International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 2, February 2015

Shoulder Surfing Resistant Illustrative Password Scheme Using Circle Composed of Colored Sectors

[1] Ekta Ahuja,[2]Rupali Badhe, [3]Jinesh Surana,[4]Mayuri Kumbhar
Computer Department (B.E.),Dr. D Y Patil Institute of Engineering and Technology, Pune, India
[1]ekta.ahuja0021@gmail.com, [2]badherupali93@gmail.com,[3] jineshsurana19@gmail.com,[4] mayurikumbhar28@gmail.com

Abstract: **With the vast introduction of the wireless world, the exchanged information now is more prone to security attacks than ever. The main objective of this paper is to secure data using passwords based on text schemas with colors. It secures user's data from shoulder attacks. Since predictable password schemes are susceptible to shoulder surfing; many figurative password schemes have been projected to avoid shoulder attacks. In this paper, we have recommended an improved figurative password scheme with the help of colors which is text based. Access to any system is mostly based on alphanumeric key. However, users have interest on figurative passwords, therefore we have projected text based figurative password scheme. In this paper, for the substantiation purpose, password schema using the figurative password which is text based is used for the login process.**

Index Terms **Authentication approaches, Figurative Password, Shoulder Surfing, and Text based password.**

I. INTRODUCTION

Authentication is an important factor for security. Authentication is supported by passwords. In the current condition, different authentications schemes have been promoted by the researchers. The conventional method used to secure password is alphanumeric password which is also known as textual authentication method. In this method, user is supposed to submit user id and textual password. This may result in susceptibilities such as complex passwords are difficult to memorize and simple passwords are easily hacked. Some problems with textual passwords such as code guessing, shoulder surfing and spyware attacks are common. The other techniques are illustrative passwords and biometrics. Biometrics, like finger prints, voice patterns have been made known but not yet broadly accepted. The chief problem of this approach is that such systems can be costly and the recognition method can be time-consuming. There are many illustrative password schemas that are recommended in the last ten years. However, the majority of them go through shoulder surfing which is becoming reasonably a big problem. In this paper, we are using substantiation scheme which is based on circle composed of colored sectors. The operation of this scheme is easy to learn for users who are well-known with textual passwords. The user can easily and safely login the system and thus it will be used to avoid shoulder attacks.

II. RELATED WORK

Problem 1

To sign in for any system, textual password along with the username is taken as input. Although this approach is safe to an extent but it has some disadvantages as in if a user chooses a short password then it becomes simple for the hacker to guess the secret code and if a user decides to keep a lengthy password, it turns out to be a burden for the user itself to memorize the password [1].

Methodology used:

Because of the drawbacks mentioned above, various graphical password schemes came into image for secure authentication. In this paper [3], they have introduced the present authentication methods and categorized into three main parts: Token based authentication, Biometric based authentication, Knowledge based authentication. They have explained briefly each technique with example along with their advantages and limitations [1].

Outcomes

Results justified that it is harder to break graphical passwords using the usual hacking methods. On the whole, the current illustrative password techniques are still untrained. Much more research is needed for illustrative password techniques to realize higher level of maturity and usefulness [1].

Problem2

Conventional passwords have password hacking problems. Researchers have proposed that password-based verification systems depending on illustrative passwords are easy to recall with enhanced password space.

In this paper [2], two authentication schemes using graphical passwords viz. Pair Pass Char (PPC) and Tricolor Pair Pass Char (TPPC) are used. These schemes support two modes of input: keyboard entry and mouse clicks. In this, the first mode

used is the text mode and the next mode is the graphical mode.

Outcomes

It was found that the average login time increases as the password length increases in both the schemes. Also, the login time for the TPPC scheme is higher than the PPC scheme for the same password length [2].

Problem 3

Illustrative password based authentication has been recommended as an alternative to alphanumeric password scheme as it is susceptible to shoulder surfing, secret camera, spyware attacks, etc. The Illustrative password scheme accomplishes security to a certain point but it is captured by direct inspection through the user's shoulder. Thus the scheme is also susceptible to shoulder-surfing attack [3].

Methodology used

In this paper [3], S3PAS is used. In S3PAS, two types of passwords are produced: real password and session password. The original password is the password that the user desires to input for creating their account. Users put in different session passwords every time. They sign in the system using these session passwords so that they can secure their real password.

Outcomes

The key argument in S3PAS scheme is some extent of more complex and lengthy login process.

III. RECOMMENDED FRAMEWORK

In this segment, we will illustrate a simple and competent graphical password scheme using circle, text and color. This scheme will contain 64 characters, including 26 capital letters, 26 small letters, 10 decimal digits, and two special symbols. The entire authentication process is divided into four parts - user registration module, set password module, login module, verification module, which can be illustrated as follow:

User Registration Module:

In this first step of registration, user fills all the details like name, email id, contact number etc. and chooses one color as his pass color from 8 colors assigned by the system. The length L of password must lie between (8≤L≤16) characters. User has to provide an e-mail address to reset account. User gets an incremental value between 1 and 9 and this value help the user to set his password.

Set Password Module:

During registration, shoulder surfing attack can be controlled using the incremental value received by the user on the contact number provided. User has to add this incremental value to his/her original password and then set the password. The system will store the user's password in the user's entry in the password table, which should be encrypted by the system key.

Login Module:

To login the system, the user has to perform the following steps:

Step 1: The user requests to login the system.

Step 2: The system displays a circle composed of 8 equally sized sectors, and places 64 characters in these 8 sectors in a random manner such that each sector contains 8 characters. The 64 characters are in three typefaces in that the 26 capital letters are in bold typeface, the 26 small letters and the two symbols "." and "/" are in regular typeface, and the 10decimal digits are in italic typeface. In addition, clockwise button, anticlockwise button, confirms button and login button displayed on the login screen.

Step 3: The user has to rotate the sector until the last alphabet of password is present in pass color and then clicks the "Confirm" button.

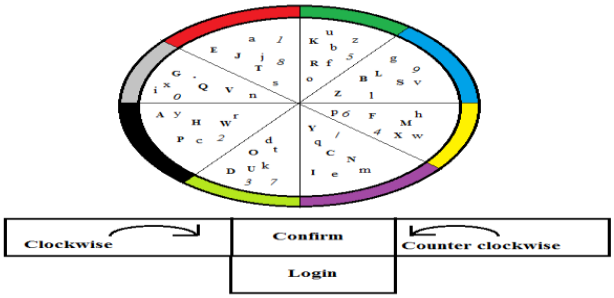

Figure 1. Login Module

Verification Module:

Here, the entered password is compared with the password which is stored in database .If the password matches then the login process goes successful and if not then the system generates an appropriate message. If the account is not successfully authenticated for three repeated times, the account will be disabled and the system will send to the user's registered e-mail address an e-mail containing a link that can be used by the user to re-enable his disabled account.

CONCLUSION

For a good system, high security and good usability both are

needed and cannot be separated. In this paper, we propose an authentication technique based on text and colors through which user can effortlessly and competently complete the login process without worrying about shoulder surfing attacks. The operation of this scheme is straight forward and easy to understand for users.

REFERENCES

[1] Xiaoyuan Suo, Ying Zhu G. Scott. Owen, "Graphical passwords: a survey", 21st Annual Computer Security Applications Conference, 2005.

[2] 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.

[3] Huanyu Zhao and Xiaolin Li, 'S3PAS: A Scalable Shoulder- Surfing Resistant Textual-Graphical Password Authentication Scheme', 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW), 2007.

[4] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme," IEEE 2nd International Symposium on Next-Generation Electronics (ISNE), February 2013.