ISSN: 2277-5528
Impact Factor: 3.145

DIGITAL PASSWORD SURVEY

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 predictable secret word patterns are subjected to eves dropping, dictionary attacks and shoulder surfing, numerous shoulder surfing unchanged graphical password patterns proposed. At the same time, the utmost public techniques used for authentication are textual passwords. A number of graphical password schemes that are planned in past years. A most of user's used word-based passwords than pure graphical passwords, so we have proposed word-based graphical password schemes. Undesirably, none of existing schemes are create hybrid digital graphical password scheme. In this paper, we propose an improved mainly textual-based, numerical based shoulder surfing resistant and other attacks like social engineering resistant, eves dropping and dictionary attacks resistant graphical password by using colors. In the predictable scheme, the operator can robustly, simply and efficiently login system and observe the security, usability and resistance to various attack of the designed system.

Index Terms: Authentication, shoulder surfing, hybrid password.

INTRODUCTION

The most general technique used for authentication is text-based password. Due to that it is exposing to well-known attack like eves dropping, social engineering, dictionary attack and shoulder surfing attack. Unpredicted and lengthy passwords can make the system secure. On the other hand this may create problem i.e. the trouble of memorizing those passwords. Studies have showing that End-users have a trend to choice small passwords or passwords that are easy to recall. Fatefully, these passwords can be simply cracked. The different types of methods are present today like graphical passwords and biometrics with some disadvantages. In Biometrics password techniques such as finger prints, facial recognition etc. have been offered but not yet commonly adopted. The main disadvantage of this method is that such systems can be expensive and the overall procedure of identification can be slow. The number of 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 somewhat a big problem. There are graphical passwords patterns that have been predicted which are resistant to shoulder-surfing and they have their particular limitation like usability problems or takes large time for login. The shoulder surfing attack in an attack that can be did by the enemy to get the user's password by watching above the user's shoulder as he enters his password. From last some year the numerous hybrid 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 expected password schemes are disposed to shoulder surfing, Sobrado and Birget [1] proposed three shoulder surfing resistant graphical password methods.

Considering that maximum users are more used textual passwords than graphical passwords, Zhao et al. [10] proposed S3APS, text based shoulder surfing resistant graphical password methods. In S3PAS, the user has to fusion his text password on the login screen to hold the session password. However, the login procedure of Zhao et al.'s methods is hard and unexciting. And then, a number of textual shoulder surfing resistant graphical password methods have been proposed, such as [11][12][13][14][15]. Undesirably, none of present textual shoulder surfing resistant graphical password schemes are both secure and efficient. In this paper, we will suggest a better textual 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 identify the pre-defined images to validate user's authenticity. In this scheme, the user chooses a number of images from a set of arbitrary images during registration. At the time of login the user has to identify the previously selected images for verification from a group of images as shown in figure 1. This method is susceptible to shoulder-surfing. In 2002, Sobrado and Birget [1] proposed three shoulder surfing resistant graphical password schemes, the Movable Frame methods, the Intersection methods and the Triangle methods. However, both the Intersection methods and Movable Frame methods have high failure rate. In the triangle methods user has to select and memorize more than a few pass-icons as his password. At the time of login the user has to suitably pass the predetermined number of challenges. In every challenge, the user has to find three pass-icons among a set of arbitrarily selected icons displayed on the login screen, and then click inside the imperceptible 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 a superior version of the Triangle scheme with better security and usability. At the time of login the user has to properly answer 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 disadvantage of Convex-Hull Click scheme is login time which may be too long. In 2009, Gao et al. [4] proposed a shoulder surfing resistant graphical password scheme with color Login, in which the background color is a working issue for declining the login time. Still, the possibility of unintended login of Color Login is too high and the space of password is too small. In 2009, Yamamoto et al. [9] also proposed a shoulder surfing resistant graphical password scheme i.e. TI-IBA, in which icons are presented spatially and temporally. TI-IBA is less embarrassed by the screen size and easier for the user to find his pass-icons. Fatefully, TI-IBA's resistance to unintended login is not tough. 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 conventional text-based and text based password verification methods have no shoulder surfing resistance. In 2007, Zhao et al. [10] proposed a textual-based shoulder surfing resistant graphical password scheme known as S3PAS, in which the user has to determine his textual password and then follow some rule to mix his textual password to hold a session password to login the system. At the same time, the login methods of Zhao et al.'s are complicated and uninteresting. Sreelatha et al. [12], in 2011, also proposed a text-based shoulder surfing resistant graphical password scheme by using colors. Noticeably, as the user has to in addition memorize the order of some colors which make the memory load of the user is too high. In the similar year, Kim et al. [13] proposed a another text based shoulder surfing resistant graphical password scheme, and at the same time employed an analysis method for shoulder surfing resistance and accidental login resistance to analyze the safety measures of their scheme. Fatefully, the resistance of Kim et al.'s scheme to accidental login is not satisfactory. Rao et al. [15], in 2012, suggested a text-based shoulder surfing resistant graphical password scheme i.e. PPC, in which 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 boring and hard.

In this methods user should rate colors during registration as shown in figure 2. The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". Identical rating can be given to unlike colors. At the time of login phase, when the user 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 and this grid encloses digits 1-8 placed arbitrarily 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.

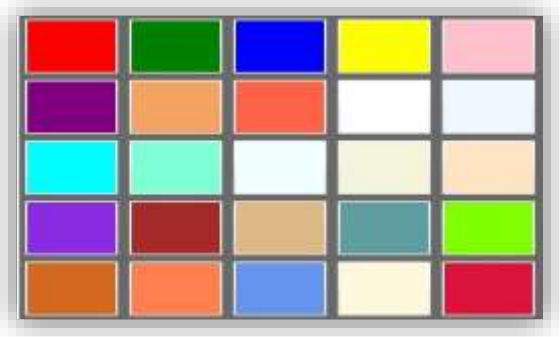

Fig 2 Hybrid color grid

Haichang et al [19] proposed a shoulder-surfing resistant scheme where the user is crucial to draw a curve through their password images randomly rather than indicating them directly. This graphical method combines DAS and Story method to bring authenticity to the user. Syukri [20] proposed a method where mouse is used to sketch the signature and through which authentication is done. This technique involved two stages i.e. verification and registration. At the time of registration phase the user draws his signature with the help of mouse, afterward that the system retrieved the signature zone. Then in verification phase first it takes the user signatures as input and fixes the standardization, then excerpts the parameters of the signature. The disadvantages of this method are the imitation and forgery of the signatures. this method not shoulder surfing resistance.

THE PROPOSED SCHEME

In this section, I will describe an efficient and easy shoulder surfing resistant graphical password scheme based on text with colors. The letters used in the propose scheme contains 64 characters, containing 26 upper case letters,26 lower case letters, symbols "/" ,".",10 decimal digits. The proposed scheme includes two stages, the registration stage and the login stage, which can give as in the following.

Stage 1:- Registration

The user has to set his text password M of length N characters, and select one color as his pass_color from colors allocated by the system. The remaining colors which are not selected by the users are his decoy colors. At the same time the user has to register an e-mail address for re-enabling his inactivated account. The registration stage should continue in condition which is free of shoulder surfing. In addition, a restricted channel should be established between the system and the user during the registration stage by using SSL/TLS [16][17] or any other secure broadcast mechanism. The system stores the user's textual password in the user's entry of the password table that textual password should be encrypted by using the system encryption key.

Stage 2:- Login stage

At the time of login to the system, the system shows a circle composed of uniformly sized subdivisions. The colors of the curves of the subdivisions are contradictory, and each subdivision is accepted by the color of its arc, e.g., the red subdivision is the subdivision of red arc. First of all, all the characters are positioned arbitrarily and averagely between these sectors. All they showed characters can be at the same time as switched into either the neighboring sector clockwise or right handed by ticking the "clockwise" key or button once or the adjacent sector counterclockwise or anticlockwise 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 verified by an example as following.

The user wishes to login the system.

The system is composed of sixteen equally sized segments of circle, and places sixty four characters between the sixteen sectors arbitrarily and averagely so that each segment covers sixteen characters. The sixty four characters are in three typefaces in that the twenty six lower case letters are in bold typeface, the twenty six upper case letters and the two symbols "/" and "." are in italic typeface, and the ten decimal digits are in regular typeface. In addition, there is key or button for rotating anticlockwise and clockwise. The "Confirm" button and the "Login" button are also showed on the front login screen. All the shown characters can be concurrently 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 actions can also be done by scrolling the mouse wheel. Let j = 1. The rotation operation can be demonstrated. The user has to rotate the sector containing the j-th pass_character of his password M, denoted by M_j, into his pass_color region, and then ticks the "Confirm" button. Let j = j + 1.

If j< N, the system arbitrarily permutes all the sixty four shown characters, and then again. Or else, the user has to click the "Login" key to comprehensive the login procedure.

This account will be inactivated, if the account is not successfully authenticated for three successive times, 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 legal user to re-enable his inactivated account. The user has to rotate the region having Mj into his pass_color sector.

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 N is 16×64^N. Therefore, the password space of the proposed scheme is

ISSN: 2277-5528
Impact Factor: 3.145

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

2 Accidental login resistances

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

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

For example, if N = 10, then

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

Fig. 3 shows the $P_{al\,(N)}$ for different values of N. However, since the password length is a secret, the rival has to guess the password length first. As the probability distribution of the lengths of the passwords to be used is

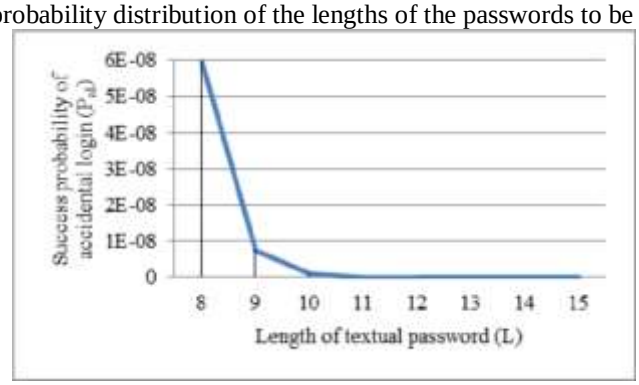

Fig. 3: The success probability of accidental login for different values of L.

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

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

In addition, if the attacker fails to login system repeatedly 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 genuine user to re-enable his inactivated account. That is, only the genuine user can able to access his deactivated account. Thus, accidental login cannot be done simply.

3. Shoulder surfing resistance

If the enemy has recorded the login process T times, he can eradicate 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_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 from 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 N. Clearly, the proposed scheme can resist the shoulder surfing with at least two recorded login processes.

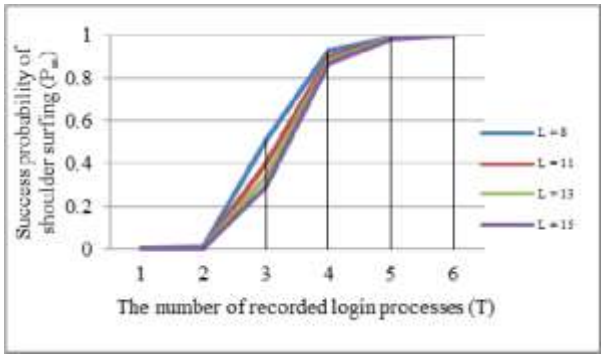

Fig. 4: The success probability of shoulder surfing for T times login process records and different values of L.

4. Usability

The user chooses usual text passwords and one color as his password in the designed scheme. As maximum users are conscious with text passwords, it is generally easier for the user to find characters than icons on the login screen. In addition, since the system shows the, the upper case letters ,lower case letters, the symbols "/" and ".", and the 10 decimal digits in three unlike typefaces on the login screen, the user can simply and capably find his pass_characters. And, the process of the proposed methods is straightforward and easy to learn, the user only has to spin the segments to login the system.

CONCLUSIONS

In this paper, we have planned a simple textual-based shoulder surfing resistant graphical password with color, in which the user can capably and effortlessly login the system procedure without worrying about shoulder surfing attacks. The operation of the proposed scheme is simple to study for users aware with text-based passwords. The user can easily to login the system without using any keyboard i.e. virtual or physical. Lastly, we have studied 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.

REFFERENCES

[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 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*.