ISSN No. 0976-5697

Volume 5, No. 8, Nov-Dec 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Shoulder Surfing and Keylogger Resistant using Graphical Password Scheme

Prof Raut S.Y.
Pravara Rural Engineering College, Loni
Ahmednagar, India

Jayesh Bhaskar Baviskar
Jalgaon, India

Kharde Rahul S
Pravara Rural Engineering College, Loni
Ahmednagar, India

Shrishrimal Aditya N
Pravara Rural Engineering College, Loni
Ahmednagar, India

Shelke Yogesh S
Pravara Rural Engineering College, Loni
Ahmednagar, India

Abstract: When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual's authentication session. This is referred to as shoulder-surfing and is a known risk, of special concern when authenticating in public places. Attacker can also use various keylogger tools which are freely available over internet. This paper reports on the design and evaluation of a game-like graphical method of authentication that is resistant to shoulder-surfing. 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.

Keywords: Shoulder surfing, Authentication Scheme, Passwords, Graphical Authentication, password Attack.

I. INTRODUCTION

Today, password is the most popular way to authenticate a user to login to computer systems. However, we all know that traditional text-based password systems are vulnerable to the shoulder- surfing attack. Through this paper we use the word "shoulder-surfing" in the following sense: A shoulder-surfing attack consists of a user being filmed during his/her login.

To protect customers' passwords, E-commerce vendors adopted various encryption techniques. Text passwords are encrypted before they were sent across networks. A wire-tapping attacker cannot capture the passwords unless they have enough computing power and advanced decryption techniques. However, with a camcorder aiming at the screen of a computer and its keyboard, traditional text-based passwords will be captured with 100% accuracy.

Seeing that most users are more familiar with textual passwords than pure graphical passwords, Zhao et al. [1] 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., [2][3][4][5][6][7]. 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.

II. SHOULDER-SURFING PROBLEM AND DEFENSES

Shoulder-surfing occurs when an attacker learns a user's password by watching the user log in. Shoulder-surfing is a well-known method of stealing passwords and other sensitive information and is recognized by practitioners as a serious security threat. It can occur in offices and public places without the user's awareness. In the simplest version of shoulder-surfing a human attacker takes up a position where a user's login can be seen. Typically this might occur at a wireless hotspot in a busy, crowded public environment, such as a shopping mall, airport, or coffee shop. Using an alphanumeric password, though the user's password is not displayed on the screen, a practiced attacker can "read" the user's keystrokes as the user types the password. The user's only defense is to shield the keyboard with an object or one's body. Using a graphical password, the user would have to shield the screen. The same considerations apply to entering PINs at ATMs. High tech versions of shoulder-surfing are also a threat, although it is not known how prevalent the threat is. Technology-based

attacks include using binoculars or a low power telescope to enhance vision, using video cameras, video mobile phones, keystroke logging software, or Trojan software to record a login, and listening to a user input a PIN or account number on a telephone keypad. Remote electro-magnetic sensors can also be used to capture actions without the user's knowledge.

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 ($8 \leq L \leq 15$) 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 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 sections of the 8 sectors are different, and each sector is identified by the color of its section, e.g., the red sector is the sector of red section. Initially, 64 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated clockwise. 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 is rotated along the adjacent sector clockwise. 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 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.

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).

Figure 1 : Login Screen

Figure 2 : Rotation Screen

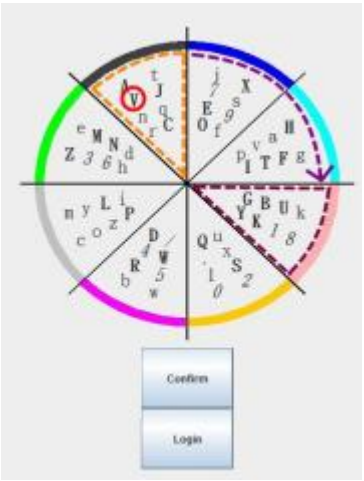

Figure 3: Rotation of Sectors

IV. SECURITY

We consider a shoulder-surfing attack, in which a user's login has been filmed s times by an attacker. In other words, the attacker clearly knows s strings that can possibly be used for the password. The total number of all possible passwords with length L is 8 X 64. Therefore, the password space of the proposed scheme is

$$\sum_{i=8}^{15} 8X\ 64 \approx 1.006\ X\ 10$$

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 $Pa_{l(L)}$, is

$$\mathrm{Pal}(L) = \left(\frac{1}{8}\right)^{L}$$

For example, if L = 10, then

$$\mathrm{Pal}(10) = \left(\frac{1}{8}\right)^{10} \approx 9.31\ \mathrm{X}\ 10^{-10}$$

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 the adversary correctly guesses the password length is 1/8. 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. 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

$$P_{rp} = 1 - \left(\frac{C_8^{56}}{C_8^{64}}\right)$$

Notation password represents the success probability of cracking the user's pass-color of shoulder surfing. 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.

V. CONCLUSION

To have a good system high security and good usability are both needed and cannot be separated. Shoulder surfing attack is under security provision. There are few proposed methods to shoulder surfing problem but they still need to be improved 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.

VI. ACKNOWLEDGMENT

We would like to express our appreciation to our parents, all the teachers and lecturers who help us to understand the importance of knowledge and show us the best way to gain it.

VII. REFERENCES.

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

[6] M. K. Rao and S. Yalamanchili. "Novel shoulder-surfing resistant authentication schemes using text-graphical

[7] passwords," International Journal of Information & Network Security, vol. 1, no. 3, pp. 163-170, Aug. 2012 .

[8] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[9] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[10] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[11] K. Elissa, "Title of paper if known," unpublished.

[12] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[13] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[14] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[15] Electronic Publication: Digital Object Identifiers (DOIs):

[16] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467.

[17] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.