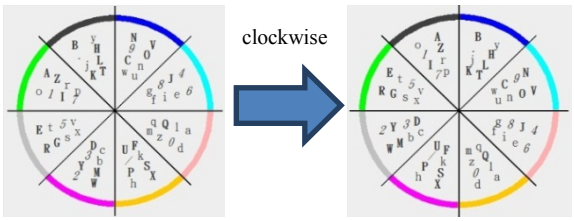

Fig. 2: An example of the rotation operation.

www.redpel.com
+917620593389

Step 4: If i < L, the system randomly permutes all the 64 displayed characters, and then GOTOs Step 3. Otherwise, the user has to click the "Login" button to complete the login process.

If the account is not successfully 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 legitimate user to re-enable his disabled account. The login process of the proposed scheme can be illustrated by an example shown in Fig. 3. The user has to rotate the sector (marked with orange dotted line for illustration only) containing K_i (marked with small red circle for illustration only) into his pass-color sector (marked with brown dotted line for illustration).

Fig. 3: An example of rotating the sector containing K_i into the pass-color sector.

IV. Analysis

The security and the usability of the proposed scheme are analyzed in this section.

A. Password space

The total number of all possible passwords with length L is 8×64^L. Therefore, the password space of the proposed scheme is

$$\sum_{L=8}^{15} 8 \times 64^L \approx 1.006 \times 10^{28}$$

B. Resistance to accidental login

Since the probability of correctly responding to K_i is 8/64, i.e., 1/8, the success probability of accidental login with the password with length L, denote by $P_{al(L)}$, is

$$P_{al(L)} = \left(\frac{1}{8}\right)^L$$

For example, if L = 10, then

$$P_{al(10)} = \left(\frac{1}{8}\right)^{10} \approx 9.31 \times 10^{-10}$$

Fig. 4 shows the $P_{al(L)}$ for different values of L. However, since the password length is a secret, the adversary has to guess the password length first. As the probability distribution of the lengths of the passwords to be used is

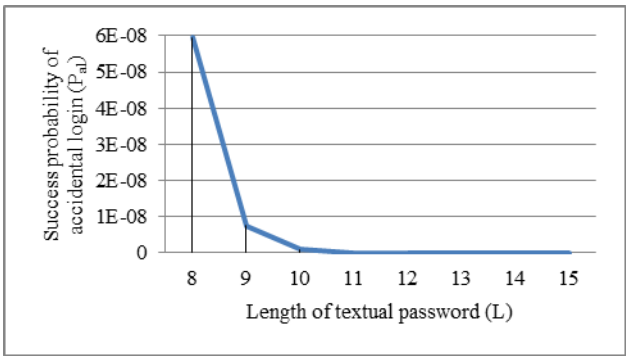

Fig. 4: The success probability of accidental login for different values of L.

assumed uniform between 8 and 15, the probability that the adversary correctly guesses the password length is 1/8. Thus, the probability of accidental login for the proposed scheme is

$$P_{al} = \frac{1}{8} \times \sum_{L=8}^{15} P_{al(L)}$$

In addition, if the attacker fails to login system consecutively for three 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 legitimate user to re-enable his disabled account. That is, only the legitimate user can re-enabled his disabled account. Thus, accidental login cannot be performed easily and efficiently.

C. Resistance to shoulder surfing

If the adversary has recorded the login process T times, he can eliminate some combinations of the characters in guessing the pass-characters by using the recorded login information. The success probability of the same character among the same sector, denoted by P_{rp}, is

$$P_{rp} = 1 - \frac{C_8^{56}}{C_8^{64}}$$

The success possibility of shoulder surfing, denoted by P_{ss}, is

$$P_{ss} = P_{pass-color} \times P_{password}$$

where

$$P_{pass-color} = \frac{1}{1 + (P_{rp}{}^L)^{(T-1)} \times 7}$$

$$P_{password} = \frac{1}{1 + \left(\frac{7}{63}\right)^{(T-1)} \times 7}$$

Notation $P_{pass-color}$ represents the success probability of cracking the user's pass-color of shoulder surfing. The number of candidate colors is 8, including 1 pass-color and 7 decoy-colors. Since the length of the password is L and the number of decoy-colors is 7, the expectation of the number of the candidate pass-color of the T recorded login process is $\left(1 + (P_{rp}{}^L)^{(T-1)} \times 7\right)$. Notation $P_{password}$ represents the success probability of cracking the user's pass-color of shoulder surfing. The number of candidate

978-1-978-1-4673-3037-4/13/$31.00 ©2013 IEEE

www.redpel.com
+917620593389

characters within the pass-color sector is 8, including 1 pass-character and 7 decoy characters selected form the 63 non-pass-characters. The probability that any decoy character within the pass-color sector in the first login process also appears in the pass-color sector of each of the other T−1 login processes is $(7/63)^{(T-1)}$. Since there are 7 decoy characters within the pass-color sector, the expectation of the number of the common candidate characters in the pass-color sector is $(7/63)^{(T-1)}\times 7$. Fig. 5 shows the success probabilities P_{ss} of shoulder surfing for the number of recorded login processes and different values of L. Clearly, the proposed scheme can resist the shoulder surfing with at least two recorded login processes.

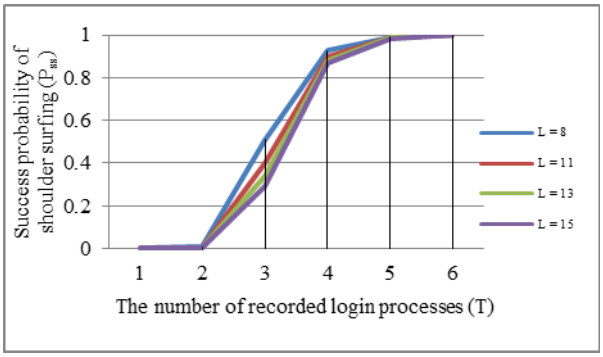

Fig. 5: The success probability of shoulder surfing for T times login process records and different values of L.

D. Usability

The user chooses traditional textual passwords and one color as his password in the proposed scheme. As most users are familiar with textual passwords, it is usually easier for the user to find characters than icons on the login screen. In addition, since the system displays the upper case letters, the lower case letters, the symbols "." and "/", and the 10 decimal digits in three different typefaces on the login screen, the user can easily and efficiently find his pass-characters. And, the operation of the proposed scheme is simple and easy to learn, the user only has to rotate the sectors to login the system.

V. Conclusions

In this paper, we have proposed a simple text-based shoulder surfing resistant graphical password, in which the user can easily and efficiently complete the login process without worrying about shoulder surfing attacks. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system without using any physical keyboard or on-screen 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 shoulder-surfing-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 — SectorLogin," *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] Network Working Group of the IETF, "The Secure Sockets Layer (SSL) Protocol Version 3.0," *RFC 6101*, 2011.

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

www.redpel.com
+917620593389