Shoulder Surfing Resistance using Two Step Graphical Password Scheme for Secure File System

Apoorva Sathe[1], Ashwin Paliwal[2],Prerna Nashte[3],Riddhima Salvi[4]

[1]UG Student, Dept. of Computer Engineering, PVPIT, Bavdhan, Pune, India.
[2]UG Student, Dept. of Computer Engineering, PVPIT, Bavdhan, Pune, India.
[3]UG Student, Dept. of Computer Engineering, PVPIT, Bavdhan, Pune, India.
[4]UG Student, Dept. of Computer Engineering, PVPIT, Bavdhan, Pune, India

ABSTRACT

These days security is one of the major factors associated with sensitive information, to access sensitive information we mostly use text password. But entering text password may lead us to lose control of our password by key logger or shoulder surfing. Shoulder Surfing is a process carried out by a person where he can note user's password by observing his or her shoulder movements. They can be captured by any recording devices such as camera and the recorded video can be used to analyze the shoulder movements. To solve this problem graphical password method is invented. Graphical Password method allows user to select his password graphically without entering the actual password. Hence we are proposing an improved version of shoulder surfing resistant authentication system and password recovery with user file system. In improved version we are adding three layers, first layer is of graphical password authentication, second layer is of personal pin authentication and third is of password recovery by email if the user fails to login in the first two layers. Thus the user file system will have robust authentication where this kind of attack can be prevented.

Keywords: Shoulder Surfing, Graphical password, Password Security, File System, OTP Authentication

ARTICLE INFO

Article History

Received: 26th May 2017

Received in revised form :

26th May 2017

Accepted: 29th May 2017

Published online :

30th May 2017

I. INTRODUCTION

Shoulder surfing is a technique of gathering information such as usernames and passwords by watching over a person's shoulder movements while he/she logs into the system, thereby helping attacker to gain access to the system. Hence while using password based system two points should be in mind:

1) Password must be secure, so that it should be hard to guess.
2) Password must be easy to recall and remember.

This project starts with an examination of solving the entry problem was based on various authentication schemes like authentication using a rotating wheel with 8 sectors [3], pin entry method [2], OTP authentication and time elapse authentication schemes. The main purpose of this paper is to propose an improved text based graphical password scheme for shoulder surfing resistance by using region number and pin entry method. The proposed scheme's working functionality is simple to understand for users, having close acquaintance with textual passwords. The user is now capable to login the system without using computer keyboard or on-screen keyboard. The personal identification number (PIN) which is the second step of this project, typically consist of four decimal digits. As pins are used in a variety of devices such as smart phones, ATM, POS (point of sale) there is a necessity for a secure pin entry method. Shoulder surfing is a process carried out by an attacker where he can note client's password by observing his/her shoulder movement. This can be done with the help of various video recording devices.

II. EXISTING SYSTEM

Text-based password systems are vulnerable to shoulder-surfing attack [1].Shoulder-surfing attack consists of a user being filmed during his/her login. To protect customer's passwords E-commerce vendors adopted various encryption techniques. Text passwords are encrypted before they were sent across networks. A wire-tapping attacker cannot capture the passwords unless they have enough computing power and advanced decryption techniques. However, with a camcorder aiming at the screen of a computer and its key-board, traditional text-based passwords will be captured with 100 percent accuracy.

III. LITERATURE SURVEY

Today, password is the most popular way to authenticate a user to login to computer systems. However, we all know that traditional text-based password systems are vulnerable to the shoulder-surfing attack. To overcome this problem various solutions came into picture respectively:

In 1999, I. Germyn proposed DAS (draw-a-secret) scheme in which a password is a simple picture drawn on a 2-dimensional grid. The coordinates of the grids in which the picture touched are recorded in temporal order of the drawing. It gives users certain degree of freedom to tolerance their drawing during login process. As long as same cells are crossed with same order, a user is authenticated [7].

In 2002, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes a) The Movable Frame scheme b)The Intersection scheme c) The Triangle scheme. The Movable Frame scheme and the Intersection scheme have high failure rate. In the Triangle scheme, the user has to choose and memorize several pass-icons as his password. Every time the user has to login he has to find three pass-icons among a set of randomly chosen icons displayed on the login screen. Then he has to click inside the invisible triangle created by those three pass-icons [9].

In 2003, Man, et al proposed another shoulder-surfing resistant algorithm in which a user selects a number of pictures as pass-objects. Each of these has several variants and each variant is assigned a unique code. During authentication process, the user has to go through various phases. Each scene contains number of decoy-objects and pass-objects. The user has to enter a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass objects in reference to a pair of eyes.

In 2005, Passface is a technique developed by Real User Corporation based on the assumption that people can recall human faces easier than other pictures. The basic idea is as follows. The user is asked to choose four images of human faces from a face database as their future password. In the authentication stage, a grid of nine faces is presented to the user, having eight decoy faces and one face previously chosen by the user. The user memorizes and recognizes the face and clicks anywhere on the known face. Repetition of this process happens for several rounds. On correctly identifying all the faces , the user is noted as an authenticated user.

In 2006, Wiedenbeck et al. proposed the Convex Hull Click Scheme as an improved version of the Triangle scheme with superior security and usability. To login the system, the user has to correctly respond several challenges. In each challenge, the user has to find any three pass-icons presented on the login screen, and later click anywhere inside the invisible convex hull formed by all the displayed pass-icons. However, the login time of Convex-Hull Click scheme may be too long and more tedious.

In 2008, Takada proposed a “fake-pointer” authentication scheme which has a double-layered user interface and uses two pieces of authentication information: passwords and disposal one-time secret information referred to as “answer-indicator”. Although this method has high resistance to shoulder surfing attacks, the users need to remember both background information and passwords for every authentication operation.

In 2009, Gao et al proposed a shoulder surfing resistant graphical password scheme, Color Login, in which the background color is a usable factor for reducing the login time. However, the probability of accidental login of Color Login is too high and the password space is too small.

As most users are familiar with textual passwords and conventional textual password authentication schemes have no shoulder surfing resistance. Zhao et al in 2007, proposed a text-based shoulder surfing resistant graphical password scheme, known as S3PAS, in which the user finds his textual password and mixes his textual password to get a session password for login. However, the login process of Zhao etals scheme is complex and tedious.

In 2011, Sreelatha et al. also proposed a text-based shoulder surfing resistant graphical password scheme by using different colors. The user has to keep in mind the order of various colors, which puts burden on user memory.

In 2012, rao et al. proposed a text-based shoulder surfing resistant graphical password scheme, known as ppc. to login. The user has to mix his textual password in order to create various pass-pairs. After this to get his session password on the login screen follow four predefined rules. But the login process of ppc is too complicated and tedious.

IV. PROBLEM STATEMENT

To propose an improved text-based shoulder surfing resistant graphical password scheme by using PIN entry method and graphical password color algorithm in order to secure a user file system.

V. PROPOSED SYSTEM

The Proposed System divided into Four Modules
1. User Registration: This module is used to register a user with his/her basic information. Also the user has to choose his region number by using PIN Entry Method

2. User Login: This Module is used to provide access to the system after successful completion of entering the password with the help of Graphical password algorithm.

3. Password Recovery: This module is used for user’s password recovery through e-mail if the user fails to login the system in first three attempts.

4. File System: This module is used to maintain sensitive data of the user and have robust security measures for information access.

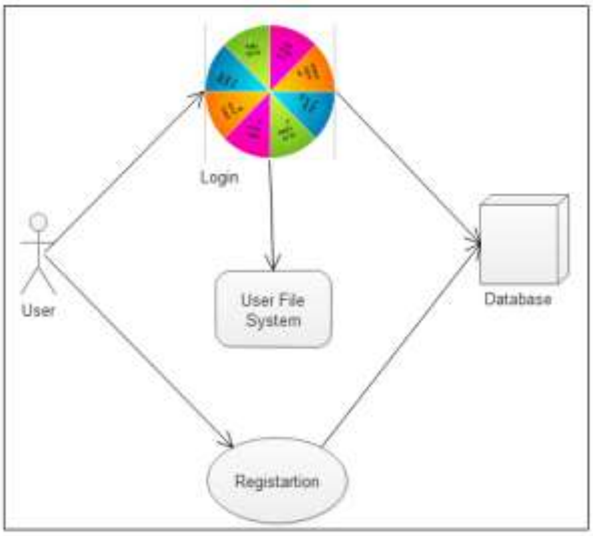


Figure 1: System Architecture

VI. ALGORITHMS

Pin Entry Algorithm

```
Step 1: Start
Step 2: Create One Dimension Array For Each Button.
        int btn_1[0,0,0,0],btn_2[0,0,0,0]….btn_8[0,0,0,0];
        Each digit represents Buttons Round Color i.e. 0=white, 1=Black.
Step 3: Create Eight Arrays for Sequence.
        int seq_1[]..seq_8[];
Step 4: Randomly select the sequence and apply each button.
Step 5:while(round<=4)
{
        Insert the value of black and white for white=0 and black=1
        Into sequence[].
        round++;
}

Step 6: Compare each Button array with sequence[].
Step 7: Match button number will return the region number.
Step 8: Exit.
```

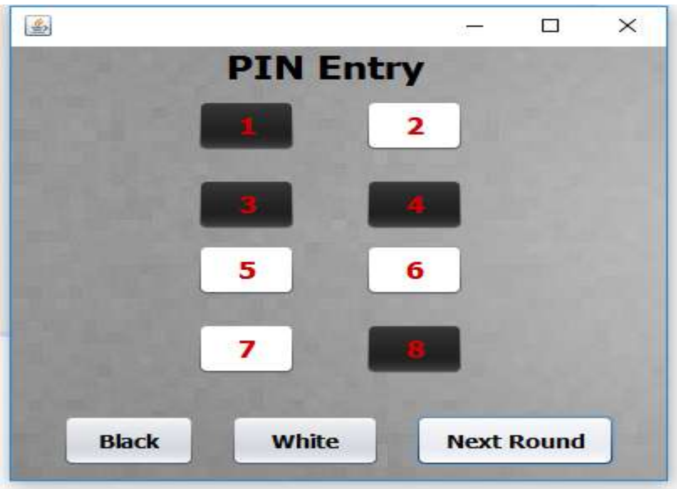


Figure 2: Representation of PIN entry implementation

Graphical Password Color Algorithm

Step 1: The user requests to login the system.
Step 2: The system displays a circle composed of 8 equally sized sectors, and places 73 characters among the 8 sectors randomly. The 73 characters are in three typefaces in that the 26 upper case letters are in bold typeface. The 26 lower case letters and the other 10 special symbols, and the 10 decimal digits are in italic typeface. In addition, the button for scan, the button for rotating clear and the Login button are also displayed on the login screen. All the displayed characters simultaneously rotated into the adjacent sector clockwise and the rotation operations can also be performed by scrolling the mouse wheel.
Let i = 1.
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- sector, and then clicks the Scan button. Let i = i + 1.
Step 4: If i ¡ L, where L is the total length of password, the system randomly permutes all the 73 displayed characters, and then GOTOs Step 3. Otherwise, the user has to click the Login button to complete the login process.

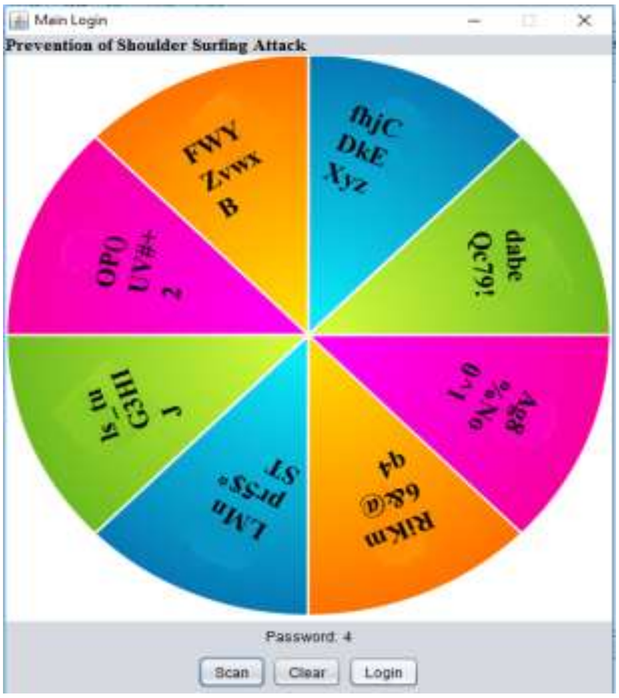
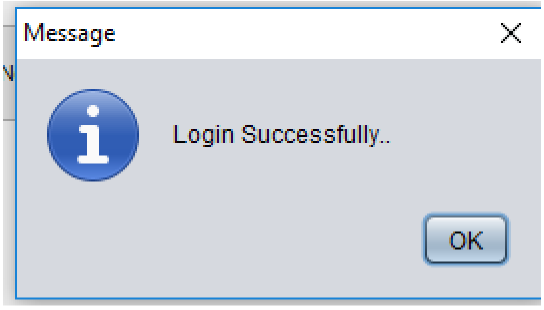


Figure 3: Representation of Graphical Password Color algorithm implementation for accessing file system


Message

Login Successfully..

Figure 4: Representation of successful login access to user's file system

VII. CONCLUSION

We have proposed a simple text-based shoulder surfing resistant graphical password [3], in which the user can easily and efficiently complete the login process without worrying about shoulder surfing attacks. The working of this proposed scheme is easy to learn for users familiar with textual passwords. The region selection is based on PIN entry method [2] which makes the system more effective and secure. The user can easily and efficiently login to the system without using any physical keyboard or on-screen keyboard. Finally, we have analyzed the resistances of the proposed scheme to shoulder surfing and accidental login. In this report, a new authentication technique is proposed based on textual as well as graphical password scheme which if used in a combination can prove highly beneficial.

.

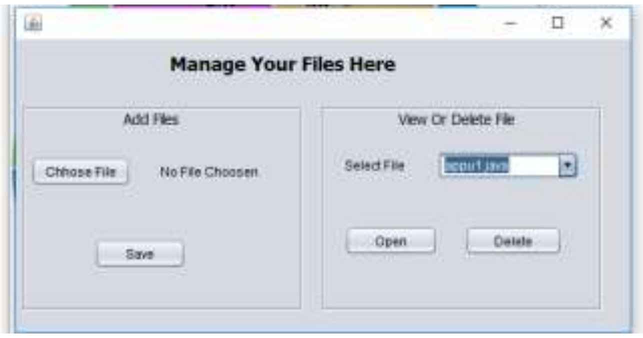


Figure 3: Representation of user file system

REFRENCES

[1] Dhanashree R. Chaudhari , Yogesh B. Gurav, Shoulder Surfing and Keylogger Resistance using Two Step Graphical Password Scheme in International Journal of Science and Research (IJSR) May 2015

[2] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao, A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme, in IEEE 2nd International Symposium on Next- Electronics (ISNE) -February 25-26 , Kaohsiung , Taiwan.

[3] Taekyoung Kwon and Jin Hong, Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder Surfing and Recording Attacks, in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 2, FEBRUARY 2015.

[4] A. Adams and M. A. Sasse. Users are not the enemy:why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM, 42:4146, 1999.

[5]. Q. Yan, J. Han, Y. Li, and R. H. Deng, On limitations of designing leakage-resilient password systems: Attacks, principals and usability, in Proc. 19th Symp. Internet Soc.Netw.Distrib. Syst. Secur. (NDSS), Feb. 2012.

[6] V. Roth, K. Richter, and R. Freidinger, A PIN-entry method resilient against shoulder surfing, in Proc. 11th ACM Conf. Comput. Commun.Secur.(CCS), 2004, pp. 236245.

[7] I. Jermyn, A. Mayer, F. Monrose, M. Reiter and A. Rubin.The design and analysis of graphical passwords.In Proceedings of the 8th USENIX Security Symposium, August 1999.

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

[9]S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human Computer Studies, 63, 2005.

[1] [10] R. U. Corporation. How the passface system works, 2005