SECURE GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Rajguru Dipali[1], J Walunj Jyoti [2], Jadhav Jayashree [3], HandeReshma [4]

[1] *Computer Engineering, SGOI COE, Maharastra, India*
[2] *Computer Engineering, SGOI COE, Maharastra, India*
[3] *Computer Engineering, SGOI COE, Maharastra, India*
[4] *Computer Engineering, SGOI COE, Maharastra, India*

ABSTRACT

Conventional password schemes like as textual password scheme, graphical scheme are commonly used for authentication. But also these schemes are vulnerable to dictionary attack, shoulder surfing attack, accidental login. Hence the secure graphical password authentication system have been proposed. These existing schemes are not secure and efficient enough and have high failure rate. The secure graphical password authentication system is amend by using colors. So it has become more safe. User can motile login to the system. Unauthorized user cannot get the password easily. Hence this scheme supply protection against the shoulder surfing.

Keyword : *Dictionary attack, shoulder surfing attack, accidental login, textual password scheme, graphical scheme, vulnerable.*

1. INTRODUCTION

The shoulder surfing attack is an attack that can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he/she enters his/her password. As conventional password plan are vulnerable to shoulder surfing, Birget[1] as well as Sobrado proposed three shoulder surfing resistant graphical password schemes. Since then, many graphical password plans with different degrees of resistance to shoulder surfing have been proposed, and each has its pros and cons. Seeing that Unique that most of the users are more well known with textual password for user than pure graphical passwords, Zhao et al. [10]

proposed a secure graphical password authentication system, S3APS. In S3PAS, the user has to mix his textual the login screen on password to get the session password. However, the login process of Zhao et al.'s plan is tedious and hard . And then, several secure graphical password authentication systems have been proposed, Unfortunately, none of existing secure graphical password authentication systems is both efficient and secure enough. In this system, we will propose an improved secure graphical password authentication systems by using colors. The operation of the proposed scheme is easy and simple to learn for users familiar with textual passwords. The user can easily and efficiently login to the system without using any on-screen keyboard or physical keyboard. The rest of this paper is arranged as follows. In Sec. II, we will review literature survey works. In Sec. III, we will describe the proposed system. Next, we will analyze the security and system architecture of the proposed scheme in Sec. IV. Finally, we concluded in Sec. V.

2. LITURATURE SURVEY

In 2002, Birget as well as Sobrado proposed three shoulder surfing resistant graphical password schemes, the Movable Intersection scheme, the Frame 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 memorize and to

choose several pass-icons as his/her password. In every time whenever login 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. proposed the Convex Hull Click 1Scheme as an improved version of the Triangle scheme with superior usability as well as security. 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 and more tedious. In 2009, Gao et al proposed a secure graphical password authentication scheme, Color Login, in which the background color is a usable factor for reducing the login time. However, the password space is too small and probability of accidental login of Color Login is too high. As most users are familiar with textual passwords as well the conventional textual password authentication schemes have no shoulder surfing resistance, Zhao et al. in 2007, proposed a secure graphical password authentication system, S3PAS, in which the user has to find his textual password and also then follow 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 tedious and complex . In 2011, Sreelatha et al. also proposed a secure graphical password authentication system 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 2012, Rao et al. proposed a secure graphical password authentication system, PPC. To login the system, the user has to mix his/her textual password to produce several pass-pairs, and then follow four predefined rules to get his/her session password on the login screen. However, the login process of PPC is too complicated and tedious.

3. PROPOSED SYSTEM

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

3.1 *Registration Phase*

The user has to set his/her textual password K of length is L($8 \leq L \leq 15$) characters, and then choose one color as his pass color from 8 colors assigned by the system. The remaining 7 colors not selecting by the user are his bait colors. And, the user has to note an e-mail address for re-enabling his/her disabled account. The registration stage should proceed in an environment free of shoulder surfing. In addition, a secure channel should be created between the system and any other secure transmission mechanism or the user during the registration phase by using SSL/TLS [16][17]. the system accumulation the user's textual password in the user's entry in the password scheme, which should be decoded by the system key.

3.2 *Login Phase*

The user requests to login the system, and the system displays a circle designed of 8 equally sized sectors. The colors of the arcs of the 8 sectors are separated, and each area is identified by the color of its arc, e.g. the red area is the area of red arc. Initially, 64 characters are placed randomly and averagely among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector counterclockwise by clicking the "counter clockwise" button once or, the adjacent sector clockwise by clicking the "clockwise" button once and the rotation operations can also be performed by the scrolling the mouse wheel. The login screen of the proposed scheme,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 designed of 8 equally sized sectors, and places 64 characters among the 8 sectors randomly and averagely so that each sector contains 8 characters. The64 characters are in three typefaces in that the26 lower case letters ,the26 upper case letters are in bold typeface and the 10 decimal digits are in italic typefaceand the two symbols "." and "/" are in regular typeface. In addition, the button for rotating

counterclockwise, the button for rotating clockwise, 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 counterclockwise by clicking the "counterclockwise" button once,or the adjacent sector clockwise by clicking the "clockwise" button once and the rotation operations can also be performed by scrolling the mouse wheel .

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

Step 4: If i < L, the system randomly permutes all the64 displayed characters, and then GOTOs Step 3. Otherwise, the user has to click the "Login" button to absolute the login process.

ADVANTAGE-The operation of the proposed plan is simple and easy to learn for users well known with textual passwords. The user can easily and efficiently login to the systemwithout using any on-screen keyboard or physical keyboard.

4. SYSTEM ARCHITECTURE

Fig -1: system architecture for ATM system.

5. ANALYSIS

In this section we described analysis of our project. The security and the usability of more important part of system this is analyzed in this section for our project.

5.1 Password space

The total number of all possible passwords with length L is 8 *64^l. Therefore, the password space of our project is

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

5.2 Resistance to accidental login

Our system is more resistance of accidental login Since the probability of correctly responding to password (Ki) is 8/64, that is 1/8, the success probability of accidental login

with the password (ki) with length L, denote by Pal(L), is

Pal(L)=(1/8)^L

since the password length is a more secret, if hacker's want to hack the system he first of all guess the user password then he try to hack but as the probability distribution of the lengths of the passwords to be used is assumed uniform between 8 and 15, the probability that the hacker correctly guesses the password length is 1/8.

Thus, the probability of accidental login for the our project is

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

And if the attacker fails to login system consecutively for three times, then this account will be disabled and the system will send to the user's registered re-enter e-mail address and 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 user can re-enabled his disabled account. Thus, accidental login cannot be performed easily and efficiently is to be complicated.

6. USABILITY

The user chooses traditional textual passwords and one color as her password in the registration screen . As most users are familiar with textual passwords, it is usually easier for the user to find characters than icons on the login screen. since the system displays the upper case letters, the lower case letters, the symbols and the 10 decimal digits in three different typefaces and color on the login screen, the user can easily and efficiently find her pass-characters from login screen. 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

7. RESULT

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 Prp, is

The success possibility of shoulder surfing, denoted by Pss , is P_{rp} =1-$\frac{C_8^5 6}{C_8^6 4}$

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

Where

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

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

Notation Ppass-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 $(1 + (P_{rp}{}^{L})^{(T-1)} \times 7)$.Notation Ppassword represents the success probability of cracking the user's pass-color of shoulder surfing. Fig. 5

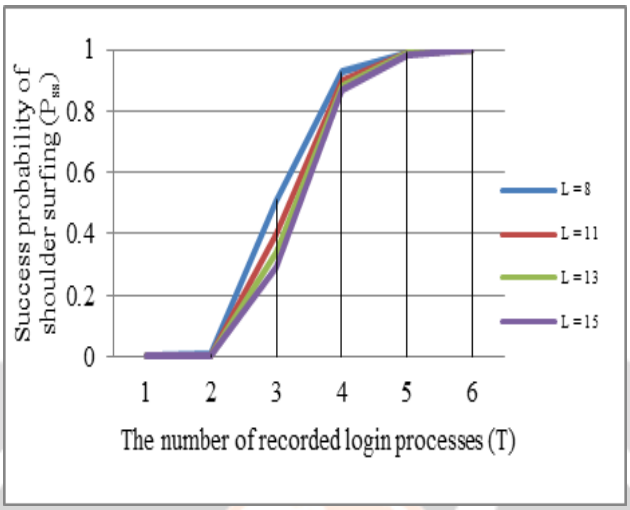

Fig -2: The success probability of shoulder surfing for T times login process records and different values of L.

shows the success probabilities Pss 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.

8. CONCLUSIONS

We have proposed at secure graphical password authentication system, 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 well known with textual passwords. The user can efficiently and easily to login the system without using any on-screen keyboard or physical keyboard. Finally, we have analyzed the resistances of the proposed scheme to shoulder surfing and accidental login.

9. ACKNOWLEDGEMENT

We offer special thanks to the Prof. M. R. Shimpi who have guided towards development of our system paper. Also thanks all who helped in the development of system and giving their valuable suggestions. So that we are able to improve our system.

10. REFERENCES

[1]. L. Sobrado and J. C.Birget,"Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[2]. Leonardo Sobrado , Jean-Camille, Birget, "Graphical passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4 2002.

[3]. L. Sobrado and J. C. Birget, The Rutgers Scholar, an Electronic Bulletin for Undergraduate Research, vol.4,2002.

[4]. S. Man, D. Hong, and M. Mathews, Proc. of the 2003 Int. Conf. on Security and Management, June 2003,pp. 105-111 .

[5]. 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 .

[6]. Shushuang Man, Dawei Hong, Manton Mathews, "A shoulder surfing resistant graphical password scheme", in Proceedings of International conference on security and management, Las Vegas,NV,2003.

[7]. Xiaoyuan Suo, Ying Zhu, G. Scott. "Graphical passwords: a survey", Computer Security Applications Conference,21st Annual Owen 2005.

[8]. L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005. (http://clam.rutgers.edu/ birget/gr Pssw/srgp.pdf)

[9]. 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.

[10]. S.Wiedenbeck,J.Waters, L. Sobrado, and J. C. Birget, Proc. Of Working Conf. on Advanced Visual Interfaces,May.2006,pp. 177-184.

[11]. SusanWiedenbeck, JimWaters, Leonardo Sobrado, Jean-Camille Birget,”Design and evaluation of a shoulder-surfing resistant graphical password scheme”, Proceedings of Advanced Visual Interfaces ,2006. SGOI COE, Department of Computer Engineering 2015-16 53

[12]. Huanyu Zhao and Xiaolin Li”S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme”21st International Conference on Advanced Information Networking and Applications Workshops (AINAW’07) 0-7695-2847-3/07 2007.

[13]. 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.

[14]. Di Lin, Paul Dunphy, Patrick Olivier, Jeff Yan, ”Graphical passwords and qualitative spatial relations”, Proceedings of the 3rd symposium on Usable privacy and security, ACM, Pittsburgh,Pennsylvania 2007.

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

[16]. Eljetlawi,A.M. and Ithnin, ”Graphical password: comprehensive study of the usability features of the recognition base graphical password methods”, Third International Conference on Convergence and Hybrid Information Technology (ICCIT ’08) ,NV,2008.

[17]. Peipei Shi, Bo Zhu, and Amr Youssef ”A PIN Entry Scheme Resistant to Recording-based Shoulder-Surfing” Third International Conference on Emerging Security Information, Systems and Technologies,2009.

[18]. H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, Proc. of 4th Int. Conf. on Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.

[19]. HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu ”A New Graphical Password Scheme Resistant to Shoulder-Surfing” 2010 International Conference on Cyberworlds.

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

[21]. 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.

[22]. 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 and Its Applications,vol.3,no.3,May 2011.

[23]. 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.

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