Shoulder Surfing Resistant Graphical Password Scheme

Ghadge Sonal[1] Kale Poonam[2] Mahagaonkar Ketaki[3] Sonawane Bhagyashri[4]
[1,2,3,4]U.G Student
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]P K Technical campus, Chakan, Pune, Maharashtra, India

Abstract— Graphical passwords effectively used in authentication system to prevent unauthorized access to mobile device. The security of these mobile devices are limited by shoulder surfing, it refer to direct observation techniques someone's shoulder to get information. Graphical password scheme have been developed to obstruct this attack. We represent efficient techniques towards the graphical authentication system. Graphical password scheme simply refer the color. The colors are represented in the circle and circle containing the different sector having the alphabets and number. Graphical password scheme prevent the accidental login and the shoulder surfing. User is entering his information at the time of creating an account, that time user enter his favorite color. When user is login, user can rotate the sector in such a way that the alphabets or digits which is in the password that should be comes in the favorite color and then press the button confirm. Likewise user is entering his whole password, till the length of that password. Finally press the login button and then user is successfully login without shoulder surfing. So that attacker doesn't get the password whatever is entering in the system.

Key words: Shoulder Surfing, Authentication, Graphical Password, Security Password

I. INTRODUCTION

The shoulder surfing attack can be performed by unauthenticated person to obtain the user's password by watching over the user's shoulder as he enters his password. As conventional password schemes are easily detected by offender. Each time when user withdraws money from an ATM, he types the sequence of identical four-digit PIN number. Anyone who observes this four-digit PIN e.g., by looking over the shoulder of a user, he can easily memorizes the PIN. In conjunction with stolen or skimmed material such as magnetic stripe cards, account numbers printed on receipts, criminals easily gain access e.g., to a victimized user's bank account services.

User has memorizes longer or multiple PIN sequences would have a detrimental effect on recall, no substantial improvement will be achieved for as long as entered information remains constant. User has to perform complicated mathematical calculations when entering PINs is critical to remember. All this would increase the rate of difficulties in PIN entries, which would in turn annoyance to users and thereby reduce the acceptance of the technology. Moreover, service and operation costs e.g., in the retail banking sector would increase due to a growing number of requests to reset PINs which are commonly blocked after three false entries.

Our new shoulder-surfing resistant scheme CDS (Come from DAS and Story) adopts a similar drawing input method in DAS and inherits the association mnemonics in Story for sequence retrieval. It requires users to draw a curve across their password images(pass-images) orderly rather than click directly on them. The drawing method seems to be more compatible with people's writing habit, which may shorten the login time. The drawing passes through both pass-images and decoys, which used to confuse attacker. To avoid revealing the first and last pass-images, the drawing must begin and end with given random images. To enhance its shoulder-surfing resistant properties further, CDS displays degraded images which are difficult to distinguish from a distance or from a side view. Moreover, the majority of the drawing trace will be cleared away as the stylus being sliding, reducing the probability of passwords being revealed. Other complementary measures, such as limiting the length of drawing trace, are also deployed to strengthen the security.

II. LITERATURE REVIEW

Now a day we are using online transaction of money for the different purpose. The most popularly we use the ATM machine for this purpose for withdrawal of money. So we required the password for this purpose but now days shoulder surfing happen. The traditional password schemes are most affected by shoulder surfing. We have proposed the graphical password scheme to resist the shoulder surfing attack. This scheme provides security and minimizes the shoulder surfing attack.

III. RELATED WORK

The Movable Frame scheme, the Intersection scheme, and the Triangle scheme are proposed in 2002,Sobrado and Birget [1]. This three schemes are useful for to resist the shoulder surfing using graphical password schemes. In above mention three schemes two schemes have high failure rates are Movable Frame scheme and Intersection scheme . The user has to choose and memorize several pass-icons as his password in Triangle scheme. To safe login the system, the user has to correctly pass the predetermined number of task. The chosen icons displayed on the login screen, and then click inside the invisible triangle created by those three pass-icons which is selected by the user from the set of pass icon provided on randomly login screen perform this in each task. The Convex Hull Click Scheme (CHC) as an improved version of the Triangle scheme which is proposed in 2006,Wiedenbeck et al. [3].This scheme having superior security and usability. The several challenges has to correctly respond to login the system by the user. To find any three pass-icons displayed on the login screen, and then click inside the invisible convex hull generated by all the displayed pass-icons by the user in challenge. The Convex-Hull Click scheme may be take too long time for login .The proposed a shoulder surfing resistant graphical password scheme Colour Login, in which the background colour is a usable factor for reducing the login time in 2009, Gao et al. [4] However, the probability of accidental login of the password space is too small and ColorLogin is too high.

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. Unfortunately, TI-IBA's resistance to accidental login is not strong. And, it may be difficult for some users to find his pass-icons temporally displayed on the login screen. As most users are familiar with textual passwords and conventional textual password authentication schemes have no shoulder surfing resistance, Zhao et al. [10], in 2007, proposed a text-based shoulder surfing resistant graphical password scheme, S3PAS, in which the user has to find his textual password and then follow special rule to mix his textual password to get a session password to login the system. However, the login process of Zhao et al.'s scheme is complex and tedious. In 2011, Sreelatha et al. [12] also proposed a text-based shoulder surfing resistant graphical password scheme by using colors. Clearly, as the user has to additionally memorize the order of several colors, the memory burden of the user is high. In the same 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. Unfortunately, the resistance of Kim et al.'s scheme to accidental login is not satisfactory. In 2012, Rae et al. [15] proposed 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. However, the login process of PPC is too complicated and tedious.

IV. PROPOSED SCHEME

In this scheme, we will describe a graphical password scheme based on texts and colours. This scheme is used to resistant shoulder surfing attack and it is simple and efficient to use. The alphabet which is used as password contains10 decimal digit, 64 characters, also include 26 upper case letters, 26 lower case letters, and symbols "." and "/". The proposed scheme involves two phases, the authorizing phase and the login phase, which can be described as in the following.

A. Authorizing Phase

The user has to set his textual password P of length N which is of minimum of 8 characters and maximum of 15 characters, and choose one colour from the given eight colours assigned by the system. The remaining 7 colours not chosen by the user. The user has to register an e-mail address for re-enabling his disabled account. The authorizing phase should proceed in an environment free of shoulder surfing. In addition, a secure channel should be established between the system and the user during the authorizing phase by using SSL/TLS [16][17] or any other secure transmission mechanism. The system stores the user's textual password in the user's entry in the password table, which should be encrypted by the system key.

B. Login Phase

The user requests to login the ATM system for any traction of money, and the ATM system displays a circle composed of 8 equally sized sectors. The different colours are assign to the arcs of the 8 sectors , and each sector is identified by the colour of its arc, e.g., the pink sector is the sector of pink arc. Initially, 64 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counterclockwise by clicking the "counterclockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel. The login screen of the proposed scheme can be illustrated by an example shown in Fig. 1. To login the ATM system, the user has to finish the following steps:

- Step 1: The user requests to login the ATM system.
- Step 2: The ATM system displays a circle composed of 8 equally sized sectors, and places 64 characters among the 8 sectors averagely and randomly so that each sector contains 8 characters. The 64 characters are in three typefaces in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the two symbols "." And "/" are in regular typeface, and the 10 decimal digits are in italic typeface. In addition, the button for rotating clockwise, the button for rotating counterclockwise, the "Confirm" button, and the "Login" button are also displayed on the login screen. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counterclockwise by clicking the "counterclockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel. Let I = 1. The rotation operation can be illustrated by an example shown in Fig. 2.
- Step 3: The user has to rotate the sector containing the i-th pass-character of his password K, denoted by Ki, into his pass-color sector, and then clicks the "Confirm" button. Let i = i + 1.

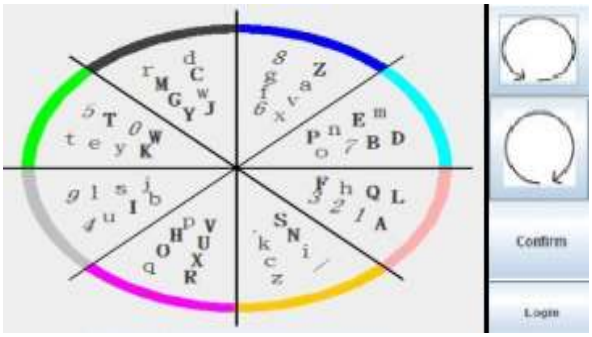

Fig. 1: An Example of the Login Screen

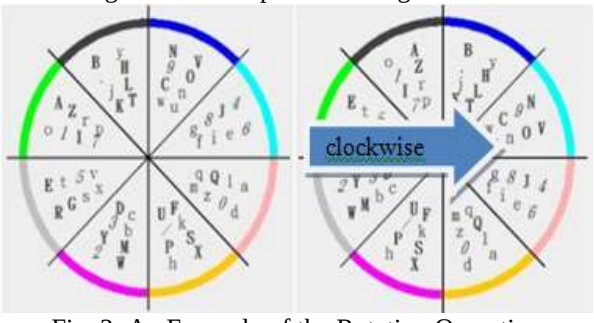

Fig. 2: An Example of the Rotation Operation

- Step 4: If i < N, the ATM system randomly permutes all the 64 displayed characters, and then GOTOs Step 3.

Otherwise, the user has to click the "Login" button to complete the login process. If the account is not successfully authenticated for three consecutive times, this account will be disabled and the system will send to the user's registered e-mail address an e-mail containing the secret link that can be used by the legitimate user to re-enable his disabled account. The login process of the proposed scheme can be illustrated by an example shown in Fig. 3. The user has to rotate the sector (marked with orange dotted line for illustration only) containing Ki (marked with small red circle for illustration only) into his pass-color sector (marked with brown dotted line for illustration).

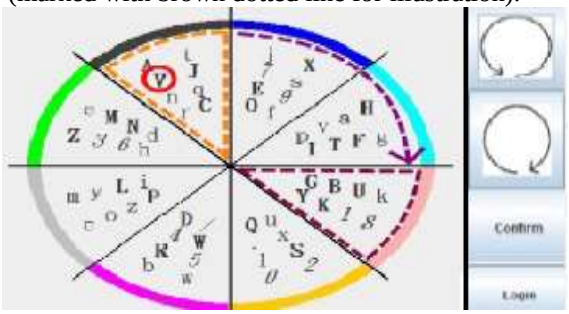

Fig. 3: An example of rotating the sector containing Ki into the pass-colour sector.

C. Advantages-

- This method prevent the shoulder surfing.
- Unauthorized user cannot recognize the password.
- It provides the better security.
- Toresistshoulder surfing using graphical password scheme.
- To introduce graphical password scheme.
- To introduce such password scheme this is easy to use.
- To reduce the hacking of password.

D. Limitations:

When we enter the wrong password three times we can't login again after the reauthentication of user done by user.

V. Result and Discussion

We are entering the password in the systems that time the person who is behind of us he will get the idea of our password so that the hacker can access our account unauthorized. For that we are providing a new system in that the hacker doesn't recognized the password if he is behind of the user.

Shoulder surfing is happen in our system the unauthorized person can access our information which is in our system, so for avoiding such type of access of our confidential information we developed the system such as shoulder surfing resistant graphical password.

The shoulder surfing attack means attack that can be performed by the unauthorized user to get the user's password of authorized user watching from the user's shoulder as he enters his password. As conventional password schemes are guessable to shoulder surfing, so that in graphical password scheme shoulder surfing problem is avoided by using graphical password.

VI. Conclusion

Graphical password scheme will develop to avoid shoulder surfing attack. Accidental login cannot be performed easily and efficiently. This method will gives the security to authorized user and prevent the reorganization of password to unauthorized user. This system will play the vital role in day to day life for avoiding shoulder surfing attack. we have proposed a simple text-basedshoulder surfing resistant graphical password, in whichthe user can easily and efficiently complete the loginprocess without worrying about shoulder surfing attacks.The operation of the proposed scheme is simple and easyto learn for users familiar with textual passwords. Theuser can easily and efficiently to login the system withoutusing any physical keyboard or on-screen keyboard.Finally, we have analyzed the resistances of the proposedscheme to shoulder surfing and accidental login.

References

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

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

[3] 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. onAdvanced Visual Interfaces, May. 2006, pp. 177-184.

[4] 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.

[5] 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.

[6] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," Proc. of the 2003 Int.Conf. on Security and Management, June 2003, pp. 105-111 .

[7] 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.

[8] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme," Proc. of the FirstInt. Workshop.on Education Technology and ComputerScience, Mar. 2009, pp. 90-95.

[9] T. Yamamoto, Y. Kojima, and M. Nishigaki, "A shoulder surfing-resistant image-based authentication system with temporal indirect image selection," Proc. of the 2009 Int.Conf. on Security and Management, July 2009, pp. 188- 194.

[10] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," Proc. of 21st Int. Conf. on Advanced InformationNetworking and Applications Workshops, vol. 2, May 2007, pp. 467-472.

[11] B. R. Cheng, W. C. Ku, and W. P. Chen, "An efficient login-recording attack resistant graphical password

scheme Sector Login," Proc. of 2010 Conf. on Innovative Applications of Information Security Technology, Dec.2010, pp. 204-210.
[12] 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.
[13] 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.
[14] Z. Imran and R. Nizami, "Advance secure login," International Journal of Scientific and Research Publications, vol. 1, Dec. 2011.
[15] 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 .
[16] Network Working Group of the IETF, "The Secure Sockets Layer (SSL) Protocol Version 3.0," RFC 6101, 2011.
[17] Network Working Group of the IETF, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246,2008.

