IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Graphical Gauze Authentication

Mr. Vicky Ghaytadak[1], Prof. Kulkarni P.R[2]

Department of Computer Engineering, Aditya Engineering College, Beed[1,2]

Abstract: Currently predictable secret word patterns 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 utmost public technique used for authentication. There are several graphical password schemes that are planned in the past years. A maximum users are used 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 engineering resistant graphical gauze by using colors. In the projected scheme, the operator can strongly, simply and professionally login system and examine the security and usability of the planned system 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 technique similar 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 to choice small passwords or passwords that are stress-free to recall. Unluckily, these passwords can be easily predicted or cracked. The different methods are graphical passwords and biometrics. On the other hand these methods have their particular disadvantages. In Biometrics password techniques such as facial recognition, finger prints etc. have been presented but not yet commonly adopted. The main disadvantage 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 past years. On the other hand most 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 particular weaknesses 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 observing above the user's shoulder as he enters his password. From the time numerous graphical password methods with different degrees of resistance to shoulder surfing has projected, 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 [2] 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 of text-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 effectual sufficient. In this paper, we will suggest a better 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.

II. RELATED WORKS

Perrig and Dhamija [3] 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 [2] 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 remember more than a few pass-icons as his password. To login the system, the user has to properly pass the predetermined number of

DOI10.17148/IJARCCE.2017.65102

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

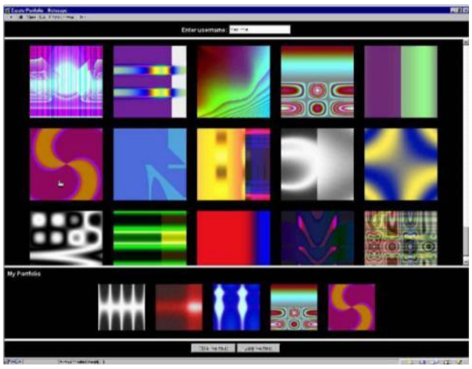

Figure 1: Random images used by Dhamija and Perrig

Wiedenbeck et al. [4] proposed in 2006, the Convex Hull Click Scheme (CHC) as a better version of the Triangle scheme with greater 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. [5] 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 Color Login is too high and the password space is too small. In 2009, Yamamoto et al. [10] 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. [12] 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 to mix 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. [13], in 2011, also proposed a text-based shoulder surfing resistant graphical password scheme by using colors. Clearly, as the user has to in addition remember the order of some colors, the memory load of the user is high. In the similar year, Kim et al. [14] 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. [16], 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.

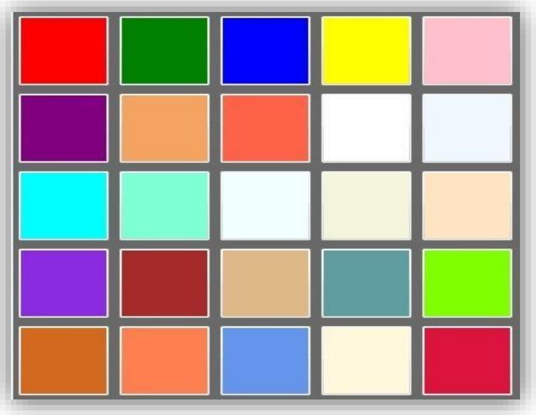

Fig 2 Hybrid color grid

DOI10.17148/IJARCCE.2017.65102

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.

Haichang et al [20] 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 [21] proposed a methods where authentication is done by sketch user signature using a mouse.This technique involved two phases, verification and 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 phase takings 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.

III. THE PROPOSED SCHEME

In this section, we will describe a simple and efficient shoulder surfing resistant graphical password scheme based on colors and texts. Our proposed schemes is divided into two phases first phase is registration and second phase is login phase. We proposed two different technique for username and password first for username in that scheme the letters used in the propose scheme contains characters, containing 26 lower case letters, 26 upper case letters, symbols and 10 decimal digits. Same for the password. 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 username and password K of length L characters, and select one color as his pass color from colors allocated by the system. The remaining colors not selected by the user are his decoy colors. And, the user has to register an e-mail address for re-enabling his inactivated account. The registration stage should continue in a situation free of shoulder surfing. In addition, a protected channel should be established between the user and the system during the registration stage. 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, for username 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 blue subdivision is the subdivision of blue arc. Firstly, characters are positioned randomly and averagely between these sectors. All the showed characters can be concurrently switched into either the neighboring sector right-handed or clockwise by ticking the "clockwise" key or 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. Then for Password system shows the virtual keyboard with the help of that keyboard user enters his password. During registration user submits his password. When the user enters his username an interface consisting of a grid that means virtual keyboard is displayed. That virtual keyboard consists of alphabets and numbers. These are randomly placed on the virtual keyboard and the interface changes every time. This password is a session password. We describe it as follows with the help of example.
The user wishes to login the system. The system shows a circle composed of sixteen equally sized segments, and places characters between the sixteen sectors averagely and randomly 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, 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 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 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 Ki, into his pass- color region, and then ticks the "Confirm" button. Let i = i + 1.

If i < L, the system randomly permutes all the characters, and then again. Or else, the user has to click the "confirm" key to complete the procedure. Now consider for password User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session 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 AV intersection latter of that AV is may be L 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 verified then to authenticate the user. If the password is correct, the user is allowed to enter in to the system.

DOI10.17148/IJARCCE.2017.65102

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.

A Mathematical Model

Mathematically, we can achieve the following: we ask a user to choose password of length l, 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 pass color from 16 colors assigned by the system. Then all this characters are randomly 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 randomly positioned on the screen, it is hard for shoulder Surfing attacker to make the correctly responses and more difficult to obtain the password. Now to provide security, larger the value of k, more secure our password scheme can be, but more difficult to use. We found that most users are from variety of groups and are comfortable with k=8. We will set mathematical model to prove that by randomly distributing all objects in sectors confidence level greater than $1\text{-}2e^{-54}$ we have following three cases happen with equal probability 1/3.

Case 1:- 16 pass objects are in same sectors. Case 2:- 16 pass objects in different sectors.

Case 3:- Some pass objects are in same sectors and some in different.

For implementation 1 and 2 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 1, case 2, case 3} --> {s1,s2,s 3}

Implementation 1:-

Pass a series of three senses as follows, enter sm1(Case i) and i=1,2,3.

For example s1= Avinash 123, s2= Avinash.Sabale, s3= avinash/amol.

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 user specifies one pass objects and remember two variations as first and second. A password consists of the following : a set {s1,1 , s1,2 , s2,1 , s2,2 ,s3 , 1 ,s3,2 } of six string and one to one mapping

M2: {case k, Variation l) | k=1,2,3; l=1,2 case 3} --> { si,j |i=1,2; ; j=1,2,3}

1 Password space

The total number of all possible Password with length L 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 resistance for username

Since the probability of correctly responding to Ki is 16/64, i.e., 1/16, the success probability of accidental login with the password with length L, denote by Ual (L), is

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

For example, if L = 10, then

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

Implementation 2:-

Pass a series of three senses as follows, enter sm2 (Case k, variation l) if case k, k=1,2,3 is rendering on screen and lth variation of specied pass object ,l=1,2 , is being displayed.

This implementation requires training but it meets higher security than implementation 1.

Implementation 3:-

It is for session password in that password is different on each login session its depends upon size of that virtual keyboard that means number of rows and number of columns.

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

Fig. 3 shows the Ual (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.

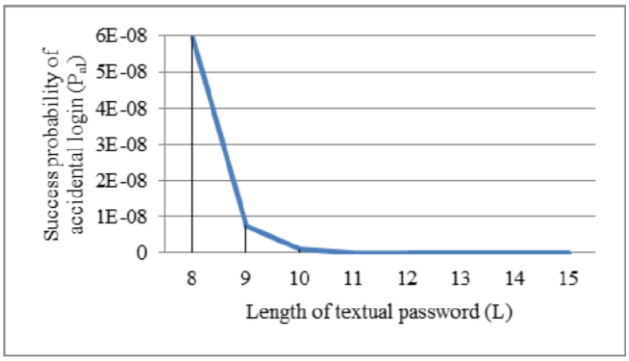

Fig. 3: The success probability of accidental login for different values of L.

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

$$U_{al} = \frac{1}{16} \times \sum_{\square\square - 16}^{15} .$$

IV. RESULT ANALYSIS

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

1 Username space

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

4. Security analysis
As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing. Due to 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 hidden so the session password can't be enough to find secret pass in one session.
Brute force attack: These are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility.

3. 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 shows the, 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 easily whole the login procedure without worrying about shoulder surfing attacks. The operation of the proposed scheme is easy and simple to learn for users aware with text-based passwords. The user can efficiently and easily to login the system without using any physical keyboard. Finally, we have examined 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 Management, 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] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfin.
[21] 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.
[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.