INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

DIGITAL LOCK: A HYBRID AUTHENTICAION

Mr. Dipak P. Umbarkar[1], Prof. Megha singh[2]
Computer Enggineering Department
RKDF School Of Engineering,Arandia, Indore.
dipak.umbarkar1990@gmail.com

ABSTRACT:

At present conventional secret word patterns are exposed to dictionary attacks, eves dropping and shoulder surfing, numerous shoulder surfing unaltered graphical password patterns proposed. On the other hand, Textual passwords are the utmost public technique used for authentication. There are several graphical password schemes that are planned in the past years. Most users are used word-based passwords than untainted graphical passwords sentence or word-based or character based graphical password schemes have been proposed. Undesirably, none of existing schemes are create graphical lock to resisting the impersonation. The shoulder surfing resistant and other attacks like eves dropping, dictionary attacks, and social engineering attack on text and character are improved by this paper by using colors. In the expected scheme, the operator can robustly, cleanly and professionally login system and inspect the security and usability of the planned system and show the resistance of the proposed scheme to unintended login.

Keywords— Authentication, shoulder surfing, Gauze, Impersonation.

I. INTRODUCTION

Textual password is the most common technique used for authentication. The weaknesses of this technique likely produce eves dropping, social engineering, dictionary attack and shoulder surfing are well-known. Unpredicted and long passwords can make the system protected. On the other hand the main problem is the trouble of memorizing those passwords. Studies have uncovered that users have a tendency to choice small and stress-free password to recall. Fatefully, these passwords can be easily predicted or broken. Other techniques uses are graphical passwords and biometrics. On the other hand these methods have their particular drawback. In Biometrics password techniques such as facial recognition, finger prints etc. have been offered but not yet generally adopted. The main disadvantage of this method is that such systems can be valuable and slow. There are numerous graphical password methods that are planned in the past years. On the other hand most methods are suffered from shoulder surfing attack which is becoming relatively a large problem. There are some graphical passwords patterns that are resistant to shoulder-surfing but they have their particular weaknesses like usability problems or takes large time for login or it has tolerance levels 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. From the time many graphical password methods with different degrees of resistance to shoulder surfing has estimated, e.g., [2] [3] [4] [5][6][7][8][9], and each has its pros and cons. As expected password schemes are vulnerable to shoulder surfing, Sobrado and Birget [2] proposed three shoulder surfing resistant graphical password methods. Maximum users are using text-based passwords than graphical passwords, Zhao et al. [10] proposed S3APS text-based shoulder surfing resistant graphical password methods. In S3PAS, the user has to combine his textual password on the login screen to catch the session password but the login procedure of Zhao et al.'s methods is hard and boring. And then, a number of text-based shoulder surfing resistant graphical password methods have been proposed, such as [11][12][13][14][15]. Undesirably, none of present textual based shoulder surfing resistant graphical password schemes is both protected and effectual adequate. In this paper, we will suggest a better text-based shoulder surfing resistant graphical password structure by with colors and session. The process of the proposed methods is simple and easy to study for users aware with word-based passwords. The user can easily and efficiently to login the system without using any physical keyboard.

II. PREVIOUS WORK

Perrig and Dhamija [3] proposed a graphical authentication method where the user has to distinguish the pre-defined images to confirm user's authenticity. In this scheme, the user chooses a number of images from a group of arbitrary images during registration. After, during login the user has to recognize the formerly selected images for authentication from a group of images as shown in figure 1. This method is susceptible to shoulder.

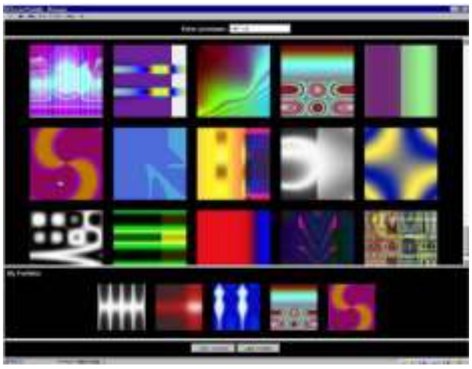


Figure 1: Random images used by Dhamija and Perrig

Wiedenbeck et al. [4] proposed in 2006, the Convex Hull Click Scheme (CHC) as a better version of the Triangle scheme with greater safety and usability. To login the system, the user has to face some challenges. In each challenge, the user has to choose three pass-icons displayed on the login screen, and then click inside the imperceptible convex hull designed by all the showed pass-icons. But, the login time of Convex-Hull Click scheme may be too extensive. In 2009, Gao et al. [5] proposed another shoulder surfing resistant graphical password scheme i.e. Color Login. In which the background color is a practical issue for decreasing the login time. Still, the possibility of accidental login of Color Login is password space is too small and too high. In 2009, Yamamoto et al. [10] proposed a shoulder surfing resistant graphical password scheme, TI-IBA, in which icons are presented spatially and temporally. TI-IBA is less guarded by the screen size and easier for the user to find his pass-icons. Fatefully, TI-IBA's resistance to accidental login is not tough. And, it may be problematic for some users to find his pass-icons temporally displayed. As most users are awake with word-based passwords and conventional text-based password authentication schemes resistance to shoulder surfing. Sreelatha et al. [13], in 2011, also proposed a text and color based shoulder surfing resistant graphical password scheme. In this method user has to in remember the order of some colors. In the similar year, Kim et al. [14] also proposed a text based shoulder surfing resistant graphical password scheme, which employed an analysis method for accidental login resistance and shoulder surfing resistance to analyze the security of their scheme. Fatefully, the resistance of Kim et al.'s scheme to accidental login is not suitable. Rao et al. [16], in 2012, suggested a text-based shoulder surfing resistant graphical password scheme i.e. PPC. To login, the user has to mix his textual password to produce several pass-pairs, and then chase four predefined rules to get his session password on the login screen. The login procedure of PPC is too multipart and uninteresting. During registration user should rate colors that are shown in figure 2. The User should rate colors from 1 to 8 and he can recall it as "RLYOBGIP". The same rating can be given to dissimilar colors. During the login phase, a one interface is showed based on the colors designated by the user. The size of grid is 8×8. This grid encloses digits 1-8 placed randomly in grid cells. The interface also contains strips of colors with four pairs of colors. Each pair of color signifies the row and the column of the grid.

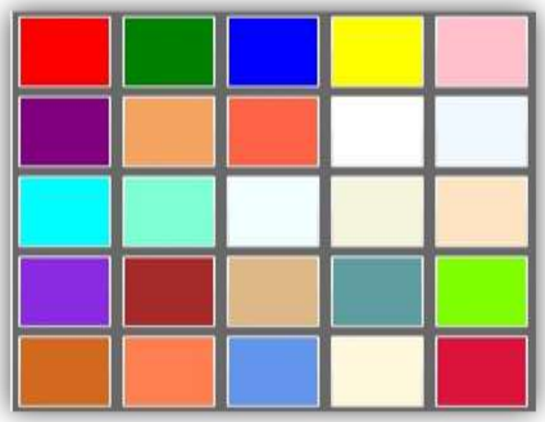


Fig 2 Hybrid color grid

Haichang et al [21] proposed a shoulder-surfing resistant scheme where the user in which has to draw a curve through their password images orderly rather than mark on them directly. This graphical method combines Story and DAS method to deliver validity to the user. Syukri [20] proposed a method where verification is done by drawing user signature using a mouse. This technique involved two phases, registration and verification. In first phase the user draws his signature using mouse, afterward that the system extracts the signature zone. In second phase takings the user signature as input and fixes the standardization of parameters of the signature. The drawback of this method is the copy of the signatures. Is not shoulder surfing resistance.

III. PROPOSED SCHME

Here, we will describe a simple and efficient shoulder surfing resistant graphical password scheme based on texts and colors. Our proposed schemes involved two phases, registration and login phase. We proposed two different techniques, first scheme for username in that the letters used in the propose scheme contains characters, containing 26 lower case letters, 26 upper case letters, symbols and 10 decimal digits. Login scheme contain same things i.e. character and symbol for the password. The proposed scheme includes two stages, first registration stage and second login stage, which can be designated as in the following.

Stage 1:- Registration

At the starting the user has to set his textual username and password X of length Y characters, and select one color as his pas color from colors allocated by the system. The remaining colors not selected by the user are his decoy colors. And, the e-mail address should be resister for re-enabling his inactivated account. The registration stage should continue in a suh circumstances which are free of shoulder surfing. In addition, at the registration stage a confined channel should be established between the user and the system. 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

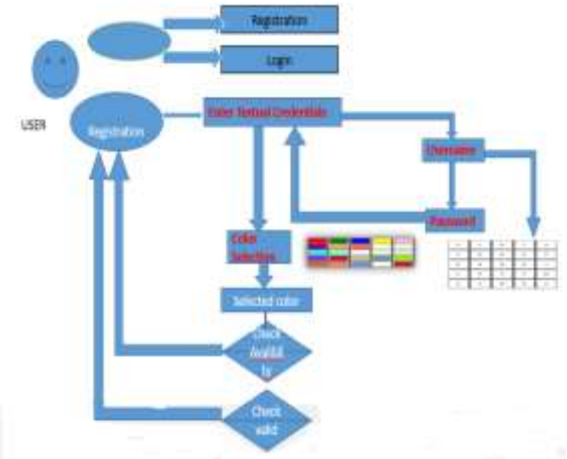
The user how wishes to login the system, for username the system shows a circle composed of uniformly sized subdivisions. The colors of the curves of the subdivisions are different, and each subdivision is accepted by the color of its arc, e.g., the blue subdivision is the subdivision of blue arc. First of all, the characters are positioned averagely and arbitrarily between these sectors. All the showed characters can be concurrently switched into either the neighboring sector clockwise by ticking the “clockwise” key or button once or the adjacent sector anticlockwise by clicking the key or button once, and we also used scrolling mouse for the rotation operations. Then for Password system user enters his password using virtual keyboard i.e. the password submitted during registration of user. When the user login his username an interface consisting of a grid i.e. virtual keyboard is displayed. That virtual keyboard consists of alphabets and numbers that are randomly placed on the virtual keyboard and the interface changes every time. This password which enters using virtual keyboard is a session password. We describe it as follows with the help of example. The user requests to login the system. The system shows a circle composed of sixteen equally sized segments, and places every character between the sixteen sectors averagely and arbitrarily so that each segment covers characters. The 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 symbols are in regular typeface, and the ten decimal digits are in italic typeface. In addition, the button or key for rotating anticlockwise and 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 neighboring region anticlockwise by clicking the “anticlockwise” button once or the neighboring region clockwise by clicking the “clockwise” button once, and the rotation procedures can also be done by scrolling the mouse wheel. Let j = 1. The rotation operation can be illustrated. The user has to rotate the sector containing the j-th pass-character of his password X, denoted by X_i, into his pass-color region, and then ticks the “Confirm” button. Let j = j + 1.

If j < Y, the system arbitrarily permutes all the characters, and then again. Or else, the user has to click the “confirm” key to complete the procedure. Then for password, user has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. Password consists of alphabets and digits. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. Suppose our password is CD intersection latter of that CD is may be U its depending upon position on that character at that time. Next time it will be different. This is repeated for all pairs of password. The password entered by the user is confirmed then to authenticate the user. If the password is correct, the user is permitted to enter in to the system.

If the account is not successfully authenticated for three consecutive times, this account will be inactivated and the system will send an e-mail having the secret link to the user’s registered e-mail address that can be used by the legal user to re-enable his inactivated account.

A. ARCHITECURE

The main security goal is to control a shoulder surfing, brute force attack from large intruder on single or multiple accounts. The users choose traditional textual username and passwords and one color as his pass color in the proposed scheme. As the majority of users are familiar with textual username and 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 the 10 decimal digits in three different typefaces on the login screen, the user can efficiently and simply find his pass-characters. And, the operation of the proposed scheme is easy and simple to learn, the user only has to rotate the sectors to login the system.



B. MATHEMATICAL MODEL

Mathematically, we can achieve the following: we ask a user to choose password of length y, the minimum length of username and Password is 8 Characters and the maximum length of username and password is 16 characters i.e. username length is between 8 to 16 Characters, and choose one color as his pas color from 16 colors assigned by the system. Then all this characters are arbitrarily distributed in 16 sectors of different colors. We call all character as object and chosen characters as a pass object. Then with position of k pass object we have 3 different cases each of which happens with probability of 1/3. Since k pass object are part of password user surely knows which case happens.

In mean time since k pass objects are hidden in N (all characters) objects arbitrarily located on the screen, it is hard for shoulder Surfing attacker to make the properly responses and more hard to obtain the password. Now to provide security, larger the value of k make system more secure with our password scheme but it is more difficult to use. We found that most users are from diversity of groups and are at ease with k=8. We will set mathematical model to prove that by arbitrarily distributing all objects in sectors assurance level greater than $1\text{-}2e^{-54}$ we have following three cases happen with equal probability 1/3.

Case 0: - 16 pass objects are in same sectors.
Case 1: - 16 pass objects in different sectors.
Case 2: - Some pass objects are in same sectors and some in different.

For implementation a and b we have conducted a number of experiments, suppose that password consists of following, a set { s1,s2,s3} of three string and one to one mapping. M1: {case 0, case 1, case 2} --> {s1, s2, s 3}

Implementation 1:-

Pass a series of three senses as follows, enter $s_{m1\ (Case\ i\ )}$ and i= 0,1, 2.

For example s1= Dipak 123, s2= Dipak.Umbarkar, s3= dipak/rohit.

In implementation 2, we let each object has two variations. We note that all other (64-8) =56 objects must also have two variations (to confuse attacker) A user specifies one pass objects and remember two variations as first and second. A

password consists of the following : a set $\{s_{1,1}, s_{1,2}, s_{2,1}, s_{2,2}, s_{3,1}, s_{3,2}\}$ of six string and one to one mapping
M2: {case k, Variation l) | k=0,1,2; l=0,1 case 2} --> { $s_{i,j}$ | i=0,1; ; j=1,2,3}

Implementation 2:-

Pass a series of three senses as follows, enter $s_{m2\ (\text{Case } k,\ \text{variation } l)}$ if case k, k=0, 1, 2 is described on screen and lth variation of specified pass object l=0, 1 is being displayed.
This implementation requires training but it meets higher security than implementation 1.

Implementation 3:-

In this session password depends upon size of that virtual keyboard that means number of rows and number of columns in each case password is different on each login session.

$$\text{Pass} = 7! \times 7!$$

IV. RESULT ANAYLYSIS

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

a) Username space

The total number of all possible Username with length Y is 16 × 64^y. Consider the 64 characters .Therefore, the username space of the proposed scheme is

$$\sum_{y=16} 16 * 64\text{^}y$$

1 Password space

The total number of all possible Passwords with length Y is 7! *7! Consider the 7 rows and 7 Coolum in the virtual keyboard .Therefore, the password space of the proposed scheme is

$$\text{Pass} = 7! \times 7!$$

2 Accidental confirmation resistances for username

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 Y, denote by $U_{al\ (Y)}$, is

$$U_{al\ (Y)} \text{ ---- } \left(\frac{1}{16}\right)^{Y}$$

For example, if L = 10, then

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

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 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

$$U_{al}=\frac{1}{16}\times\sum_{y\ 16}^{15} U$$

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.
We conducted the Analysis of existing systems study of the proposed techniques with 10 participants for each technique. As the techniques are new, first the participants were briefed about the techniques. They were given demonstrations for better understanding purpose. Then each user was requested to login. After that, the usability study was conducted with the students in two sessions. The sessions were conducted in time frame of one week.

Table 1 shows the registration time for each technique. Table 2 shows the log-in time for each technique for the first session of user study. Table 3 shows the log-in time for the second session which was taken after one week of first session.

Table 1 registration time for passwords

Technique	Avg	Min	Max
Text Based	48	36	64
Pair-based Authentication	58	48.8	78.4

Table 2 login time for correct passwords at session 1

Technique	Avg	Min	Max
Text Based	21.6	18.2	34.21
Pair-based Authentication	29.95	24.6	43.26

Table 3 login time for correct passwords at session 2

Technique	Avg	Min	Max
Text Based	24	17	36
Pair-based Authentication	26.25	18	40.4

It is observed that, as the user get practiced over, he is able to login without any problem. If the user is able to remember the username and password or choose the colors, the schemes are resistant to shoulder surfing.

3. Security analysis

As the interface change every time, the session password changes this technique resistant to shoulder surfing. Due to the use of dynamic passwords, dictionary attack is not applicable.

Shoulder Surfing: These are Shoulder Surfing Resistant. In this scheme, resistance is provided by the fact that secret pass created during registration phase remains secret so the session password can’t be enough to find hidden pass in one session.

Brute force attack: The brute force attack due to use of the session passwords is particularly resist by these. The use of these will take out the traditional brute force attack out of the possibility.

4. Usability

The user generally chooses traditional textual passwords and one color as his password in the planned scheme. As maximum users are responsive with textual passwords, it is usually easier for the user to find characters as compare with icons on the login screen. In addition, since the system shows the, the upper case letters ,lower case letters, the symbols “/” and “.”, and the ten decimal digits in three different typefaces on the login screen, the user can easily find his pass-characters. And, the process of the proposed methods is simple to learn, the user has to just rotate the segments to login the system.

V. CONCLUSION

In this paper, we have proposed a hybrid simple text-based shoulder surfing resistant graphical password, in which the user can simply enter the login procedure without worrying about shoulder surfing attacks. The operation of the proposed scheme is straightforward to learn for users attentive with text-based passwords. The user can easily to login the system using virtual keyboard. Finally, we have observed the proposed method resistances of shoulder surfing, brute force attacks and accidental login.

REFERENCES

[1] Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh,” A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme,” IEEE 2nd International Symposium on Next- Generation Electronics (ISNE),February 2013 , Kaohsiung , Taiwan.

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

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

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

[5] 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.

[6] 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.

[7] 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.

[8] 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 .

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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. 20 11.

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

[17] 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 .

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

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

[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.

[21] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, “*A New Graphical Password Scheme Resistant to Shoulder-Surfin.*

[22] M Sreelatha, M Sashi,MD Sultan Ahamer,VManoj Kumar ,”Authentication Schemes for Session Passwords using Color and Images” in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.