Shoulder Surfing Resistant Text-based Graphical Password Scheme

Sumit H. Wagh
Student ME (Computer)
YTCEM, Bhivpuri Road,
Karjat, Mumbai

Aarti G. Ambekar
Assistant Professor
D.J.Sanghavi College of Engg
Mumbai

ABSTRACT
Many authentications schemes are presented, but users are familiar with textual password schemes. Textual password schemes are vulnerable to shoulder surfing andkeyloggers. To overcome this problem many other authentication systems like token based authentication, biometric based authentication systems, graphical password schemes have been proposed. However biometric based authentication systems are costly and graphical password systems are not that secure and efficient.In this paper, an improved text-based graphical password scheme by using sectors is proposed, which is shoulder surfing as well as keylogger resistant.

Keywords
Shoulder surfing, Graphical password, Key logger, Sector base, Authentication

1. INTRODUCTION
Shoulder surfing is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping attacker to gain access to the system. Keylogging is the practice of noting the keys struck on a keyboard , typically in a manner so that person using the keyboard is unaware that such action is monitored. There are two types of keyloggers viz. software keylogger and hardware keylogger. Software keylogger are installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and saves every keystroke into the file or In the memory of the hardware device.Many authentication systems are invented to avoid problem of shoulder surfing and keyloggers for e.g. biometric systems. But these systems are costly and each and every individual user cannot afford to purchase biometric system.As conventional password system is vulnerable to shoulder surfing and keyloggers. To avoid the thread from keyloggers many graphical password schemes have been proposed e.g.[1] [2][3][4] [5] [6] [7][8][9][10][11][12] and each has its advantage and disadvantages. However, most of the current graphical password schemes are vulnerable to shoulder surfing[1][2][3][4][5][6] a known risk where attacker can capture a password by direct observation or by recording authentication session. Due to visual interface, shoulder surfing becomes an exacerbated problem in graphical passwords. Several approaches have been developed to deal with this problem, but they have significant usability drawbacks, usually in time and effort to log in, making them less suitable for everyday authentication

2. RELATED WORK
Sobrado and Birget[1][2][3]proposed three shoulder surfing resistant graphical password schemes, in 2002. Those passwords schemes where namely Movable Frame scheme, The intersection scheme and Triangle scheme. In Movable frame password scheme user's picture password is located in the frame user have to create an invisible straight line that connect entire picture password. In Intersection scheme user has to intersect all the pass images. Both of these scheme has high Triangle scheme is complex and tiresome as user has to choose and memorize several pass icons and his password. In 2009, Yamamoto et al.[4] proposed shoulder surfing resistant graphical password scheme, TI-IBA. In this system, it was easy to find pass icons as this proposed system was less constraint by screen size, but this system was vulnerable to accidental login.Blonder et al [5] proposed a graphical password scheme, in which user has to create his password by clicking on various locations on an image. While login into the system, user must click on the approximate areas of those location. "Passface" technique [6] was proposed by Real User Corporation, the user is asked to select four images of human faces as a desired password. In authentication phase, the user is presented with matrix of nine human faces, consisting of one previously selected face and eight decoy faces. The user recognizes and clicks on the chosen face. Same process is repeated several times. The user is authenticated if he correctly identifies all the faces. However, these systems were highly susceptible for shoulder surfing. In 2007, Zhao [7] et al. proposed a text-based shoulder surfing resistant graphical password scheme. In this scheme user has to memorize his textual password, this password is referred as " Original password" . While login, the user must find all his original pass-characters in login image and then make some clicks inside the invisible triangle which are called as "pass triangles" created by three original pass-character following a certain click rule. These session pass-clicks is user's "session passwords". By using these session password user has to login the system. However, login process of this system is complex and tiresome. Sreelatha et al. ,[8] In 2011 proposed a text-based graphical password scheme using colours. This scheme was less effective as effort of memorizing colour is involved.

3. PROPOSED SYSTEM
In this, section, a simple and efficient shoulder surfing resistant and keylogger resistant graphical password scheme based on text and sectors is described. The user can choose his password from 72 character set. The character set is consists of 26 lower case(a-z) alphabets, 26 upper case(A-Z) alphabets, 10 decimal digits(0-9)and 10 special symbols(.,/,!,@,#,$,%,^,&,*). In proposed system, login screen is consisting of a circle and that circle is divided into six sectors, all the 72 characters are equally and randomly distributed among these six sectors. The proposed scheme involves Registration phase and Login phase. This can be described as following.

3.1 Registration Phase:

It is suggested that user must carried out registration phase in environment free of shoulder surfing and keylogger. In addition secure transmission mechanism such as SSL/TSL should be established during registration phase. The user has to set his textual password P of length L(7<L<16) characters, and choose one sector as his pass sector from 6 sectors. The user's textual password is stored in the system in password table, which should be encrypted using system key.

3.2 Login phase:

The user request to login the system and system displays a circle composed of 6 sectors. Each sector is identified by sector number. 72 characters are placed among these sectors, 12 characters in each sector. There are two buttons '"clockwise" and " anti-clockwise" to simultaneously rotate the characters in adjacent sectors.The user can rotate characters clockwise to adjacent sector by clicking "clockwise" button once and anticlockwise to adjacent sector by clicking "anticlockwise" button once. An example of login screen is shown in Fig. 1.and an example of rotation operation is as shown in Fig. 2.

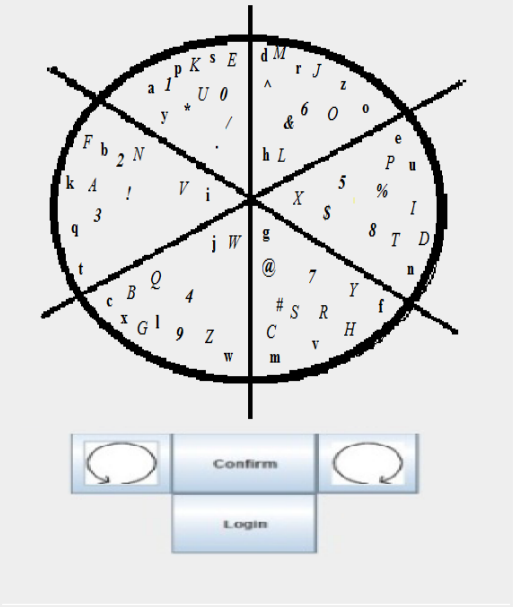

Fig.1 An example of login screen.

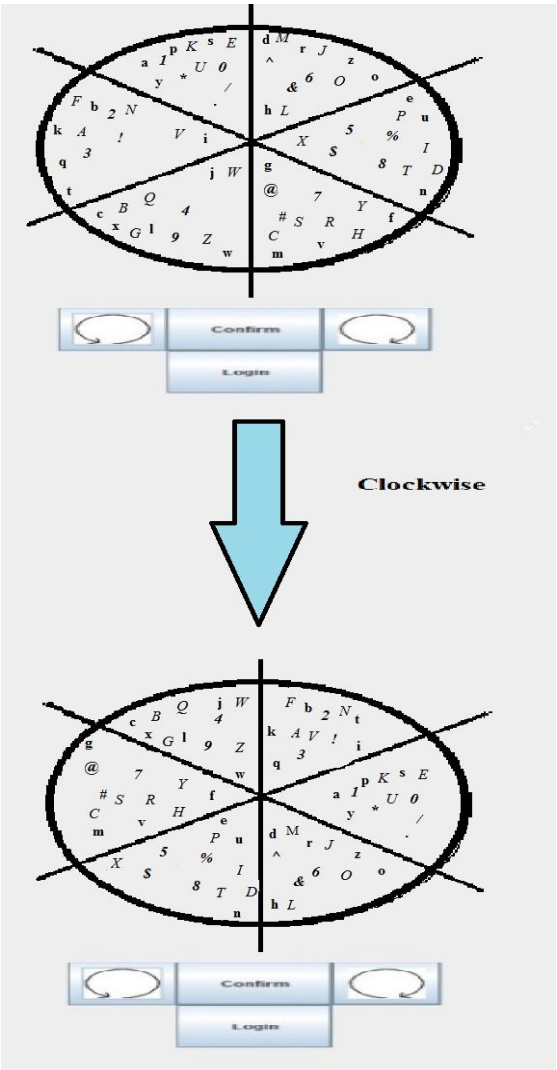

Fig.2 An example of rotation operation.

To login the system user has to finish following steps.
Step 1: The user request to login the system.

Step 2: The login screen displays a circle composed of 6 equally sized sectors, and places 72 characters among the 6 sectors randomly such that each sector contains 12 characters. The 72 characters are in three typefaces in that the 26 upper case latter in regular typeface, 26 lower case characters and special symbols in regular typeface, and 10 decimal digits in bold typeface. In addition, the button for rotating clockwise, the button for rotating anticlockwise, the "Confirm button", and "Login" button are also displayed on login screen. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking "clockwise" button or adjacent sector anticlockwise by clicking "anticlockwise" button once, and rotation operation can also be performed by using mouse wheel.

Step 3: The user has to rotate the sector containing the

i-th pass character of his password K, denoted by K_i ,into his designated sector, and then clicks the "Confirm" button. Let i= i+1.

Step 4: If i<L, the system randomly permutes all the 72 characters, and then goes to step 3. Otherwise, user has to click the login button to complete log in process.

The account will be disabled, if the account is not successfully authenticated for three consecutive times. In such case, an email containing secret link will be sent to user which can be used for re-enable his disabled account.

4. ANALYSIS

The analysis of the proposed system is done in this section on basis of usability and security.

4.1 Password space

The proposed system has character set of 72 characters, these characters are equally and randomly divided among 6 sectors and password length L is in between 7<L<16. Therefore total number of all possible

password with length L is 6 * 72L. . Therefore, password space of proposed scheme is given by,

$$\sum_{L=8}^{15} 6 * 72^{L} = 4.346 * 10^{28}$$

4.2 Resistant to accidental login

Since the probability of correctly responding to Ki is 6/72 i.e. 1/12. The success probability of accidental login with the password with length L, denote by Pal(L), is

$$P_{al(L)} = \left(\frac{1}{12}\right)^{L}$$

5. CONCLUSION

In this paper, Shoulder surfing and key logger resistant text-based graphical password scheme is proposed. In this system user can easily login into system without worrying about shoulder surfing and key logger attack. User just have to remember pass sector and alphanumeric password. This scheme is simple and efficient. Unlike other graphical password schemeuser can easily log into the system without remembering graphical sequences.Thissystem do not need use of physical or on-screen keyboard.

6. 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.

[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. or Advanced VisualInterfaces, May.2006, pp. 177-184.

[4] T. Yamamoto, Y. Kojima, and M.,Nishigaki"Ashouldersurfing resistant image-based authenticationsystem with temporal indirect imageselection," Proc. of the 2009 Int. Conf.on Security and Management,July 2009,pp. 188- 194.

[5] G. E. Blonder. Graphical passwords. United States Patent 5559961, 1996.

[6] R. U. Corporation. How the passface system works, 2005

[7] H. Zhao and X. Li, " S3PAS: Ascalable shoulder-surfing resistant textual-graphicalpasswordauthentication scheme," Proc. of 21st Int. Conf. on AdvancedInformationNetworking and ApplicationWorkshops, vol. 2, May2007, pp. 467-472.

[8] M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. ManojKumar."Authenticationschemes for session passwords using color and images," *International Journal of NetworkSecurity& Its Application*, vol. 3, no. 3, May 2011

[9] B. Hartanto, B. Santoso, and S. Welly, " The usage of graphical password as a replacement to thealphanumerical password,"*Informatika*, vol.7, no 2, 2006, pp. 91-97.

[10] 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

[11] 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

[12] 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.

[13] B. R. Cheng, W. C. Ku, and W. P Chen, "An efficient login-recording attack resistant *of* graphical password scheme －SectorLogin,"

[14] Proc. of 2010 Conf .on Innovative Applications Information Security Technology, Dec. 2010.