www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 10988-10991

Textual Graphical Password Scheme against Shoulder Surfing Attack

Saurabh Saoji[1], Swapnali Bhadale[2], Harshada Wagh[3]

[1] *Professor Computer Engineering, Savitribai Phule Pune University/ISB&M School Of Technology, saurabh.saoji22@gmail.com*

[2]*Computer Engineering, Savitribai Phule Pune University/ISB&M School Of Technology, swapb693@gmail.com*

[3]*Computer Engineering, Savitribai Phule Pune University/ISB&M School Of Technology, swapb693@gmail.com*

Abstract: ***Schemes like conventional password schemes such as textual password scheme, graphical scheme are commonly used for authentication. But these schemes are vulnerable to dictionary attack, shoulder surfing attack, accidental login. Hence the text-based shoulder surfing resistant graphical password schemes have been proposed. These existing schemes are not secure and efficient enough and have high failure rate. The text-based shoulder surfing resistant graphical password scheme is improved by using colors. In addition one time password is also used. So it has become more secure. User can easily login to the system. Unauthorized user cannot get the password easily. Hence this scheme provide protection against the shoulder surfing.***

Keywords: accidental login, dictionary attack, shoulders surfing attack, textual password scheme, vulnerable**.**

1. Introduction

The shoulder surfing attack is an attack in which unauthorized person can get user's password by watching over his shoulder when he enters his password .however, as most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password. The existing text-based shoulder surfing resistant graphical password schemes are not secured and efficient enough. In this paper the text-based shoulder surfing resistant graphical password scheme is enhanced by using colors .in the proposed scheme, the user can easily and efficiently login to the system without using any keyboard. It is very easy for the user to login. It has become very difficult to guess the password because of text and color combination. This scheme provides more security.

2. Related Work

Sobrado et.al[1] proposed three shoulder surfing resistant schemes, triangle scheme, movable frame, and intersection scheme. In triangle scheme the system will randomly spread the N number of object and user has to select the pass object as his password which is selected previously to login into the system. User must select the pass object and has to click inside the invisible triangle created by those objects. The same concept is used in movable frame. Only the difference is one object out of the pass object is placed on frame. The pass objects are placed randomly within the frame. User will move the frame until the object on the frame lines up with the remaining both. In intersection method this concept has made more complex. It uses two invisible lines and increased the number of pass object. User has to click near the intersection of two invisible lines, inside the convex quadrilateral formed by those objects. Both the interaction and movable frame have high failure rate. In triangle scheme user has to memorize the pass objects and choose those objects. In July 2009, T. Yamamoto et.al[2] proposed a shoulder-surfing-resistant image-based authentication system with temporal indirect image selection scheme which consist TI-IBA. In TI-IBA icons are displayed temporally. It requires small screen size and easy to find the pass icons for user. The possibility of accidential login is high. After that, the color login is implemented. Color login uses background color, a method not previously considered, to decrease login time greatly. Multiple colors are used to confuse the peepers, while not burdening the legitimate users. So in Dec 2009, H. Gao et.al[3] proposed graphical password scheme using color login. In this color login uses background color which decrease login time. Possibility of accidental login is high and password is too short. The above system is improved by combining text with images or colors to generate session passwords for authentication. Session passwords can be used

only once and every time a new password is generated. In May 2011,M. Sreelatha et.al[4] proposed Hybrid Textual Authentication Scheme. This scheme uses colors and user has to rate the colors in registration phase. During login phase four pairs of colors and 8*8 matrix will be displayed. As the color rating given by the user, the password will generate. First color shows row number and second shows column number of the grid. Intersecting element is the first letter of the password. The user has to memorize the rating and order of the colors. So it becomes very hectic to user. Novel Shoulder-Surfing Resistant Authentication Schemes using Text-Graphical Passwords system is proposed by M.K.Rao in 2012. In PPC some rules are defined and those are followed by the user to get the session password. But this scheme is very complicated and hectic. Then, Yi-Lun Chen et.al[6] proposed a simple text based shoulder surfing resistant graphical password scheme in 2013. The text based shoulder surfing resistant graphical password scheme is improved by using color. In the registration phase, user has to choose one color and set his textual password. In login phase, system displays circle which is divided into 8 sectors and each sector has different colors. All the characters are placed randomly in these sectors. User has to rotate the sector till all characters come into previously chosen color. But characters are not clearly noticeable and hacker can guess the color.

3. Proposed Scheme

It describes a simple and convenient shoulder surfing resistant graphical password scheme based on texts and colors. The 64 characters are used in this scheme which consist 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols "." And "/". This scheme involves two phases, the registration phase and the login phase, which can be described as in the following.

A. Registration phase

The user has to enter his personal details, contact details and account details. User will choose one color as his pass color from 8 colors given by the system. In account details user will enter the 10 digit card number. The account number and textual password pi of length l will be automatically generated by the system. Textual password will be sent to users through sms. The user has to enter an e-mail address for re-enabling his disabled account. 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.

B. Login phase

The user requests for login in to the system, and the system displays a circle which is divided into 8 equal sizes of sectors. Each sector has different color, and each sector is recognized by the color of its arc, e.g., the yellow sector is the sector of yellow arc. Initially, 64 characters are placed randomly in these sectors. These 64 characters can be rotated simultaneously into adjacent sector either clockwise or anticlockwise by clicking the "clockwise" button or "Anticlockwise" button once respectively. The login screen of the proposed scheme can be illustrated by an example shown in Fig.1. For login into the system, the user has to follow the following steps:

Step 1: The user requests for login into the system.

Step 2: The system displays a circle which is divided into 8 equal sizes of sectors. The button for rotating clockwise, the button for rotating anticlockwise, "Confirm" button, and the "Login" buttons are displayed on the login screen. The 64 characters among the 8 sectors are placed randomly and averagely, so that each sector contains 8 characters. All these 64 characters are in three different colors that is the 26 upper case letters and the two symbols "."and "/" are in red color, the 26 lower case letters are in blue color , and the 10 decimal digits are in black color. All these characters can be rotated simultaneously into adjacent sector either clockwise or anticlockwise by clicking the "clockwise" button or "Anticlockwise" button once respectively.

Step 3: The user has to rotate the sector containing the first pass-character of his password P, denoted by Pi, into the color sector which he has chosen in the registration phase, and then clicks on the "Confirm" button.

Step 4: After each confirmation all the characters in each sector will be shuffled. The rotation operation can be illustrated by an example shown in Fig.2.

Step 5: If i < L then do the Step 3 else the user has to click the "Login" button to complete the login process.

Fig.1: An example of the login screen.

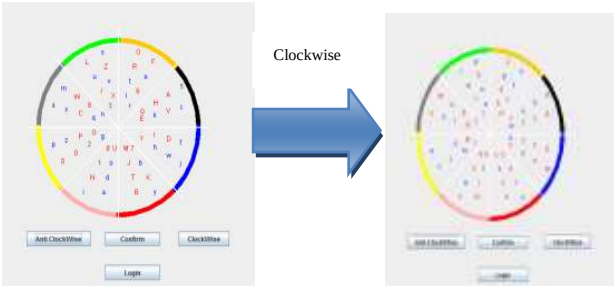

Fig. 2: An example of the rotation operation.

Fig. 3: An example of rotating the sector containing Pi into the pass-color sector.

After this system will display one time password screen which provide second layer authentication and improve security to login process. System will automatically generate one time password. This password would be different for every login session. It consists of 8 characters. These password characters may be the combination of A-Z capital letters, a-z small letters, 0-9 digits, special characters that is "." And "/". System will send him one time password to user through the sms. If the one time password is correct then only user is allowed to move for further transaction.

If the login process is not successful for three times, then this account will be disabled and the system will send the e-mail to the user's registered e-mail address which consist the secret link that can be used by the legitimate user to re-enable his disabled account. The login process of the proposed scheme can be illustrated by an example shown in Fig.3. The user has to rotate the sector.

The textual graphical password scheme and one time password scheme is used for ATM transaction. So at first layer authorized user can login to system by rotating the circle and bringing all characters to pass color one by one and if password is correct then system will display OTP window and one time password is sent to user mobile through sms for second layer of authentication. Legitimate user will enter the one time password which is received on his mobile and if one time password is correct then user will go to further transaction process.

4. Algorithms

Bresenham's Line Drawing Algorithm
This algorithm is used to divide the circle into 8 sectors ang to place the characters in each sector at one line.

1. Read the line end points(x1,y1) and (x2,y2) such that they are not equal. If they equal then plot that point and exit.
2. dx=|x2-x1| and dy=|y2-y1|
3. [Initialize starting point]
   x=x1
   y=y1
4. e=2*dy-dx
5. i=1[Initialize counter]
6. Plot(x , y)
7. while(e>=0)
   {
    y=y+1
    e=e-2*dx
    }
   x=x+1
   e=e+2*dy
8. i=i+1
9. if(i<=dx) then go to step 6
10. Stop

Random Number Generation Algorithm

This algorithm is used to place the 64 characters randomly in each sector
1. To generate a two dimensional matrix with row and column 8*8
2. Put 0 to 63 number into matrix .
3. Select one random number from 0 to 63 .
4. For putting number into matrix system check number is already present or not .
5. If number present then perform Step 3. If not present then put into a matrix and go to step 3.
6. Do step 5 repeatedly up to 0 to 63 inserted into matrix.
7. Print The Matrix.
8. Now Get string which have 64 character " a to z=26,A to Z=26,0 to 9=10,and . /=2" .
9. Get number present into matrix sequentially [0][0] to [7][7] i.e., total 64 character .
10. Select index of string from 64 char. put into that current location .
11. Do step 9 and 10 repeatedly upto [7][7] number.
12. Print Current Matrix With String Char.
13. Display a matrix With Random Printing
14. Stop

5. Conclusion

It is concluded that in a simple text-based shoulder surfing resistant graphical password scheme, the user can easily and efficiently complete the login process without worrying about shoulder surfing attacks. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard. Here double layer of security is provided by using one time password.

Acknowledgment

It gives great pleasure in submitting paper on "Textual Graphical Password Against Shoulder Surfing Attack ".

We would like to thank our Prof. Akanksha Goel (Guide) for giving timely & valuable guidance during successful completion of this paper. She has been a constant source of inspiration and motivation for hard work. She has been very co-operative throughout this paper work. Through this column, it could be our utmost pleasure to express our warm thanks to her for encouragement, co-operation and consent without which we mightn't be able to accomplish this paper. We also thank to all the staff members who were directly and indirectly instrument in enabling us to stay committed for the paper.

We would like to thank our Prof. Seema Bhardwaj(HOD) for giving timely & valuable guidance during successful completion of this paper. We also express our gratitude towards our Prof. J N Shinde(Principal) for his moral support and motivation. This paper has been a new learning experience, which will stand worthy for us in years to come .Finally we would like to thank all individuals directly & indirectly related to our paper.

References

[1] L. Sobrado and J. C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research,* vol. 4, 2002.

[2] T. Yamamoto, Y. Kojima, and M. Nishigaki, "A shoulder surfing resistant image-based authentication system with temporal indirect image selection," *Proc. of the 2009 Int. Conf. on Security and Management*, pp. 188-194, July 2009.

[3] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, "Design and analysis of a graphical password scheme," *Proc. of 4th Int Conf. on Innovative Computing, Information and Control*, pp. 675-678, Dec. 2009.

[4]M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar, "Authentication schemes for session passwords using color and images," *International Journal of Network Security & Its Applications*, vol. 3, no. 3, May 2011.

[5] 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 .

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

Author Profile

MR. SAURABH SAOJI.
Currently pursuing Ph.D in Image processing with Nanotechnology and completed M Tech in Mobile technology from Nagpur and BE in Information Technology from Aurangabad and working in ISB&M School of Technology Pune.

MS. SWAPNALI BHADALE
Currently pursuing BE in Computer Engineering Department from Savitribai Phule Pune Univercsity completed Diploma in Computer Engineering from Maharashtra Board.

MS. HARSHADA WAGH
Currently pursuing BE in Computer Engineering Department from Savitribai Phule Pune Univercsity completed Diploma in Computer Engineering from Maharashtra Board.