International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Shoulder Surfing and Keylogger Resistance using Two Step Graphical Password Scheme

Dhanashree R. Chaudhari[1], Yogesh B. Gurav[2]

[1, 2]Department of Computer Engineering Savitribai Phule Pune University, Pune, India

Abstract: ***In today's world, we use most of the system where we require authentication process for security of sensitive information. Authentication process requires password which could be text password or graphical password. The main problem with text password is shoulder surfing. The shoulder surfing is a process carried out by a person where he can note client's password by observing his or her shoulder movement. The another problem with text password is it can be captured by camera recording. Hence to overcome the problem of shoulder surfing graphical password system is invented. It allows user to enter the password in a graphical instead by direct entering of text password. Hence in this paper we proposed an improved version of shoulder surfing resistant system by using region number. The second step is to enter the personal identification numbers (PINs) which is secure and usable practically which also recover the problem shoulder surfing attack. Here we are using key logger resistance also to avaoid the hacking.***

Keywords: shoulder surfing, authentication, PIN, graphical password

1. Introduction

An authentication method is used in any authentication system and for mobile devices. Easiest way to authenticate is textual based password where generally user tends to choose short length password which is easy to recall[1]. The main limitation of textual based password is that it is easy to guess. Anyone can guess this short password. Hence while using password based system two points should be in mind:

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

Hence an alternative authentication method graphical password authentication method is proposed to recover some limitation of textual based graphical method based on human psychology in which users are better at remembering pictures rather than text. Mouse, stylus and touch screen are used for graphical password authentication process. Graphical passwords are placed to workstations, web login applications, TM machines and mobile devices. Shoulder surfing is a tech-nique of direct observation that is by looking user's shoulder movement, to get information.

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, PIN entry method, OTP Authentication and Time Elapse Authentication schemes. The main purpose of this paper is an improved text based graphical password scheme for shoulder surfing resistant by using region number and PIN entry method. The proposed schemes 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. Since PINs are used in a variety of devices that is smartphones, ATM, PoS (Point of Sale), hence there is a necessity for a secure PIN entry scheme.

Various security schemes have been developed to overcome from this condition, but having system as a both secure and usable remains challenge[2].In this paper we focus on a simple PIN entry method[3]. This method removes shortcomings of the previous method. The BW method is proposed in this paper. The decimal digit keypad to the user is presented in basic BW method which has standard layout, which is divided into two parts one part having keys black in color and the remaining are white in color, and the user has to show the color of his PIN by pressing a separate black or white button. In this, 4-round execution is followed which indicates each PIN digit, so that the 4-digit PIN entry requires 16 rounds to finish. Each round is easy for the user. The remaining of this paper is organized as follows. In next section II, we discuss and review the related works where existing systems will be defined. In section III, we will describe the proposed system. In Section IV, used algorithm will be defined. In Section V expected result will be define.In Section VI possible future works will be discussed, before conclusion in section VII and Section VIII contains acknowledgment will defines before references in Section IX.

2. Related Works

The first recall-based graphical password scheme is DAS having password free-form picture drawn on a 2D grid [4]. In this user need not to remember complex text password. Hence large space for saving that password is saved. But there are difficult to follow drawing rules. Cued-recall is a system which requires users to recall and have to remember selective locations under a given image. Blonder [5] developed another graphical password method in which a creation of password is done by clicking on various locations on an image. Hence during login process, a user has to click on the appropriate areas of those locations. The image can help users to remember their passwords and hence this method is usable than other methods of textual password.

PassPoints[6] is an extended technique of Blonder's system which totally eliminate boundaries which was predefined

Licensed Under Creative Commons Attribution CC BY

and it uses random images. Hence for creating a password in this scheme a user can click on any place on an image. The value of tolerance for each selected pixel is calculated. The user should click within the value of tolerance for authentication.

Passface[7] is a new technique where user has to select four pictures of human faces from the database. In the authen-tication process, the user is given a set of nine faces which consist one face selected by user previously. The user identifies that face and clicks on that identified images anywhere. This process is a loop process having various rounds. The user is authenticated when he identifies all the faces correctly.

The graphical password systems which are explained above all are liable to shoulder surfing attacks. Hence to recover from this issue, Sobrado and Birget developed a graphical password technique [8]. In this technique, the system shows 3 objects among many other objects. A user has to identifies pass-objects and click inside the triangle formed by the 3 pass-objects for authentication.

Hence we know that most of the users are known to textual password. By considering this point S3PAS(Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme)[9] technique is implemented in which user need to find his textual password and then he has to follow a special rule to mix with this password to get a session password for login process. But this process is very complex and tedious also.

A text-based shoulder surfing resistant graphical password method by using colors is proposed by Sreelatha et al[10]. In this user need to remember the order of colors, here the more memory space is required.

PPC[11] is proposed in which user need to mix his textual password for authentication to deliver several pass-pairs. Later user has to follow four predefined rules to get his session pass-word. However, the login process of PPC is too complicated and tedious.

3. Proposed Scheme

We will explain an easy and liable shoulder surfing resistant graphical password scheme based on texts and sector number and white and black PIN entry scheme. The system is more secure and usable also. The proposed system is a two step system in which text based graphical password system is a first step and PIN entry method is a second step.

In first step, text password is used with sector number as a provided factor. The text password contains total 73 characters having 26 alphabets in upper case letters, 26 alphabets in lower case letters, 10 decimal digits and other special symbols. The first step consist of three phases i.e registration phase, login phase and average time phase. The second step consist of 10 digits keypad including two special symbols. The overall description of proposed system is as follows:

A. Text-based graphical password scheme

This is the first step of project. We know that most users are more known to textual password than pure graphical password , so we will use text password with graphical password system in the proposed system. Hence to increase the security and usability in this paper we have proposed an improved text based graphical password scheme which consist of circle or wheel which are divided into eight sectors where each sector consist of characters randomly. Each sector has unique sector number which will be used as a provided factor for authentication process. This step consist of three phases as follows:

1) Registration Phase

In this system, two levels are used for authentication. We use the textual password first and later we use sector number of the wheel or circle. We use One Time Password(OTP) when login failed three times. This OTP is sent to the users mobile number and to the email with secret link. In Registration phase every user has to create account.The user need to give all the details in this phase. During this phase, user has to give one textual password. This is the real password of user. The password would contain characters, numbers and special characters. After textual password, user have to select sector number. The user has to set his textual password and select sector number as his pass-sector from 8 sectors assigned by the system. The remaining 7 sectors are not selected by the user are decoy-sectors. User has to enter mobile number and an e-mail address for re-acquiring his failed account. The password is stored in the database which we are using SQL in this project.

2) Login Phase

During login process system displays a wheel or circle composed of 8 equally sized sectors. Each sector is identified by unique sector number. Initially, 73 characters are divided randomly among these sectors. These all displayed characters simultaneously rotated into adjacent sector clockwise direction only. The rotation operations can also be performed by scrolling the mouse wheel. The relative rotation time difference between adjacent sectors is 2 seconds.

3) Average Time Phase

Average Time of a system to com-plete all authentication phases is recorded and it is compared with a previous average time value of login. User gets authen-ticated only after passing this last phase. If authentication will not be done successfully for three times following in orders, so this account will be unable to do something and secret link will forward to the users e-mail address or mobile number to re-enable his enabled account.

B. PIN Entry Scheme

As we know that PIN entry method is widely used in many application like ATM machine, mobile ,point of sale terminal (PoS) etc. But the main problem with this method is shoulder surfing attack where an attacker can capture password by observing or by camera recording. Hence this paper mentioned an improved PIN entry method having black and white keys.

We have seen different methods to prevent shoulder Surf-ing

Licensed Under Creative Commons Attribution CC BY

attacks we have seen many different methods. These techniques are good to prevent the attacks. But some techniques require more steps and memory to enter a 4 digit pin.Complicated passwords are difficult to remember. For this, we propose new technique i.e. Black and White method(BW method). In this BW technique, in each rotation numeric keypad is displayed black keys and white keys. By triggering a separate button of color below the keypad,to indicate the present color of password key. Suppose if the pin 2 is in Black colour, then user needs to press Black key present below to the key pad. BW method is a 4 cycle method to enter single digit pin. That means to enter 4 digit pin total 16 rounds are carried out. The digit 2 is selected by performing 4 cycles. Hence after performing this 2 added into the matrix. Similarly 4 digits of pin are entered in matrix by applying same technique and then further process of authentication starts. Although it takes more steps to enter pin, but it takes less memory to execute and also it is easy to carry out by user.

C. Keylogger Resistance

A keylogger is a tool which is implemented to acquire the keystrokes entered by using keyboard. It is a battery sized tool which is connected between keyboard and computer. It does not require physical access to the computer. Keylogger tool is used to record messages and emails or any data type through keyboard. All these keystrokes are saved into the log file which can be send to third party. The main purpose behind keylogger tool is to keep monitor that work computers are used for business purpose only. But unfortunately all the information saved in log file can be accessed by third person.Hence there is a necessity to resist this type of attack. Here in this paper, the memory usage per process is calculated and the processes who are getting more memory are considered as suspicious process and which we have to kill for keylooger resistance.

4. Algorithms Used

A. Text-based graphical password scheme

To login the system, following algorithm is used: Step 1: The user request for login to the system. Step 2: Wheel or circle is displayed consist of 8 equally sized sectors, and places 73 characters among the 8 sectors randomly. The 73 characters are set of 26 upper case letters, the 26 lower case letters and the other 10 special symbols, and the 10 decimal digits. The system displayed the button for scan, the button for rotating clear and the Login button. All the displayed characters simultaneously rotated into the adjacent sector clockwise.

Let us assume a = 1.

Step 3: The user need to rotate the sector containing the a-th character of his password K, denoted by K_a, into his pass-sector, and then clicks the Scan button.

Let a = a + 1.

Step 4: If a < L, where L is the total length of password and then GOTO Step 3. Otherwise, user has to click the Login button to complete the login process.

B. PIN Entry Scheme

BW (Black and White) method is used for PIN entry scheme. In this project we are using PIN of length 4 as we can use any length of PIN.

Algorithm 1 PIN Entry Algorithm

1: Start

2: Create one dimension array for each button

int btn1[0,0,0,0], btn2[0,0,0,0],..... btn8[0,0,0,0];

// Each digit represents button's round color i.e. 0=White, 1=Black.

3: Crate eight arrays for sequence. int seq1[], seq2[],..... seq8[];
4: Randomly select the sequence and apply each button.

LOOP Process

5: whilefround 4 g f

Insert the value of black and white for white=0 and black=1 into sequence[];

round++; g
6: Compare each button array with sequence[].

7: Match button number with the return region number.

8: End.

Above Algorithm 1 defines whole description of PIN Entry method. In this algorithm for each button one dimension array is created. There are total eight buttons so initially all arrays will be 0. Every digit represents button's round color that is 0 for white color and 1 for black color. There are eight sequences totally and each will apply to each button. For each sequence unique eight arrays are created. Each sequence select randomly and will apply to each button. PIN Entry method is a 4 round method in which for each round value of black and white button is inserted into sequence array. After completion of 4th round each button array compared with sequence array and button number matched with the return region number.

C. Keylogger Detection

Algorithm for keylogger detection is:

Algorithm 2 Keylogger Detection Algorithm

1: Start
2: // Get Current Running processes while(processlist.hasnext())
f
addprocessname(processname, memoryusage); g
3: // Repeat the step 2 after 30 seconds.so we get two list of processe. Before 30 seconds and after 30 secnds. processlist; //arraylist

Licensed Under Creative Commons Attribution CC BY

processlist1;//arraylist of after 30 seconds
4: //compare memory usage of process of first and second arraylist;
int i=0; while(processlist.hasnext()) f int usage = 0;
Processlist[i].memoryusage-Processlist1[i].memoryusage;
If(usage>0)
f
Addsuspecious(Processlist[i].processname);
g g
5: Step 5: //Display the list of Suspecious process that might be keylogger.
Display-suspeciousprocess();
6: End.

5. Results

In our project as you can see in the shown result , a dialog box will appear first where two options are available that is registration for new users and login for existing users. By selecting registration button , new users can create account by entering all the details. When user complete registration process by filling all the required information , he will press on submit button which will show that new user account is created successfully and information of user is saved in the database. After registration process user will open the login window. After entering username a rotating wheel is displayed which rotate in clockwise direction only. User has to enter the sector number that is pointer in the registration phase only. A window of wheel is displayed with the position of each sector. After pressing next button of that window, a new window will display where the wheel will start to rotate in clockwise direction only and it contains all the alphanumerical symbols. User will click on the scan button when desired symbol comes under the selected region. This step will continue until user enters his complete password. After completion of the password user will click on the login button. After clicking on the login button a dialog box will appear which displays the message as user authentication successful. User will get three chances for login. If he fails to login for three consecutive times , the account will be blocked and One Time Password(OTP) will send to users mobile number. Security and usability are the important factors of this project as we are going to analysis in this section.

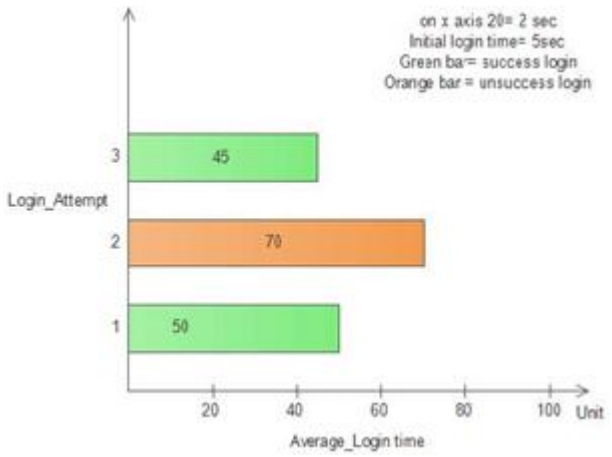


Figure 1: Average Login Time Graph

In above Average login time graph, for first login 5 seconds are taken by system. In next login phase the user took 7 seconds time wich is greater than pevious login time. Hence by calculating average time phase it is required that login time should be less than or equal to previous login time. In next login attempt user has taken 4.5 seconds which is less than previous login time so the user can access system.

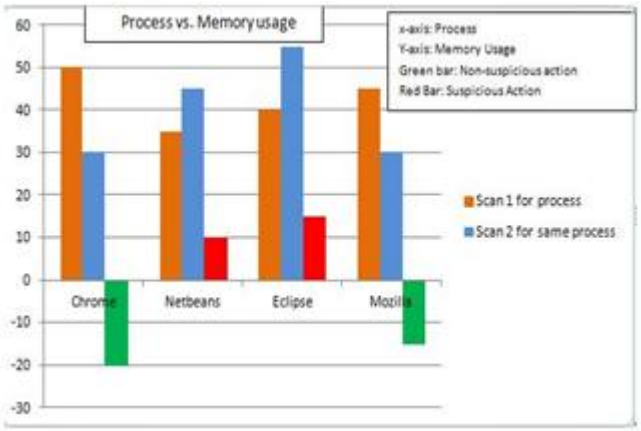


Figure 2: Process vs Memory usage Graph

In above Process vs Memory usage graph, how much memory used by different process is shown. Here the more memory used by process are calculated and shown to the user as a suspicious processes. Hence by result graph we can conclude that processes use very less memory.

6. Possible Future Work

In first step, our primary goal is to resist shoulder surfing attack, but time is important factor in which system should take minimum time to login , hence in future there is a necessity to work on long time taken by registration process and log in process of first step.

Many forms of future enhancements can be done to this system. It is possible to upgrade the application and can make it adaptable to all environments. The number of rounds taken for the PIN entry method can be minimized by optimization methods in future. Any further changes can be easily adaptable because it is based on object-oriented design concept. The security of the PIN entry method can be improved using latest and emerging technologies. In India, this PIN entry based authentication scheme is not used in any net banking application. Hence the banks could follow this authentication technique to increase their security.

In future this PIN entry scheme can be used in:
1) Military
2) Organizations for storing their sensitive information
3) Lockers
4) Other application having security issues.

7. Conclusion

In this paper, we have mentioned improved authentication technique to resist it from shoulder surfing attack by using tex-tual based graphical password system and PIN entry scheme, which gives more flexibility and security used in combination. The proposed system easy to understand and easy to use for users.The proposed method can be used by

Licensed Under Creative Commons Attribution CC BY

many android application which can be in smartphones which increase the security level of the system.

8. Acknowledgment

I am really grateful to the principal for encouragement to carry out this work and I also heartily thank Prof.Y.B.Gurav for giving me an opportunity to complete this research. I would like to thank you for encouraging my research. Your advice on research has been priceless.

References

[1] 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-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan.
[2] 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.
[3] 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.
[4] Paul Dunphy and Jeff Yan, Do Background Images Improve Draw a Secret Graphical Passwords?, ACM October 29November 2, 2007.
[4] Harsh Kumar Sarohi, Farhat Ullah Khan, Graphical Password Authentication Schemes: Current Status and Key Issues, in IJCSI International Journal of Computer Science , March 2013.
[5] M SREELATHA, M SHASHI, M ANIRUDH, MD SULTAN AHAMER, V MANOJ KUMAR Authentication Schemes for Session Passwords using Color and Images",in International Journal of Network Security and Its Applications (IJNSA), Vol.3, No.3, May 2011.
[6] B. K. Alese, A. A. Omojowo, A. T. Adesuyi, A F. Thompson, O. S. Adewale, and F. O. Osuolale, An Enhanced Graphical Password Technique Using Fake Pointers, in Proceedings of Informing Science and IT Education Conference (InSITE) 2015.
[7] Alexander De Luca1, Marian Harbach2, Emanuel von Zezschwitz1, Now You See Me, Now You Dont Protecting Smartphone Authentication from Shoulder Surfers, in ACM April 26May 1, 2014.
[8] Nikam Archana, Bhujbal Tejshri, Warpe Santosh, A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme, International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 2, Special Issue (NCRTIT 2015), January 2015.
[9] Peipei Shi, Bo Zhu, and Amr Youssef A PIN Entry Scheme Resistant to Recording-based Shoulder-Surfing, 2009 Third International Conference on Emerging Security Information, Systems and Technologies.

Licensed Under Creative Commons Attribution CC BY