International Journal of Engineering & Technology, 7 (1.1) (2018) 234-236

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Graphical password scheme to diminish shoulder surfing

D. Sri Ram Varma [1] *, K. Meghana [1], V. Sai Deepak [1], R. Murugan [2]

[1] Student, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation
[2] Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation
**Corresponding author E-mail: d.sriramvarma999@gmail.com*

Abstract

Many authentication schemes are known to us but none of them are completely secure. Textual password is the most common technique used by majority of the people in the industry. But Textual passwords are vulnerable to dictionary attacks, keyloggers, brute-force attacks, even guessing may work out sometimes. Alternative authentication schemes have been proposed to overcome this problem, some of them are Biometric authentication, retina based authentication, graphical password scheme ETC., Authentication Schemes such as biometric and retina scans are too costly, so they are not always preferred. Not every graphical authentication is secure and efficient. In this paper, an authentication scheme with a combination of text and colour is proposed. This allows the user to log-in to the framework a little more secure.

Keywords: *Authentication; Graphical Password; Shoulder Surfing; Keylogger.*

1. Introduction

Text based password is the most common method to provide access to the protected resources. But there are many limitations for text based password system. Our known way to create a strong password is by using lowercase, uppercase letters, numbers and special characters. But, this can be cracked by using various attacks like dictionary attack, brute force attack, keyloggers, Shoulder Surfing and many such practices. A keylogger records every stroke or entry that the user enters on the keyboard, the attacker can later check the log and get the credentials. Brute force attacks use trial and error method to gain information about the user's credentials such as password, pin. In this attack it uses dictionary words and guesses to the value of the desired data. In the case of Shoulder surfing, the attacker can view the credentials entered by the user by staying behind the victim's shoulder or through security cameras which are unknown to the victim. To overcome the problems observed in the textual password scheme, Graphical password schemes, biometric and retina based authentication schemes are also proposed. However, use of biometric and retina based authentication systems are too costly and graphical password systems are not that efficient and secure enough for our requirement. Graphical Password schemes such as especially picture based system suffer from many known problems, one of such problem is the Shoulder surfing attack. In these pictures based schemes, they are always visible in the interface readily during authentication. If the attacker has a view towards the screen while the user enters or selects the picture, then it's a cake walk for the violator. To address this problem many other methods have been designed to conceal information about the user's credentials, but there are drawbacks regarding usability and security issues.

2. Literature survey

2.1. Dhamija and perrig

Dhamija and Perrig [1] has proposed a solution where the user is asked to select images from a set of random images that is generated by the system in the registration phase.

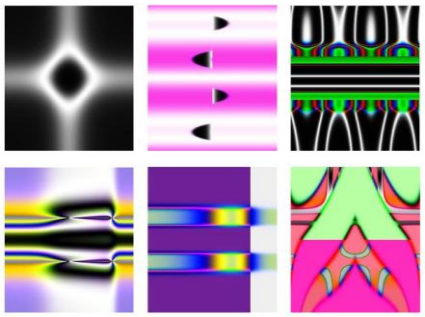

Fig. 1: An Example of the Scheme Proposed by Dhamija and Perrig.

Later in the login phase the user need to identify the previously selected images to gain access into the system. This scheme has been found helpful to majority of the people because remembering a picture is easier than remembering a textual password. This solution has found helpful instead of text based password, but it couldn't solve the shoulder surfing problem as if the attacker has a vision towards the screen where user selecting the pictures, then he can later use the same to gain access.

2.2. Jensen et al method

In this scheme [2], a picture is segmented into 30 blocks and the user needs to select the segments of his choice. A numerical se-

quence is registered based upon the user's selection to generate a password. In the login phase the user has to select the images in the same order as selected previously. Here, the major disadvantage is that the password space is small.

Fig. 2: An example of Jensen et al. Method.

2.3. Graphical password scheme developed by blonder

This scheme [3] allows the user to click on various pixels on an image through which password is created. In the authentication phase, user need to click on the approximate locations where he had chosen previously. If the approximations match the previously selected points, then user gains access to the content.

Fig. 3: An Example of the Scheme Proposed by Blonder.

2.4. Pattern lock

This Scheme [4] is most commonly used in the modern cellular devices to authenticate. This involves in joining minimum four points among the given nine points to form a pattern. User initially registers a pattern and later use the same pattern to gain access. This replaced the textual password in many mobile phones for better convenience and usability. The problem in this technique is that it leaves smudges on the screen. If the violator has access to the device immediately after the user's login, then he could try to guess the pattern to gain access.

Fig. 4: Pattern lock.

2.5. Sobrado and birget

In order to login the framework, the client needs to discover three pass-symbols from an arrangement of symbols that are generated randomly on the login screen, [5] user has to select such that the symbols are in the triangular sector as shown below.

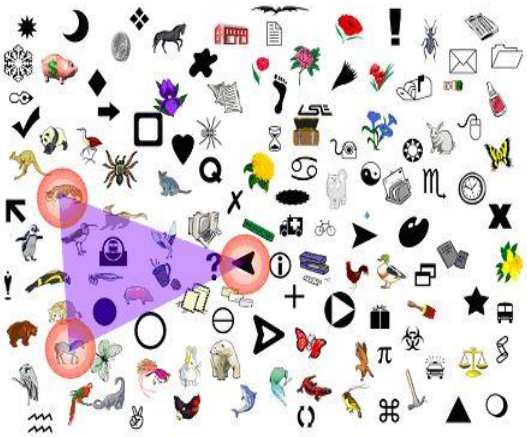

Fig. 5: An Example of the Scheme Proposed by Sobrado and Birget.

2.6. Wiedenbeck et al. Method [6]

In this method, the user is asked to use an image and select any three arbitrary points in that image. The selected point in that image is preserved in the password space with the leverage of some radius. In the login phase the user has to select the same points that were used in the registration phase. However, the time taken to login using this scheme is more.

3. Proposed scheme

In this scheme, we use text and colour as a combination for the password to diminish shoulder surfing attack. The proposed scheme contains upper-case letters, lower-case letters, as well as numbers. This scheme is mainly divided into two phases:

1) Registration and.
2) Login.

User must take care that the registration procedure must be carried out in the domain free from shoulder surfing.

3.1. Registration Phase

In this phase the user has to enter name, email, D.O.B, phone number, password and the colour. Email/username, password and colour are used together to gain access to the framework. The length of the password must be from 8 to14 characters. Colour must be chosen among the eight colours that are displayed on the screen or he can enter the name of the basic colour manually. The

colour chosen by the user is considered to be the pass colour and the remaining seven colours are his decoy colours. Moreover, a secured channel need to be built between the framework and the client in the enrolment stage. For example, SSL/TLS can be used as the security component. The framework need to store the textual-credentials along with the colour in the password table securely.

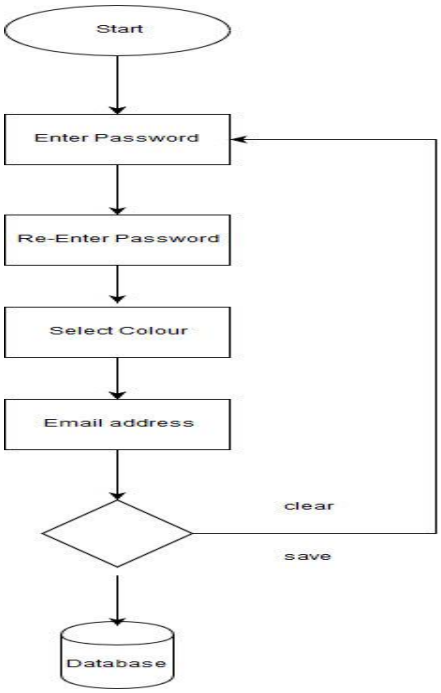

Fig. 6: Flowchart for Registration Phase.

3.2. Login phase

In this phase, the user need to enter the username or email that he used to register in the registration process. If the username is incorrect, then it asks the user to check and enter the username again. If the username entered is correct, then it asks to enter the password.

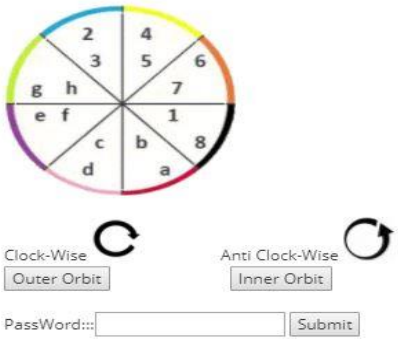

Fig. 7: Working of the Scheme.

A circle divided into 8 segments is shown to the user on the screen. Here, each segment is filled with a colour and characters. colours can be rotated clockwise and anti-clockwise by using the buttons placed under the circle. When the user turns the colour, the characters inside the segment remain constant. User can select the character in the desired colour by using the button. The selected characters will be filled in the textbox arranged in the interface. If the password or colour is incorrect it asks the user to enter again. It can be done up to two incorrect attempts. Further, the account is disabled, and the user need to re-enable the account using the D.O.B, Phone number provided during the registration phase.

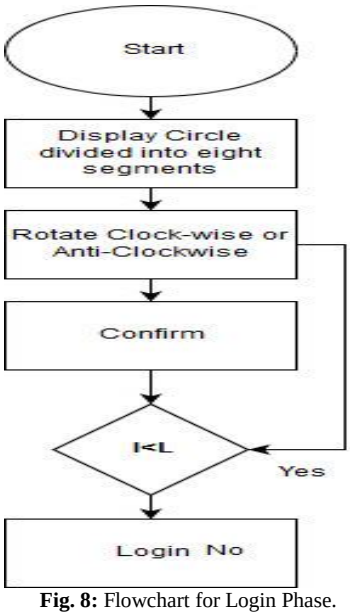

Fig. 8: Flowchart for Login Phase.

4. Conclusion

In this scheme, password is set with the combination of colour and text. The setup of the login environment helps the user to login to the framework efficiently using the mouse. Using this scheme, the user can login to the framework without worrying about the shoulder surfing problem. In future, this scheme can be utilized in web applications where it is prone to shoulder surfing problem.

References

[1] R.Dhamija and A.Perrig. 'Déjà vu:"A User Study Using Images for authentication," in proceedings of 9th USENIX Security Symposium, 2000.
[2] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[3] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium. https://doi.org/10.1007/978-3-540-74835-9_24.
[4] Research in Computer Security (ESORICS), LNCS4734, September 2007.
[5] L. Sobrado "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4,2002.
[6] S. Wiedenbeck 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. https://doi.org/10.1145/1133265.1133303.
[7] Yi-Lun Chen; Wei-Chi Ku; Yu-Chang Yeh; Dun-Min Liao, "a simple text based shoulder surfing resistant graphical password scheme."