Graphical Gauze to Resisting Impersonation

Mr. Avinash V. Sabale

Department of Computer Engineering.
G.H.Raisoni College of Engineering and Management, Ahmednagar.

Abstract

Currently predictablesecret wordpatterns are susceptible to dictionary attacks, eves dropping and shoulder surfing,numerous shoulder surfing unaffected graphical password patterns proposed. On the other hand, Textual passwords are the utmostpublictechnique used for authentication. There are several graphical password schemes that are planned in the pastyears. A maximum users areused word-based passwords than untainted graphical passwords, word-based or character based graphical password schemes have been proposed.Regrettably, none of existing schemes are create a graphical gauze to resisting the impersonation. In this paper, we propose an improved mainly text-based or character based shoulder surfing resistant and other attacks like eves dropping, dictionary attacks, and social engineeringresistant graphical gauze by using colors. In the projected scheme, the operator can strongly, simply and professionally login system andexamine the security and usability of the plannedsystem and show the resistance of the proposed scheme to unintended login.

Index Terms: Authentication, shoulder surfing, Gauze, Impersonation.

I. INTRODUCTION

The most common technique used for authentication is textual password. The weaknesses of this techniquesimilar eves dropping, social engineering,dictionary attack and shoulder surfing are well-known. Unexpected and long passwords can make the system secure. On the other hand the main problem is the trouble of memorizing those passwords. Studies have exposed that users have a tendency tochoicesmall passwords or passwords that are stress-free to recall. Unluckily, these passwords can be easily predicted or cracked. The differentmethods are graphical passwords and biometrics. On the other hand these methods have their particular disadvantages. In Biometricspassword techniques suchas facial recognition, finger printsetc. have been presented but not yet commonly adopted. The maindisadvantage of this method is that such systems can be costly and the identification procedure can be slow. There are numerous graphical password methods that are planned in the pastyears. On the other handmost methods are suffer from shoulder surfing attack which is becoming somewhat a large problem. There are graphical passwords patterns that have been projected which are resistant to shoulder-surfing on the other hand they have their particularweaknesses like usability problems or takes more time for login or it has tolerance levels.The shoulder surfing attack in an attack that can be did by the opponent to get the user's password by observingabove the user's shoulder as he enters his password. From the timenumerous graphical password methods with different degrees of resistance to shoulder surfing hasprojected, e.g., [2] [3] [4] [5][6][7][8][9], and each has its pros and cons. As predictable password schemes are susceptible to shoulder surfing, Sobrado and Birget [1] proposed three shoulder surfing resistant graphical password methods.

Seeing that maximum users are more used text-based passwords than graphical passwords, Zhao et al. [10] proposed a text-based shoulder surfing resistant graphical password methods, S3APS. In S3PAS, the user has to fusion his textual password on the login screen to catch the session password. However, the login procedure of Zhao et al.'s methods is difficult and boring. And then, a number oftext-based shoulder surfing resistant graphical password methods have been proposed, such as [11][12][13][14][15]. Regrettably, none of present text-based shoulder surfing resistant graphical password schemes is both safe and effectualsufficient. In this paper, we will suggestabetter text-based shoulder surfing resistant graphical password structure by with colors. The process of the proposed methods is easy and simple to study for users aware with word-based passwords. The user can effortlessly and professionally to login the system without using any physical keyboard.

RELATED WORKS

Perrigand Dhamija[2] proposed a graphical authentication methods where the user has to recognize the pre-defined images to verify user's authenticity. In this scheme, the user chooses a number of images from a group of random images during registration. After, during login the user has to recognize the previously selected images for authentication from a group of images as shown in figure 1. This methods is vulnerable to shoulder-surfing. In 2002, Sobrado and Birget [1] proposed three shoulder surfing resistant graphical password schemes, the Intersection methods, the Movable Frame methods, and the Triangle methods. However, both the Movable Frame methods and the Intersection methods have high failure rate. In the triangle methods, the user has to choose and remembermore than a few pass-icons as his password. To login the system, the user has to properly pass the predetermined number of challenges. In every challenge, the user has to find three pass-icons among a set of randomly selected icons displayed on the login screen, and

ISSN: 2278 – 7798

then click inside the invisible triangle created by those three pass-icons.

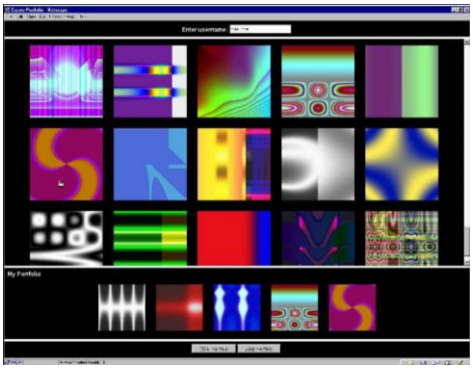

Figure 1: Random images used by Dhamija and Perrig

Wiedenbeck et al. [3] proposed in 2006, the Convex Hull Click Scheme (CHC) as abetter version of the Triangle scheme with greater security and usability. To login the system, the user has to properly respond some 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 designed by all the showed pass-icons. But, 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, Color Login, in which the background color is a usable issue for decreasing the login time. Still, the possibility 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. Unluckily, TI-IBA's resistance to accidental login is not strong. And, it may be problematic for some users to find his pass-icons temporally displayed on the login display.

As maximum users are aware with word-based passwords and conventional text-based password authentication schemes have no shoulder surfing resistance. In 2007, Zhao et al. [10] proposed a text-based shoulder surfing resistant graphical password scheme, S3PAS, in which the user has to discover his textual password and then follow a special rule tomix his textual password to catch a session password to login the system. On the other hand, the login procedure of Zhao et al.'s methods is difficult and boring. Sreelatha et al. [12],in 2011, also proposed a text-based shoulder surfing resistant graphical password scheme by using colors. Clearly, as the user has to in additionremember the order of some colors, the memory load of the user is high. In the similar 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. Unluckily, the resistance of Kim et al.'s scheme to accidental login is not acceptable. Rao et al. [15], in 2012,suggested 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. On the other hand, the login procedure of PPC is too complex and boring.

User should rate colors during registration as shown in figure 2. The User should rate colors from 1 to 8 and he can recall it as "RLYOBGIP". Identical rating can be given to dissimilar colors. During the login phase, when the user write or enter his username a one interface is showed based on the colors designated by the user. The login interface consists of grid of size 8×8. This grid encloses digits 1-8 placed randomly in grid cells. The interface also contains strips of colors. The color grid contains of four pairs of colors. Each pair of color denotes the row and the column of the grid.

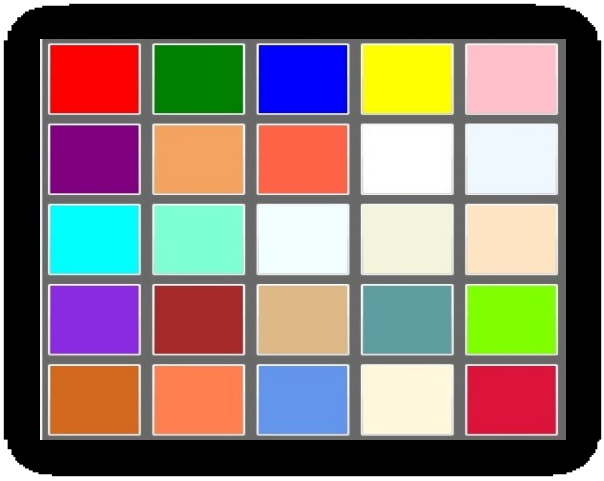

Fig 2 Hybrid color grid

Haichang et al [19] proposed a shoulder-surfing resistant scheme where the user is essential to draw a curve through their password images orderly rather than ticking on them directly. This graphical method combines Story and DAS method to deliver authenticity to the user. Syukri [20] proposed a methods where authentication is done by sketch user signature using a mouse.This technique involved two phases, verificationand registration. At the time of registration phase the user draws his signature with the help of mouse, afterward that the system extracts the signature zone. Then in verification phasetakings the user signature as input and fixes the standardization and then excerpts the parameters of the signature. The drawback of this method is the forgery of the signatures. Is not shoulder surfing resistance.

II. THE PROPOSED SCHEME

In this section, we will describe a simple and efficient shoulder surfing resistant graphical password scheme based on colors and texts. The letters used in the propose scheme contains 64 characters, containing 26 lower case letters,26 upper case letters,symbols "." and "/" and 10

ISSN: 2278 – 7798

decimal digits. The proposed scheme includes two stages, the registration stage and the login stage, which can be designated as in the following.

Stage 1:- Registration

The user has to set his textual password K of length L characters, and select one color as his passcolor from colorsallocated by the system. The remaining colors not selected by the user are his decoycolors. And, the user has to register an e-mail address for re-enabling his inactivated account. The registration stage should continue in asituation free of shoulder surfing. In addition, a protected channel should be established between the user and the system during the registration stage by using SSL/TLS [16][17] or any additionalsafebroadcast mechanism. The system stores the user's textual password in the user's entry in the password table that should be encrypted by the system encryption key.

Stage 2:- Login stage

The user wishes to login the system, and the system shows a circle composed of equally sized subdivisions. The colors of the curves of the subdivisions are dissimilar, and each subdivision is recognized by the color of its arc, e.g., the bluesubdivision is the subdivision of blue arc. Firstly, characters are positioned randomly and averagelybetween these sectors. All the showed characters can be concurrentlyswitched into either the neighboring sector right-handedor clockwise by ticking the "clockwise" keyor button once or the adjacent sector anticlockwise or counterclockwise by clicking the "counterclockwise" key or button once, and the rotation operations can also be did by scrolling the mouse wheel. The login screen of the proposed scheme can be demonstrated by an example as following.

The user wishes to login the system.

The system shows a circle composed of sixteen equally sized segments, and places sixty four characters between the sixteen sectors averagely and randomly so that each segmentcoverssixteen characters. The sixtyfour characters are in three typefaces in that the twenty six upper case letters are in bold typeface, the twenty six lower case letters and the two symbols "." and "/" are in regular typeface, and the ten decimal digits are in italic typeface. In addition, the button or key for rotating anticlockwise, the button for rotating clockwise, the "Confirm" button, and the "Login" button are also showed on the login screen. All the shown characters can be simultaneously rotated into either the neighboringregionanticlockwise by clicking the "anticlockwise" button once or the neighboringregion clockwise by clicking the "clockwise" button once, and the rotation procedures can also be done by scrolling the mouse wheel. Let i = 1. The rotation operation can be illustrated. 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 region, and then ticks the "Confirm" button. Let i = i + 1.

If i< L, the system randomly permutes all the sixty four shown characters, and then again.Or else, the user has to click the "Login" key to complete the login procedure.

If the account is not successfully authenticated for three successive times, this account will be inactivated and the system will send to the user's registered e-mail address an e-mail having the secret link that can be used by the valid user to re-enable his inactivated account. The user has to rotate the region havingK_i into his pass-color sector.

IV. ANALYSIS

The security and the usability of the proposed system are examined in this section.

1 Password space

The total number of all possible passwords with length L is 16×64^L. Therefore, the password space of the proposed scheme is

$$\sum_{L=16} 16 \times 64\text{^}L$$

2 Accidental login resistance

Since the probability of correctly responding to K_i is 16/64, i.e., 1/16, the success probability of accidental login with the password with length L, denote by $P_{al\,(L)}$, is

$$P_{al\,(L)} \text{ ---- } \left(\frac{1}{16}\right)^L$$

For example, if L = 10, then

$$P_{al\,(10)} = \left(\frac{1}{16}\right)^{10}$$

Fig. 3 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

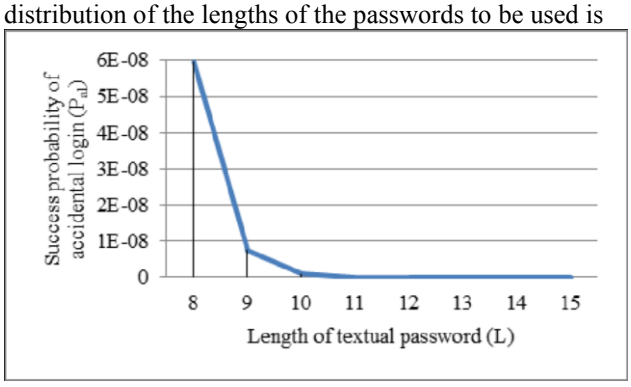

Fig. 3: The success probability of accidental login for different values of L.

Assumed uniform between 8 and 15, the probability that the adversary correctly guesses the password length is 1/16. Thus, the probability of accidental login for the proposed scheme is

ISSN: 2278 – 7798

$$P_{al} = \frac{1}{16} \times \sum_{L=16}^{15} P$$

In addition, if the attacker fails to login system consecutively for three times, this account will be inactivated and the system will send to the user's registered e-mail address an e-mail having the secret link that can be used by the legitimate user to re-enable his inactivated account. That is, only the legitimate user can reenabled his deactivated account. Thus, accidental login cannot be done easily and efficiently.

3. Shoulder surfing resistance

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

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

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

Notation $P_{pass\text{-}color}$ represents the success probability of cracking the user's pass-color of shoulder surfing. The number of candidate colors is 16, 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$1 \quad P^{L\,T} \; 7$.Notation $P_{password}$ represents the success probability of cracking the user's pass-color of shoulder surfing. The number of candidate characters within the pass-color sector is 16, 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. 4 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

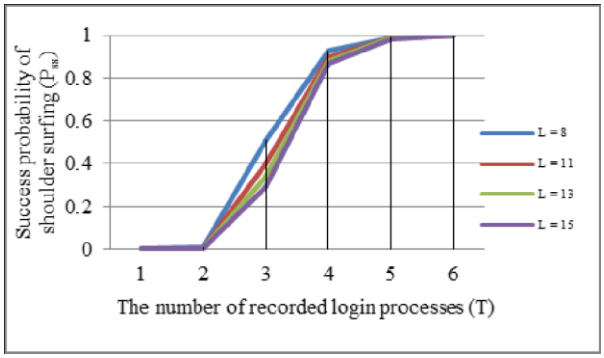

Fig. 4: The success probability of shoulder surfing for T times login process records and different values of L.

Processes.

4. Usability

The user chooses old-style textual passwords and one color as his password in the planned scheme. As maximum users are aware with textual passwords, it is usually easier for the user to find characters than icons on the login screen. In addition, since the system showsthe, the lower case letters ,upper case letters, the symbols "." and "/", and the ten decimal digits in three dissimilar typefaces on the login screen, the user can easily and efficiently find his pass-characters. And, the process of the proposed methods is easy and simple to learn, the user only has to rotate the segments 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 efficiently and easilywhole the login procedure without worrying about shoulder surfing attacks. The operation of the proposed scheme is easy andsimple to learn for users aware with text-based passwords. The user can efficiently and easily to login the system without using any virtual keyboard or physical keyboard. Finally, we have examined the proposed method resistances of shoulder surfing and accidental login. This text-based shoulder surfing scheme is used for authenticating the cloud with the help of this scheme we secure the cloud.

References

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

[2] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". *In 9th USENIX Security Symposium, 2000.*

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

[4] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant

ISSN: 2278 – 7798

graphical password scheme," *Proc. of Working Conf. on Advanced Visual Interfaces*, May. 2006, pp. 177-184.

[5] 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.

[6] 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.

[7] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," *Proc. of the 2003 Int. Conf. on Security and Managemen*t, June 2003, pp. 105111 .

[8] 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.

[9] 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.

[10] 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. 188194.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] 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 .

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

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

[19] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "*A New Graphical Password Scheme Resistant to Shoulder-Surfin*.

[20] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," *in Third Australasian Conference on Information Security and Privacy (ACISP) : Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.*

ISSN: 2278 – 7798