A NOVEL GRAPHICAL PASSWORD SYSTEM RESISTANT TO SURFING

Dr. D. Hevin Rajesh
Associate Professor, Department of Information Technology

ABSTRACT

Passwords are widely used when accessing computers, networks, accounts and websites. A big drawback of password is called password problem which is not being resist against several password attacks such as guessing, dictionary attack, key-loggers, shoulder-surfing and social engineering. Other than being secure against these attacks passwords should be easy to remember. Usability and security are two important issues to be concerned about while working with passwords. Graphical passwords seem to be the solution as it. A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). Despite the high standards of Graphical Passwords, they are still vulnerable to some kinds of attacks. The goal is to propose a new Graphical Password scheme that takes advantage of graphical input displays capabilities to achieve better security than text-based passwords. The proposed research is an approach to enhance the existing Graphical Password techniques and resist against attacks like Shoulder Surfing. This system can be improved to provide a wider password space if more server variables are involved. Since conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. However, as most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password schemes have been proposed. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. In this paper, an improved text-based shoulder surfing resistant graphical password scheme by using colour is introduced. In the proposed scheme, shoulder surfing attack is not possible and the user can login to the system easily and efficiently.

Keywords: Shoulder surfing, Dictionary attack, Key-loggers, Authentication, Graphical user interface, Graphical password.

1. INTRODUCTION

AUTHENTICATION METHODS

The existing authentication methods can be divided into three main areas - Token based authentication, Biometric based authentication knowledge based authentication. Token based techniques, such as key cards, bank cards and smart cards are widely used. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted [1]. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. Now the most widely and most commonly used method is alphanumeric username and password authentication. Usually users tend to pick passwords that can be easily guessed, On the other hand, if a password is hard to guess, and then it is often hard to remember [2]. The Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated by the fact that humans can remember pictures better than text. If the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes

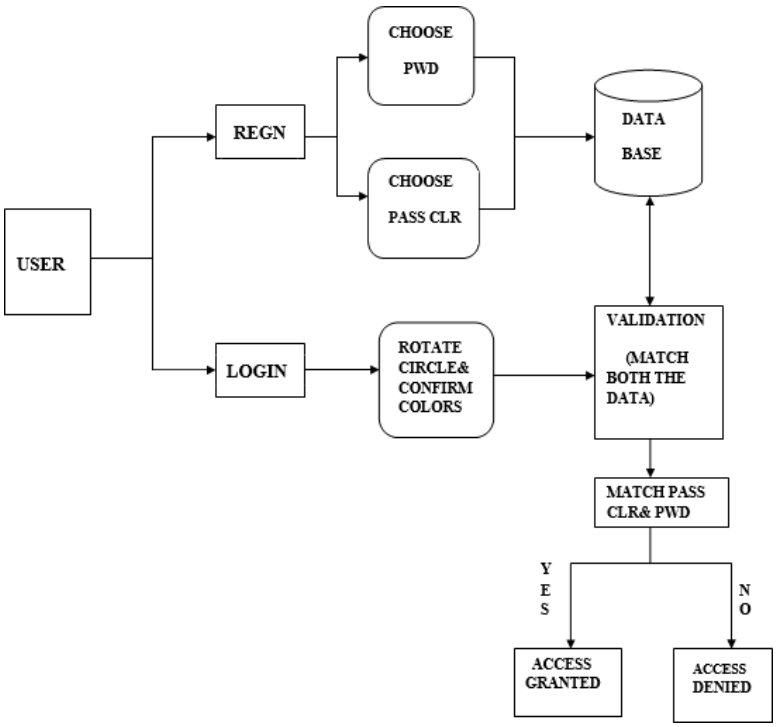
and thus offer better resistance to dictionary attacks. The two category of Graphical password techniques used are recognition-based and recall-based graphical techniques In recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Sobrado and Birget scheme, DAS-Draw a Secret, Persuasive Cred Click Points, and Passfaces etc. are the most commonly using graphical password schemes. All the Graphical password schemes found very secure than alphanumeric passwords. Since it is hard to guess and not easily vulnerable to dictionary attack.

The disadvantages of authentication method is Graphical password scheme require much more storage space than other schemes and the login phase is considerably too long than others.

Every existing password scheme compromised before shoulder surfing when authenticating in public places. An attacker can easily observe and remember a graphical password than others [3].

Even the existing systems are efficient in secure places the main feature we need for a perfect authentication scheme is a secure authentication at anyplace anytime[4].

2. SYSTEM DESIGN



Graphical password authentication method is more secure and flexible than other password authentication scheme. Since it is compromised to shoulder surfing, several text- based shoulder surfing resistant graphical password schemes have been proposed. Unfortunately, none of the existing scheme is not both secure and efficient enough.

Our scheme is an improved text-based shoulder surfing resistant graphical password scheme by using colors .Alphabets used in the propose scheme contains 64 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols "." and "/". This proposed scheme involves two phases, the registration phase and the login phase. In the Registration phase the user has to set his textual password K of length L ($8 \leq L \leq 15$) characters, and choose one color as his pass-color from 8 colors assigned by the system and he needs to give an e-mail address for re-

enabling his disabled account. The registration phase should proceed in an environment free of shoulder surfing. 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. In the login phase displays a circle composed of 8 equally sized sectors. The colors of the arcs of the 8 sectors are different, and each sector is identified by the color of its arc. Initially, 64 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either clockwise or anticlockwise by scrolling the mouse. The user needs to rotate the circle for each character in his password to the pass-color sector. Login button pressed after login phase gives successful login if the password and color is same that we have given in the registration phase, otherwise shows an error message. If the account is not successfully authenticated for three consecutive times, this account will be disabled and system will send secret link to the user's registered e-mail address that can be used by the legitimate user to re- enable his account.

Advantage

1. Operation of this scheme is simple and easy to learn for every user.
2. A complete resistant to shoulder surfing.
3. Login process does not need a physical keyboard or on-screen keyboard.
4. Accidental login cannot be performed easily and efficiently.
5. Login process is comparatively fast and need less storage space.
6. Each pictures selected must be unique.
7. To validate a password, the respondents should create a valid straight line thrice.

3. CONCLUSION

Now a day's computer and internet systems are very common, and the use of these systems is increasing day by day. As its uses increases the need of security is also increasing. Most of the graphical passwords are very difficult to understand, but the operation of our scheme is very simple and easy to learn for users. It provide a complete resistant to many of the password attacks such as shoulder surfing, brute force etc. One of the main advantage is, the login process does not need a physical keyboard or on-screen keyboard. It also provides a strong resistance to Accidental login. Login process is comparatively fast and need less storage space. We can implement our scheme in many of the existing applications.

REFERENCES

[1.] "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme", Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao. IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) -25-26 Feb. 2013, Page(s):161 – 164.

[2.] "Graphical Passwords: A Survey", XiaoyuanSuo Ying Zhu ,G. Scott. Owen ,Computer Security Applications Conference, 21st Annual at Tucson, AZ, 5-9 Dec. 2005. Pages:10 pp. – 472.

[3.] "Design and evaluation of a shoulder-surfing resistant graphical password scheme" , S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, Proc. of Working Conf. on Advanced Visual Interfaces, May. 2006, pp. 177-184.

[4.] "The usage of graphical password as a replacement to the alphanumerical password", Budi Hartanto, BagusSantoso, Siauw Welly , Informatika, vol. 7, no. 2, 2006, pp. 91-97.